TAKE BACK CONTROL *of Your* CYBERSECURITY NOW

Game Changing Concepts on AI and Cyber Governance Solutions for Executives

BY PAUL A. FERRILLO & CHRISTOPHE VELTSOS

published by Advisen Transforming • Insurance℠

sponsored by K2 Intelligence Investigations · Compliance Solutions · Cyber Defense

sponsored by AIG

To my beautiful wife Patricia, my one and only, my Northstar, my guiding light, and my best friend. Thank you for being there for me always.

— Paul

To my wife, Jennifer, thank you for your love, your support, and for enabling me to reach new heights. To my kids, N1 & N2, thank you for your patience and unconditional love. To my parents, thank you for nurturing my curiosity, and for instilling in me a love of learning. To my students, thank you for your drive to learn; it inspires me.

— Chris

published by Advisen Transforming • Insurance

sponsored by K2 Intelligence Investigations • Compliance Solutions • Cyber Defense

sponsored by AIG

Strength and capability

Helping clients better prepare for tomorrow

Forward-thinking answers and technology

WHY AIG

Reliable and responsive claims

Creative and tailored customer solutions

Pioneers and market leaders

AIG®

Bring on tomorrow®

www.aig.com/whyaig

ABOUT PAUL A. FERRILLO

PAUL FERRILLO is counsel in Weil's Litigation Department, where he focuses on complex securities and business litigation, and internal investigations. He also is part of Weil's Cybersecurity, Data Privacy & Information Management practice, where he focuses primarily on cybersecurity corporate governance issues, and assists clients with governance, disclosure, and regulatory matters relating to their cybersecurity postures and the regulatory requirements which govern them.

Mr. Ferrillo has substantial experience in the representation of public companies and their directors and officers in shareholder class and derivative actions, as well as in internal investigations. In particular, Mr. Ferrillo has coordinated numerous internal investigations on behalf of audit committees and special committees, and handled the defense of several significant securities class actions alleging accounting irregularities and/or financial fraud.

Mr. Ferrillo has represented companies in a wide range of industries, including retail, apparel, insurance, financial services, energy, oil and gas, and real estate.

Mr. Ferrillo also regularly counsels clients in the growing field of cybersecurity corporate governance, which is an increasingly important part of a Board's enterprise risk management function. Mr. Ferrillo also counsels clients on cyber governance best practices (using as a base the National Institute of Standards and Technology cybersecurity framework, which was announced on February 14, 2014), third-party vendor due diligence issues, cybersecurity regulatory compliance issues for Private Equity firms, Hedge Funds, and Financial Institutions that have been promulgated by the SEC, FINRA, the FTC, and the FDIC/OCC, the preparation and practicing of cybersecurity incident response plans, as well as evaluating and procuring cyber liability insurance to protect against losses suffered by Companies as a result the theft of consumer or personally identifiable information, or as a result of the destruction of servers and corporate infrastructure.

Outside of his D&O insurance practice, Mr. Ferrillo is a prolific writer, speaker, and commentator on a wide range of subjects. He is a frequent contributor of articles concerning securities, cybersecurity, corporate governance, and accounting fraud issues to the New York Law Journal, D&O Diary, Harvard Law School's Forum on Corporate Governance and Financial Regulation, and other national publications and forums, and is a frequent speaker on securities law, corporate governance, and directors' and officers' liability insurance issues for the ALI-ABA, the New York State Bar Association, the American Conference Institute, NACD, and the Directors' Roundtable. Mr. Ferrillo also is a co-editor of and contributor to The 10b-5 Guide, Weil's annual review of securities fraud litigation in the United States. In 2015, Mr. Ferrillo published the widely acclaimed book "Navigating the Cybersecurity Storm: A Guide for Directors and Officers ("NCSS").

This book is provided "as is," with all faults, without warranties of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Paul.Ferrillo@weil.com | (212) 310-8372 Direct

K2 Intelligence

Investigations · Compliance Solutions · Cyber Defense

Securing the Right Outcome:

Our priority is to achieve what our client needs to achieve.

K2 Intelligence is redefining 21st-century corporate intelligence by combining deep subject-matter expertise with cutting-edge technology in an unprecedented way. We bring to bear the best multidisciplinary and multinational team in the business to solve our clients' most difficult problems.

- Investigations and Disputes
- Regulatory Compliance
- Cyber Defense
- Construction and Real Estate
- Strategic Risk and Security
- Private Client Services

K2intelligence.com

New York · London · Madrid · Tel Aviv · Geneva · Los Angeles

ABOUT DR. CHRISTOPHE VELTSOS

CHRIS – AKA DR.INFOSEC – is passionate about helping organizations take stock of their cyber risks and manage those risks across the intricate landscape of technology, business, and people.

Both faculty and practitioner, Chris understands the value of clear communication, the need to manage human assets and relationships, and the need to manage risks in the digital age. He has advised CEOs, has worked with CIOs, has shadowed and mentored CISOs, and interacted with a wide range of other business executives.

Chris enjoys working with business and security leaders to improve their organization's cyber risk posture. That means you might find him performing cybersecurity risk assessments, working alongside CIOs & CISOs to set and communicate strategic cybersecurity priorities, working with CEOs and CFOs to ensure risks are properly managed, or advising board directors on effective governance of cyber risks.

On campus, Chris works to educate and inspire the next generation of cybersecurity professionals attending Minnesota State University, Mankato. Off campus, he is a frequent speaker and author on all things cybersecurity and privacy related. He has presented at the regional and national level, including at major security conferences like RSA. He has written articles, book chapters, blog posts, and even a white paper. More recently, he's authored over 35 articles for IBM's SecurityIntelligence blog on topics ranging from traits of successful CISOs, questions board directors are asking, to the nature of conversations top leaders should have about cyber risks.

Email: chris@drinfosec.com
Blog: www.drinfosec.com
Twitter: @drinfosec
LinkedIn: Search for Chris Veltsos or drinfosec
Phone: +1 (507) 389-6560

PREFACE:

Many of you noted after reading our first edition, "Navigating the Cybersecurity Storm (NCSS)" that the allusion to the Avengers (my favorite Marvel comic book series) and to Captain America (my favorite comic book hero) was pretty apropos for both myself and the subject matter of the book, which dealt inherently with matters of cyber crime, cyber terrorism, and, ultimately, the national security and prosperity of the United States. Well, thank you for picking up on that. That was the point then, and it remains the point of our second edition of the book.

Our freedom, our individual liberties, our economic independence, and our national security are inextricably intertwined with the strength and security of our computer and cloud networks. We cannot have liberty and national security without network and cloud security. Our right to privacy is a strong part of this puzzle too, but without strong network and data security, privacy is almost irrelevant, and unobtainable at best. The events of the past 12 months have been truly historic. We have seen broad-based ransomware, spear phishing, point of sale ("POS"), and high-powered distributed denial of service ("DDoS") attacks, including the recent attack on Dyn, a DNS provider, that almost completely shut down Internet traffic on the U.S. East Coast for about 12 hours. We should also mention the continued economic and political espionage, especially as it relates to key elections taking place here at home and all around the world. Add to that the physical terrorist attacks in Paris, Brussels, Baghdad, Nice, San Bernardino, Chelsea and countless other places, one breach away from disaster is really not far from the truth.

What's different about Version 2 and why should you read it? Well, our cyber ecosystem has dramatically changed since November 2015, and you need to know how and why it's different. And you should read it because: (1) it's a lot better and very updated, (2) we stay true to our message and purpose throughout (short, concise, mission critical, and actionable information for directors, officers, general counsel, and C-Suite executives), and (3) Chris Veltsos. Let me take those in reverse order.

I asked Chris to join me on this year's mission. He and I met through the good folks at IBM. When not teaching cybersecurity concepts to the next generation of security professionals, he advises business leaders on how to best handle the risks associated with cyber. Initially trained to be deep in the security trenches, Chris knows the weaknesses inherent in machines and networks, but works to translate these issues in ways that are relevant to help management and directors make the best possible decision for their organization. Together we seek to elevate the discussion of cyber risks to a level of strategy and governance while informing readers about the key cyber issues of today and proven approaches for dealing with those issues. Chris is a good guy and very smart. He has kept a sharp eye on every facet of the book from the very beginning. His edits, comments, and substantive writing is always on the mark. He never misses the mark. Sort of like Hawkeye on the Avengers. I am lucky he accepted my proposal to work on Version 2. It's a better book because of him.

Why is Version 2 a lot better? Because we have now had another 12 months of wartime experience in defending and protecting computer on-premises and cloud networks. We have seen the enemy and the whites of their eyes. We also have 12 months more of technological innovation and have discovered more about how to defend networks better with fewer resources (which, as we describe in this book, is a huge

problem today in corporate America). We have completely re-written the cloud security chapter. Over the last 18 months the cloud has been broadly accepted today in corporate America for not only its security but its huge capacity to store data. That acceptance has created many challenges, which we discuss herein.

We have also added a brand new chapter on cybersecurity automation, orchestration, machine learning, deep learning, and artificial intelligence. We have the best scientists and programmers in the world in this country and many of the things they are doing is truly outstanding and cutting edge. Progress in this field has been exponential. Artificial intelligence and machine learning are and will continue to be national priorities. You need to know about these advanced aids to navigating the cybersecurity storm. Put them in play because they will help you find an attacker quicker than usual, lessening dwell time and giving the attacker less of a chance to devastate your network. This is especially needed given the crisis in corporate America due to the shortage of skilled cyber professionals. We simply don't have enough people to man the battle stations. We need help from machines. They won't replace us. They will augment our cyber intelligence, and make us truly Avengers!

We have also added two easy-to-read chapters on cyber risk. Why cyber risk? For the same reason you ask about the automobile crash ratings when you buy your next car: you can't assess risk unless you understand it. And you can't understand cyber risk without some sort of a logical framework or assessment questionnaire that can help a company soundly and decisively deal with its cyber risk. There is no 5-Star Crash Rating for cybersecurity (though maybe there needs to be). Cyber risks can't be dealt with by proxy, or by sticking one's head in the sand. Those have proven not to be good strategies. We CAN and WILL help you deal with and prioritize cyber risk, if you allow us this honor.

Finally, you will see several updated chapters from Version One. These chapters are like your favorite pair of running shoes. Comfortable. Easy to understand. Effective. We will talk again about the importance of things like the National Institute of Standards and Technology Cybersecurity Framework. We will also discuss regulatory cyber guidance and rules issued by the SEC, FFIEC, the Department of the Treasury and many other agencies. Cybersecurity today has been a national priority and our government and administrative agencies are treating it as such. We will lastly discuss important developments in cybersecurity insurance over the past year.

We want you to read this book and say, "Wow, I am really glad I read this book." Not because we want royalties. Not because we want you to buy something from us. Indeed, we want and need nothing other than a few hours of your time.

But we are very passionate about our work, and can assure of one thing. It will be several of the most important hours you have ever spent. Cybersecurity is and will remain a national priority for years to come. And a business priority for years to come.

It is a known fact that we are creating 2.5 quintillion bytes of data each day in our companies and businesses. For this reason, given the data we store and hold and use, data breach and theft losses run into the hundreds of billions of dollars each year, in addition to incalculable loss of intellectual property and capital. In one instance alone, the loss of plans to the F-35 fighter jet resulted in a catastrophic loss of time, effort, and, of course, billions of taxpayer dollars. And we have not even mentioned attacks on critical infrastructure. In this era, we simply cannot conduct

business like this anymore. In a speech this summer, James C. Trainor, Jr., former assistant FBI director for Cyber Operations, cited the U.S. Intelligence Community's annual Worldwide Threat Assessment, which for the last three years has ranked cyber threats as the No. 1 danger to national and economic security. Trainor said cyber is a "bigger [threat] than standard forms of espionage and bigger even than terrorism. From where I stand, the issue is getting worse by the day."[1]

Now, the final point. As events of the summer of 2016 are proving, we live in very dangerous times. Despite near-heroic efforts, our government (and other governments in the UK and EU) cannot fight cyber crime and terrorism alone. They need help. Our help. Now. And we need the government's help just as much. FBI Director James Comey recently re-emphasized the continuing urgent need for a public-private partnership this summer at Fordham Law School, when he noted:

> The majority of our private sector partners do not turn to law enforcement when there is a system breach. That is a big problem. It is fine when they turn to one of the excellent private companies that provide attribution or remediation, but we have to get to a place where it's routine for all of us to work together. For you to call us when there's an intrusion and not just a private sector enterprise.
>
> We understand that your primary concern in the private sector is to get back to business; to get back to where you were. By we, I mean not just the government, but we, all of us, need to figure out who's behind the attack. There may be on the surface a divergence of interest but our long-term interests are tightly aligned. Because if we don't find out who the actors are and impose costs on them, they will be back and they will victimize you and your industry again and again.[2]

Through threat intelligence sharing, Information Sharing and Analysis Center's and other threat sharing methods we all can band together as a group of like-minded business people and share cyber threat intelligence for the greater good. Sharing threat intelligence helps you in your security defense posture, and it can help others. We are seeing these partnerships take hold in certain industry verticals. We are seeing these partnerships in critical infrastructure. Cybersecurity is the ultimate team sport. We are all in this fight together. It is time to act, and there is no better time than right now. But rest assured, Chris and I will be right there with you in the foxhole, slugging it out with the bad guys till we cannot swing any longer.

We hope that you enjoy the book.

Paul and Chris
December 23, 2016

---

[1] See Speech of Former Assistant FBI Director James C. Trainor, which is available at http://news.fordham.edu/politics-and-society/presidential-directive-lays-out-government-response-to-cybersecurity-threats/.

[2] See Speech of FBI Director James B. Comey, dated July 27, 2016, which is available at https://www.fbi.gov/news/speeches/humility-adaptability-and-collaboration-the-way-forward-in-cyber-security.

TABLE OF CONTENTS

Paul Ferrillo is one of those rare writers who can guide the non-expert through the complex field of cyber security in a way that you can understand and trust. This is a valuable book.

— Jonathan Evans. Former head of MI5.

The cyber threat has never been more dynamic. And, securing the cyber infrastructure in the United States is one of the most formidable and complex challenges faced by our government and corporate America. "Take Back Control of Your Cybersecurity Now" addresses the most relevant cyber security topics in a clear, concise, and straightforward manner that will appeal to executives and managers who have a role in cybersecurity. It's a roadmap for doing all the right things to better secure your networks and information.

"Take Back Control of Your Cybersecurity Now" is informative, thought-provoking, and a great read!

It should be required reading for the entire C-Suite and Board of Directors.

— Don Good, former Deputy Assistant Director of the FBI's Cyber Division, and current Director, Navigant Consulting's Information Security Practice.

"Take Back Control of Your Cybersecurity Now" is a MUST-read for all board members, C-Suite leaders, CISOs and business owners, especially in banking, finance, retail, health care, who are responsible for personnel, customer, or patient data. Paul A. Ferrillo and Christophe Veltsos serve up an easy-to-read and digest primer on the prudent cybersecurity actions business leaders and owners should take to protect their company's and clients' data against countless cyber security threats. The authors improved on the first edition of this book by updating chapters with the newest cyber incidents and defensive methodologies as well as adding two chapters on cyber risk in order to help prioritize actions. This well -documented, authoritative cyber security instruction for business leaders has the potential save hundreds of millions of dollars for those fortunate enough to read and heed its sage advice. Do not miss the conclusion's 15 steps to improve your organization's cyber security posture. Read this book now and implement its recommendations as soon as possible.

— Colonel Roger Sangvic
U.S. Army Retired
Former Chief of Targets
US CYBERCOM

Paul Ferrillo and Chris Veltsos have written the definitive book for understanding the commercial, national security, and governance implications of cyber threats to the global digital economy. Their book is a compendium of insights, advice, and resources for those wanting to understand both technologies and policies shaping the rapidly evolving world of cybersecurity. As someone with a passion for emerging technologies and their exponential impact on society, I found the chapter on cybersecurity automation, orchestration, machine learning, deep learning and artificial intelligence to be particularly informative and illuminating. The authors state that "Cybersecurity is and will remain a national priority for years to come, and a business priority for years to come". There have already been 15 percent more data breaches in the first half of 2016, compared to the last six months of 2015 and that trend will likely continue. Indeed, as the authors note, we are all one hack away from disaster. Reading their book is an essential first step in helping prevent and mitigate that potential disaster.

— Charles (Chuck) Brooks
Vice President of Government Relations & Marketing for Sutherland Government Solutions
Chairman of the CompTIA New and Emerging Technologies Committee

"Take Back Control of Your Cybersecurity Now" is an engaging overview of the cyber security challenges facing companies and directors today. From regulation, to cloud security and incident response, Ferrillo and Veltsos cover significant ground—with a relevant look ahead toward how AI and machine learning can help solve some of these challenges. Any director or c-suite executive would benefit from understanding the concepts as presented here."

— Grady Summers – Chief Technology Officer, FireEye

"Take Back Control of Your Cybersecurity Now" is a book worth reading by anyone concerned about where we are today with cybersecurity and how to better protect yourself and your corporate entity. Paul A. Ferrillo and Christopher Veltsos lay out an easy to digest explanation of the issues of cyber-security and how to protect against the inevitable and in some case never-ending attacks against corporations today. No business is too small or too large to be attacked in some manner through their cyber network. Chapter one is alone worth the price of the book. In it, Ferrillo and Veltsos lay out the pitfalls of the cyber corporate environment, where are the threats coming from, and what are the threats. The book continues on with in-depth analysis of federal regulations and how to prevent attacks. Ferrillo and Veltsos go in to detail on how to respond to an attack, not only in a technical sense, but also as to a corporate response plan that includes crisis communication, dealing with law enforcement and regulators, and the relatively new field of cyber insurance. The C-Suite's would greatly benefit from reading "Take Back Control of Your Cybersecurity Now."

— Richard M. Frankel, Managing Director, USG Security Ltd; Special Agent In-Charge of the New York Criminal and Counterterrorism Divisions and Newark Field Office, Retired.

"Take Back Control of Your Cybersecurity Now" is a must-read for executives and cybersecurity experts alike. It serves as a practical guide on strategy and governance with current references to specific laws, regulations, and standards.

The authors are passionate about informing readers about the key cybersecurity challenges facing organizations today and how to address them as part of a larger team. Paul and Chris provide up-to-date advice on issues ranging from cyber insurance to cyber risk management talking points for board meetings. They also cover complex, but critical concepts like cloud computing and artificial intelligence. They do all of this while avoiding technical jargon that only techies would understand. It is a must-read.

— Jon Brickey, Ph.D., CISSP

Board members in 2016 continued to rate their level of knowledge around cybersecurity as "low" in survey after survey. Finally someone has written an easy-to-read book with the essentials every board member needs to understand. Ferrillo and Veltsos have eliminated the "techno-babble" I see so often, and describe critical risks that exist today as well as the future for protecting our organizations using advanced technology. Better yet, the authors provide suggested lines of inquiry we can use to frame insightful discussions with management in the board room. Directors need to have this book on their iPad or in their briefcase for ready reference … and not just on the bookshelf!

— Jay R. Taylor
CEO, EagleNext Advisors
Former General Director for Strategic Risk Management at a Fortune 20 Global Company"

Veltsos and Ferrillo have written THE cybersecurity book for Boards and C-Suite officers. Their cybersecurity expertise shows on every page, but it's their understanding of Board Governance and Oversight principles that sets this book apart. Cyber risks are real, and growing…but for the non-techie Director, it's been hard to gain needed insight without being overwhelmed by jargon and a management *focus. Until now!*

— Wayne Sadin, The Go Solution, Chief Digital Officer & Chief Information Officer, 2014 – Present, Data Kinetics, Advisory Board member, 2013 – Present

Paul Ferrillo might not have planned to come out with his second book so soon on the heels of his first, but the emergence of devastating new threats – particularly email hijacking and spear phishing – and important new solutions have prompted him to action. And that's a good thing for us. Now joined by Chris Veltsos, Ferrillo offers an easy-to-read, yet in-depth review of the most critical cybersecurity issues facing today's corporations. Business and technical people can both learn from this book. But Ferrillo and Veltsos don't just admire the problem. They offer practical solutions to address the threats and diminish the risks, as well as advice on how companies and boards can best position themselves to mitigate the fall out if – or should I say when – they are hacked, including how to demonstrate "due care" after-the-fact to regulators, investors, and the plaintiffs' bar. And for anyone who's looking for the evidence they need to secure greater resources to navigate their own cybersecurity storm, the authors do not disappoint. They provide the cold hard facts, statistics and dollar amounts, about cybersecurity threats and the impact they've had on affected enterprises. This update resource also contains new discussions on how Big Data analytics and Artificial Intelligence can supplement cybersecurity defenses and bridge the cybersecurity skills gap, questions to consider when moving to the Cloud, and the myriad of issues arising from the Internet of Things. There's also an increased focus and solid advice on information management business continuity planning, a crucial issue that's too often forgotten by modern enterprises, to their great detriment. At the very beginning of this book, the authors state that they want readers to say, "Wow, I am really glad I read this book." With confidence I submit, you will be.

— Judy Selby, Managing Director, BDO Seidman, Technology and Advisory

Will Rogers used to say that everybody talks about the weather but no one does anything about it. The same is true with cybersecurity. Except for rare visionaries like Paul Ferrillo and Chris Veltsos, we're so understandably focused on preventing attacks that we are ill-provisioned for dealing with the equally critical tasks of planning for the worst, managing the crisis once it happens, and having everything we need in place to ensure business continuity. Into this void Paul Ferrillo and Chris Veltsos has written an invaluable book; in fact, a necessary book. It's bedside reading for cybersecurity and crisis professionals – as well as the corporate officers and directors they serve.

— Richard S. Levick, Esq.
Chairman & CEO
LEVICK

Cyber threats are everywhere. It's not a question of "if" you'll be attacked, it's "when." Everyone has an obligation to be prepared. Paul Ferrillo and Chris Veltsos have created a comprehensive cyber readiness handbook. Every CEO should read it. Even if you think you're ready, you'll learn something new. In today's world, every organization and individual must have a plan to prevent, fight and recover from a cyber attack. This book is truly indispensable!

— Carla Lucchino, "Senior Executive (retired) Department of Defense"

Spot-on, timely, and the perfect desk book for the C-suite and business professionals! Written in plain, easy-to-understand language, Paul outlines and addresses the varying complex technical and regulatory cybersecurity issues faced today in all industries, providing expert guidance and best practices to protect business assets and effectively mitigate and recover from the inevitable cyber attack. Paul's book is required reading for all my students, and is an absolute must for all boards of directors!

— Kevin R. Powers, J.D.
Founding Director, Master of Science in Cybersecurity Policy and Governance
Boston College

Paul Ferrillo has performed the impossible: a jargon-free, objective, clear and practical guide for business and legal executives dealing with a cyber-security phenomenon that can be overwhelming in its technical and legal complexity. His new book brings the insight and actionable recommendations so sorely lacking in the existing literature on the topic. In a field that is overflowing with scare-tactics, marketing hyperbole and technical esoterica, Paul's book is a must-read for the business leader. It is direct and to the point, written in plain language that somehow manages to be entertaining and even amusing without disregarding the seriousness of the challenges business enterprises face; a pleasure to read!

— Adam Cohen CISSP CEH | Managing Director
Global Investigations + Strategic Intelligence
Berkeley Research Group, LLC

This book is an important contribution to cybersecurity thought leadership and is an excellent guide for everyone from business leaders with no cybersecurity experience to seasoned cybersecurity professionals. Its authors, both well-respected leaders in the cybersecurity space, have used their expertise to sift out the technical jargon and translate often complex cybersecurity issues into plain English in a well-written book that is easy for all to read and understand.

It is carefully organized and focuses on issues that have proven to be most important to companies in the real world, with entire chapters devoted such crucial issues as regulatory enforcement and spear phishing attacks—topics that usually are not adequately covered because they lack the sexy, exotic appeal of other more headline friendly cybersecurity topics that rarely have a practical impact on companies.

While the book is not stuffy or overly academic, it does provide deep strategic thinking by looking out over the horizon to where cybersecurity is evolving to and anticipating ways to leverage our resources to combat the cyber threat, such as through the use of artificial intelligence to exponentially improve the odds in our favor. Perhaps most importantly, the book provides practical advice and actionable solutions for business people to implement to better protect their companies and themselves from cyber risk and liability. It is an excellent book that I highly recommend everyone read because the reality is, cybersecurity now impacts each and every one of us and this book a valuable asset in the battle to protect our companies and ourselves.

— Shawn E. Tuma | Scheef & Stone, L.L.P.
Cybersecurity & Data Privacy Partner

Authors Paul A. Ferrillo and Christophe Veltsos have put together a must-read for anybody who is truly serious about their cyber and information security. "Take Back Control of Your Cybersecurity Now" lays out the critical issues industry faces today. In plain language and logical flow, this book not only identifies the challenges, but outlines a means to addresses the challenges in this ever-changing-you're-almost-certainly-going-to-be-a-victim-of-information-breach *reality we live in today. The book opens with honest and candid talk of the 2017 landscape, setting the contextual landscape and tempo required to understand what is going on around you. Walking through a series of realities – such as frameworks, laws, and responsibilities – and followed by the presentation of solutions – ranging from emerging technologies, policy development, and knowing what hard questions to ask – the authors will give the reader a set of tools that are useful to any staff, regardless of knowledge level, and organization, whether it is a small-to-mid size business or an enterprise. While designed as a book for executives, IT professionals and technologists should also give this book a read, as it will give them an understanding of the governors headspace. Learn to speak their language and understand what matters to them. Overwhelming executives with technical jargon will no longer cut it. Executives need a clear understanding of what the threats to the organization are and this book helps to get you in their headspace.* ***Spoiler Alert:*** *the conclusion mentions* "you cannot train enough"… *this is a great book to help up your cyber and information security game, whether you are every-day staff, the IT specialist, or a director.*

— George Platsis

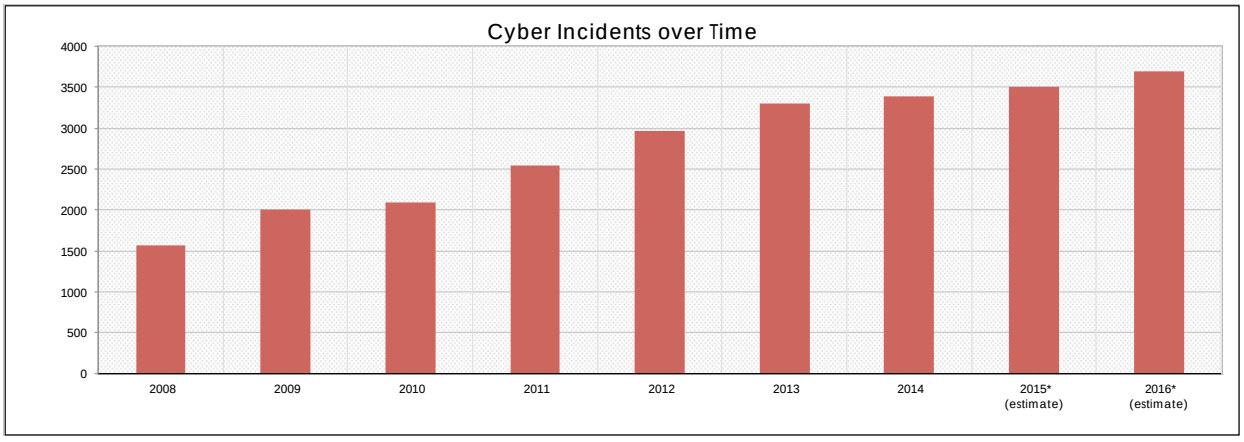
CHAPTER 1 :

TIME TO TAKE BACK CONTROL OF YOUR CYBERSECURITY NOW

PURPOSE OF THIS CHAPTER:

1. Offer a reality check about today's perilous cybersecurity environment.
2. Identify major threats to organizations of all sizes and in all industry sectors.
3. Outline the benefits of having top leadership and board directors highly engaged in managing or overseeing their organization's cybersecurity activities.
4. Introduce proven ways to help organizations take stock of their cybersecurity risks.
5. Outline this book's organization and the benefits to readers, no matter what their level of knowledge.

Hi. We are back. We had hoped to delay this update at least one more year, but that turned out not to be possible as, early on in 2016, the ransomware plague affected large swaths of corporate America and the healthcare system. And things have gotten uglier over the past few months.



Companies and organizations of great notoriety suffered cyber attacks, like the recent hacks of the Democratic National Committee ("DNC"),[1] the alleged hack on *The New York Times* by unknown sources, and very powerful distributed denial of service attacks against the website of famed blogger, Brian Krebs; a French media company called OVH; and a top-level domain name server company called Dyn.[2] There have been point of sale ("POS") hacks we definitely know about and hacks where we still don't really know the full story.[3] All these hacks and attacks make us wonder exactly how far we have come in the race for cybersecurity.

We continue to play "whack-a-mole" with cyber attackers. According to a headline summing up one expert's view, "cybercrime will cost the world in excess of $6 trillion annually by the year

2021."[4] This is up from 3 trillion in 2015. We can honestly say that while many organizations have made incremental (and, for some, major) progress, most have not. Many have done nothing helpful, refusing to admit they may be a target or maintaining that information security efforts are not in the budget. One step forward; two steps back.

And so we are back for a "pep talk," and to bring some solid good news on the advanced fronts of cybersecurity, especially as it relates to the future efforts involving artificial intelligence and machine learning.

As 2016 has shown, every organization, no matter the size or the industry it's in, is likely just a breach away from disaster.[5] This is due to many factors, including decades of relegating information security to "just an IT (Information Technology) issue." In the process, organizations and their leaders created an environment where technologists were in charge of making risk decisions, and business units — tired of being told, "No, you can't do this for security reasons!" — simply sought out ways to bypass the internal IT and security functions. Furthermore, budgets for IT, in most cases, never seem to comport to actual needs of the IT department to keep pace with the cybersecurity ecosystem in which we live.

The good news is this trend is now actively being remedied by elevating the importance and the voice of those who report on and manage cybersecurity. But these changes take time, time that your organization may not have.

While the purpose of this book isn't to spell out the doom-and-gloom of all possible disaster scenarios that may hit your organization, it is important for readers to be cognizant, if not convinced, of the reality of the situation, and the many threats organizations face in this cyber domain. So what other cyber issues contribute to the precarious state of cybersecurity? Here is a partial, non-exhaustive list:

- Your organization is facing a multitude of potential attackers whose motives are as varied as there are types of weeds. Some attackers might be after you to make a quick buck; some might be disgruntled employees or former employees looking to make a statement or take revenge for a perceived wrong;[6] some might be working for nation-states, looking to infiltrate your networks and steal sensitive email traffic or intellectual property,[7] or ruin decades of research; some might be looking to sabotage your systems because of what you stand for,[8] or because of how popular you've become. Possible motives are nearly endless, as is the patience of the most determined attackers who wait like a hunter for their prey to let down its guard.
- Your organization is a hodgepodge of technologies: some dating back decades, some adopted more recently, and both potentially insecure — either insecure right out of the box or due to the number of changes to their specifications or configuration.[9]
- Your organization is rapidly adopting new technologies — since failure to do so gives your competitors an edge — without properly addressing associated cyber risks in a systematic way and at appropriate levels. The advent of the Internet of Things ("IoT"), for example, means that even if your primary business function has nothing to do with technology, your organization has been or will soon be invaded by a multitude of IoT devices, including refrigerators, "smart" TVs, coffeemakers, air quality sensors, and light-control switches. Each of these devices could be the one an attacker uses to get in, or stay in, and commence an attack.[10]

- Your organization has likely suffered one or more episodes of ransomware — malware that takes over one or more of your systems, encrypts the data, and holds it for ransom. This is no laughing matter. It has happened to hospitals, police stations, schools, universities and even county government offices. In many cases, paying the ransom was the victim's only recourse for getting back their own data.[11]
- Your organization's cybersecurity function is likely understaffed, partly due to the tight labor market, top-of-the-scale salaries, and an abundance of opportunities for those willing to jump ship. It's also likely underfunded, especially if the security function in your organization is still housed under the IT umbrella. And it is probably under-represented and under-estimated, as only the more mature organizations have elevated the function of Chief Information Security Officer (CISO) to report directly to the CEO or in some cases to the Board of Directors directly.
- Your organization's staff is likely ill-informed and ill-prepared to deal with the onslaught of phishing attacks it is facing — attacks that exploit the human element in your organization. This issue isn't just limited to low-level staff. Executives, given their important role in the organization, are juicy targets for an attacker, a fact giving rise to the terms "whaling," which describes phishing attacks targeting the very top leadership, and "spear phishing campaigns," which target specific personnel with near-surgical precision — obviously requiring many hours of research about the targets. These attacks may be seeking personally identifiable information held by the organization spread ransomware on your network, or worse, steal secret plans to steal or IP that you don't want a third party to have access to.[12] Of course, your reply should be Security Awareness training, but how effective is that training? How often are you doing the training? Is there a metric that you are measuring, tracking, correlating with observations on the ground, and carefully improving upon every year, or are you like the thousands of businesses taking a one-size-fits-all approach to security awareness and requiring your employees to attend a mind-numbing, hour-long presentation or webcast?

Judging by the amount of news coverage of data breaches, attackers are quite resourceful, and obviously quite successful, regardless of their sophistication or age. The Dyn attack proved this point. But this isn't a book about data breaches. And there are so many data breaches that even data breach consultant or remediation websites get breached or attacked (or the people that operate them).[13]

You have likely heard the expression before: it's not a matter of IF; it's a matter of WHEN. Are you ready? Are you and your organization doing what you can to understand the risks to your continued success, and can you adequately handle those risks?

Some of you might still be thinking, "But who would want to attack ME? I don't have much of value to would-be attackers, do I?" Or the most common refrain: "Oh, I am not a target." The reality of who has been attacked over the past decade speaks for itself. Obviously major banks and financial institutions have been attacked, usually by attackers looking for a quick buck. The defense industrial base has been attacked, since it is rich with plans for the latest jet fighter, submarine, or next-gen weapons. The federal government has been attacked, including the Internal Revenue Service ("IRS") and the Office of Personnel Management ("OPM") in breaches that exposed millions of records of the people with some of the highest clearances. Critical infrastructure companies have been attacked,[14] and such attacks pose a grave threat to our very way of life and to the water, electricity, oil, and gas that power our nation. Stock markets have been attacked in attempts to disrupt our economic engine and the foundations of our way of life.

But beyond what most would consider juicy targets, thousands of other businesses in the U.S. and beyond have been attacked. Healthcare providers have been attacked, given the treasure-trove of data on their patients and the patrons who pay the bills. Movie companies and game-makers have been attacked, often because of what they stand for or how they go about their business. Universities and colleges have been attacked, as they can be a one-stop-shop for those looking to steal the identities of the bright minds that are our future generations. The hospitality industry has found itself in inhospitable waters with tens or hundreds of hotels, restaurants, and tour operators finding their systems and networks infiltrated with credit card skimming software. Retailers, from the mega-box-stores down to the mom-and-pop shops, have suffered from attacks against their networks and the Point-of-Sale (PoS) systems where our credit-cards go "chi-ching" with every purchase.

Is there hope? Yes, absolutely there is hope. Companies big and small are waking up and realizing at the very top levels that this is no longer an issue that can be relegated to the IT department. Cybersecurity risks represent major threats to your organization and as such require a high level of engagement by top leadership and board directors. There are very few other categories of risks that can, overnight, freeze your business dead in its tracks, decimate your financial resources, or even take it completely offline.

Our approach in putting together this book was to focus on the important stuff, but to do so in a way that presents the information in a clear, useful, timely manner. To this end, we organized the book in chapters that can be read on their own and out of order, to be as relevant to you as possible at the time you need it. You get the mission-critical information up front, and then we give you the tools and critical questions to help you improve your cybersecurity posture. To step it up a notch. To improve your handicap (excuse the pun).

The only way we get better at cybersecurity security is by working together and by exchanging ideas as a team. No one entity can fight this battle alone. FBI Director James Comey recently made this point over the summer, stating, "To finish, I don't know whether we can stay ahead of the cyber threat. I think talking about it that way actually shows hubris. We can hope to mitigate the threat, reduce the threat; send messages that change behavior. In the face of a threat unlike any we've seen before, we need enough humility to be agile; enough humility to take feedback from our partners to figure out how we can be better. We definitely need each other."[15]

Following this chapter is an overview of the ever-changing scene of federal regulations and oversight regarding cyber issues (Chapter 2) — the short answer is that the watchers are watching. The next chapter (Chapter 3) covers the benefits of tracking, reporting, and managing the big picture items when it comes to cyber, as well as leveraging security and risk frameworks — such as the Cyber-Security Framework ("CSF") from the National Institute for Standards and Technology ("NIST"). Chapter 4 touches on the human side of cybersecurity, as humans are involved in and drive all aspects of the business. Chapter 5 covers the key issue of incident response — being ready for cyber incidents and the importance of learning from our mistakes with every incident. Chapter 6 introduces new and promising developments in using machine learning and artificial intelligence capabilities to sift through the mountains of cyber network and incident related data and measurements from devices and sensors. Chapter 7 reminds top leadership of the cybersecurity fiduciary duties of directors and officers. Chapter 8 covers the benefits of cyber risk insurance, a burgeoning field with many insurers promising the moon — but when it comes to paying claims, well, that can be another story. Chapter 9 outlines ways that top leadership's involvement in the management and governance of cybersecurity activities benefits the organization. Chapter 10 presents several tough questions that management and the board need to be asking and having

critical discussions about. Chapter 11 covers the many benefits that moving to the cloud can provide your business. Finally, chapter 12 wraps things up, but not before reminding you of the key points of this book.

This is the end of this chapter, sort of. Those who know — or think they know — the hodgepodge of devastating cyber threats faced by their organization every day in 2016 can move on to the next chapter. Otherwise, we invite you to keep reading, because the digital cyber ecosystem is getting more complicated by the minute and we humans need all the help we can get.

> "If you can't get to some level of AI or machine learning with the volume of activity that you're trying to understand when you're [defending] networks from activity of concern, if you can't get to scale, **you are always behind the power curve** — it's got to be some combination of the two."[16] [emphasis supplied] —Admiral Mike Rogers

In the rest of this chapter, we talk about threat actors and criminals who have launched attacks against the U.S. over the past 18 months, as well as the vectors (i.e. the types of cyber-attacks they used to steal our stuff). This hopefully will give you some familiarity with terms you'll see in later chapters.

WHO ARE THE THREAT ACTORS?

> "We're moving into a new era here and frankly, we've got more capacity than anybody both offensively and defensively…. What we cannot do is have a situation where this becomes the wild, wild West, where countries that have significant cyber capacity start engaging in unhealthy competition or conflict through these means."
> — President Barack Obama, September 5, 2016 at the G20 Summit

> "Cybersecurity threats and vulnerabilities continue to be pressing concerns for companies and governments in the United States and around the world. In the U.S. financial system, cybersecurity remains an area of significant focus for both firms and the government sector. This attention is appropriate, as cybersecurity-related incidents create significant operational risk, impacting critical services in the financial system, and ultimately affecting financial stability and economic health." Annual Report of the Financial Stability Oversight Council, US Department of the Treasury[17]

> "[C]yber is one area we have to acknowledge that we have peer competitors with every bit as much capacity and capability as we do."
> — Admiral Mike Rogers, before the Senate Armed Services Committee, April 5, 2016

> "What worries me most is that ISIL's investment in social media — which has been blossoming in the last six to eight weeks in particular — will cause a significant increase in the number of incidents that we will see…. That's what I worry about all day long. "ISIL is changing [the] model entirely because ISIL is buzzing on your hip," he continued, referring to smartphones. "It's pushing its message 'all day long' on Twitter." Director of the FBI, James Comey, July 22, 2015[18]

Who are the main threat actors? First, despite vehement denials from its government, it appears — as per the comments of FBI Director Comey — that the Chinese, prior to the September 2015 agreement between the U.S. and China over the theft of intellectual property, had been the most industrious nation when it comes to cyber attacks, both in breadth and scope. As noted in the FireEye/Mandiant Trends Report, "Beyond the Breach" (hereinafter the "Mandiant Report"),[19]

"we've increasingly observed the Chinese government conduct expansive intrusion campaigns to obtain information to support state-owned enterprises. This translates into data theft that goes far beyond the core intellectual property of a company, to include information about how these businesses work and how key executives and key figures make decisions."

The Mandiant report further states that these intrusions have not just plundered agencies like the U.S. government Department of Defense, and weapons systems like the F-35 fighter jet,[20] but more importantly basic "how to conduct business" information in various industries. These persistent intrusions led to the U.S. government indictment of five officers of the Chinese People's Liberation Army on charges of cyber espionage. [21] To date, rumors persist that China may have had some involvement in both the Anthem breach and the OPM breach, though that has been heavily disputed.[22] The FBI released a study of 165 companies that reported a data breach by foreign sources. In 95% of those cases, the companies suspected China was to blame.[23] There is some evidence today that Chinese incursions into U.S. company computer networks has lessened. But it appears they are still very much in the game and have attacked other countries instead.[24]

In close second is the Russian government, which was rumored to have been involved in several recent attacks, including hacks on the White House, the DNC hacks mentioned earlier, the very recent attack on *The New York Times*,[25] and the hack of medical records of several U.S. Olympians and gold medalists who participated brilliantly at the 2016 Rio Summer Olympics.[26] These alleged attacks are no joke, and have attempted to reach into the depths of our government and the American political and election process.[27]

Next comes a variety of other nation-state actors, including North Korea,[28] Iran,[29] and Syria.[30] We have to add to the equation ISIS or ISIL, which has spent 2015 and 2016 planning attacks on the EU.[31] North Korea's defining moment as a nation-state hacker was attribution for the Sony wiper ware attack. At the time, one expert noted:

> The North Korean attack on Sony was absolutely a watershed moment for everybody. Because within hours, they saw Sony pull a movie, and the President was on TV talking about it. It was a major international incident. They didn't have to launch a bomb…all they had to do was [plant] malware. Emerging countries are probably going to see how this type of attack is effective….[32]

Excluding nation-state actors, public reports have revealed private actors (more commonly termed "cyber criminals") who have, most notoriously, devastated the U.S. retail sector with repeated attacks on retailers' point-of-sale (POS) systems using a variety of methods,[33] which will be explained below. Indeed, according to the most recent Ponemon Institute/IBM 2015 Cost of Data Breach Study[34] (hereinafter, the "Ponemon Report," which surveyed data breaches over calendar year 2014 in 11 countries), 47% of all data breaches surveyed stemmed from malicious or criminal attack. The average cost of a data breach due to malicious or criminal attacks increased to $170 per compromised record 2014 from $159 in 2013. In the United States alone, the cost per comprised record was $217.[35] Note that is the "per record" cost, and the total damages for some of the major breaches reported in 2014 could easily reach 8 or 9 figures.[36]

A key takeaway from these attacks is that it has sometimes taken companies up to five months to realize they have been breached.[37] And in many cases, the victims did not discover the breach on their own, but were informed by either a governmental authority (principally, the FBI or Secret Service) or a third-party (like a banking institution).[38] In a few cases, breaches were even first

reported by famous cyber investigative blogger and noted cyber security authority Brian Krebs.[39] This delay in discovering evidence of a breach (called in later chapters "indicators of compromise") is important for two reasons: it brings into question whether companies have the right tools, hardware and IT experience to recognize very sophisticated cyber-attacks, which may leave only "pieces" of the larger picture that have to be gathered quickly and correlated to uncover a potential breach; and, more obviously, the more time it takes to uncover a breach, (called in the business, "dwell time") the more damage an attacker can do or the more information he or she can steal. We discuss this problem later in the "Incident Response" and "AI/Machine Learning" chapters.

WHAT ARE THE THREAT VECTORS?

First, what is a "threat vector?" It is a path, or a tool, that a "threat actor" uses to get at a "target." In this chapter, the word "target" means a "target industry," but in reality a target is more than that. Targets "are anything of value to the threat actor," e.g., control of your server (and its secrets), your computer, your iPad, your social media accounts, your passwords, or your bank account.

Our favorite report that statistically documents global data breaches is the 2016 Verizon Data Breach Investigations Report,[40] (the "Verizon DBIR"), which reviews and summarizes a confirmed 2,260 data breaches (where there was disclosure or potential disclosure of confidential information) in 82 countries over the 2015 calendar year. The report does an excellent job pinpointing the exact type of threat vector used in any given cyber assault. It is not necessary to go into exhaustive detail on each type of threat vector identified in the Verizon DBIR (in fact many are way too complicated for the average director or officer to understand), but we think it's important to identify the trends involved since they correlate with the types of industries being attacked, as well as the governance and risk issues that we will explore in later chapters. Here are the top threat vectors and a short description of how they generally work:

1. Point-of-Sale ("POS") Intrusions:

These are the big cyber security breaches you read about almost every day in the newspaper or on your Twitter feed. The basic premise of a POS attack is to implant some variant of malware into a retailer's credit card processing system to collect credit card information via some sort of a "RAM" scraper at a POS terminal (like the card-swiping machine at your local department or food store). The credit card data (account numbers, expiration dates, and cardholder information) on the card's magnetic stripe is then collected via the malware-compromised server and sent (the technical term is "exfiltrated") outside the network to a third party. There have been many variants of malware used to accomplish this task, and many vectors used to deliver the malware, including spam, phishing, and now even botnets.[41] The malware has been difficult to find (sometimes taking months for a retailer to become aware it has suffered a breach). The results of POS attacks on retailers, hotels, and food-service restaurants this year have been particularly ugly.[42] Unfortunately, POS attacks are likely to continue in the near future.[43]

2. Web Application Attacks:

A web application attack is defined generally as when any web application is used as the vector for an attack. This one is a bit hard to explain. Generally the malicious actor will attempt to gain access to applications on a company's server through a variety of methods like phishing and

spear-phishing,[44] password and credential compromises, finding code vulnerabilities within certain popular network applications, or injecting code into an application to compromise the company's network. A recent study found 40% of all SQL injection attacks and 64% of all malicious HTTP traffic campaigns target retail websites. "Our study shows that retail sites are a big target for hackers. This is largely due to the data that retail websites store — customer names, addresses; credit card details — which cyber criminals can use and sell in the cybercrime underworld."[45]

3. Software Vulnerability or "Zero Day" Attacks

A zero day vulnerability (or a "Common Vulnerability Exposure" or "CVE") refers to a "hole" in software that is unknown to the vendor. Hackers then exploit this security hole to install malware on the subject server before the vendor becomes aware and hurries to fix it — this exploit is called a zero day attack. Exploits using software vulnerabilities can be extremely harmful if not caught early, and one linked to a Microsoft Windows vulnerability has been associated with high-profile attacks on critical infrastructure using the "Black Energy malware variant."[46] Nine zero day attacks have been discovered to date in 2016. Approximately 15 zero days in 2015 have been discovered so far.[47] The 2015 zero-day attacks to date were all discovered in popular Adobe and Microsoft products widely in use across private and professional IT systems."[48] Vulnerabilities are rated under a Common Vulnerability Scoring System ("CVSS"), which attempts to measure the potential severity of the vulnerability.[49]

Once discovered (very typically by a third party forensic analysis), a patch is issued by the software company to "fix" the vulnerability. The problem here is that some companies do not have the internal resources to implement the patch, or regimented patching schedules (indeed, ASAP patching for critical vulnerabilities), thus leaving them susceptible to attacks for days, months, or even years before being patched. Patching alerts and updates seem to occur now on an almost daily basis.[50] Unfortunately, many of the alerts for some reason or another are not timely remediated, allowing attackers even more time to successfully exploit the vulnerability.[51] Indeed, one recent study of software vulnerabilities stated:

> The analysis showed that over 15,000 (7.5%) of the open source components being consumed by these organizations in 2014 had known security vulnerabilities. Of those 15,000 components, an average of 66% (9,900) had known vulnerabilities dated 2013 or older. That means they were known vulnerable components ('bad') before they were downloaded.
>
> The remaining 34% (approx. 5,100) might have actually been 'good' components at the time they were downloaded by development teams from public open source repositories, but at some time during 2014 a new security vulnerability was discovered and a CVE identifier was assigned.[52]

The 2016 Verizon DBIR also reports some progress made in normalizing vulnerabilities, meaning we are fixing about the same number of vulnerabilities that have been reported in 2015 and 2014, many companies are still cannot get to all known and exploited vulnerabilities within a reasonable time. This is especially problematic for vulnerabilities known to be successful with attackers. They just reuse the good ones.

There are (at least) two points here: (1) threat intelligence is important. If you don't have time for everything, fix the known bad vulnerabilities (or the known bad ones within your industry vertical) before someone with ill intent gets to them first; and (2) prioritize patching efforts.

There are "have to have" patches, and "nice to have patches" that might affect your most critical systems. Patch the "have to have" vulnerabilities affecting your most critical systems first. Then get to the rest as soon as you can. We know that superhuman efforts might be required, but we know you'll try your best.

4. Cyber-Espionage Attacks:[53]

These are what the category indicates: blatant, yet highly disguised and nearly undetectable methods used by nation states and third party actors to steal valuable information. Methods include: injection of malware, phishing, malvertising,[54] watering hole attacks,[55] spear phishing, finding network and software vulnerabilities,[56] creating backdoors to exfiltrate information, and simply by brute force attacks. Even the notorious wiperware malware called "Shamoon" has recently been used against Saudi Arabian government agencies and companies. The methods vary from actor to actor, many are "zero day" or "APT" or "advanced persistent threat" attacks.

5. Card Skimmers:

Card skimmers are a little different from retail POS attacks in that they generally involve some device installed, for instance on an ATM or gas pump, to skim credit card data and send it to a third party. The types of card skimmers vary. They are generally very hard to detect.[57]

6. Misuse of Passwords and Privileges — One Phish, Two Phish, Red Phish, Blue Phish:

Insider misuse of IDs and passwords is relatively simple to explain. One of your employees uses his ID, password, or network privileges to gain information he either has access to, or should not have access to but does because of "over-privileging," and then uses it or sells it for his own financial gain.[58] The malicious use of passwords and privileges often happens with a third party involved, like a former employee, cybercriminal, or competitor who somehow gains access to your network through a phishing or spear phishing attack and steals information for his gain, and your loss.[59]

Because of the vast amount of information available on the Internet, phishing and spear phishing attacks have taken great prominence in the US cyber ecosystem, and they have become the primary threat vector facing U.S. companies. Eighty-four percent of organizations said a spear phishing attack successfully penetrated their organization in 2015.[60] The 2016 Verizon DBIR notes, somewhat sarcastically, "Thirty percent of phishing messages were opened by the target across all campaigns. "But wait, there's more!" (in our best infomercial voice) About 12% went on to click the malicious attachment or link and thus enabled the attack to succeed. *That indicates a significant rise from last year's report in the number of folks who opened the email (23% in the 2014 dataset).*[61] [emphasis added]. The attachment or links may lead to the seeding of malware on the recipient's computer or even ransomware, like CryptoLocker or Cryptowall.[62] "The average impact of a successful spear phishing attack: $1.6 million. Victims saw their stock prices drop 15%."[63] Socially-engineered spear phishing attacks continue to present a tremendous problem. We discuss spear phishing mitigation and employee training tactics in later chapters.

7. Wiperware Attacks:

We mention one more type of attack that has surfaced more recently: "wiper" malware. Wiper malware is "designed to erase data from PC and file-server hard drives and delete the master boot record, so the machines cannot boot."[64] Simply put, wiper malware can wipe away all the data on multiple servers infected at a target company. In two recent cases, called "Shamoon" and

"Dark Seoul," over 30,000 servers were essentially deleted.[65] Apparently, a variant of Shamoon called "Destover" attacked the servers at Sony Pictures. "Destover, and the like, are much more dangerous in that they overwrite the master boot record on a computer, not only rendering the computer useless after robbing it blind, but also leaving few bread crumbs for investigators to follow."[66] Another variant of wiper malware was apparently used to attack the Las Vegas Sands in February 2014, rendering thousands of servers useless. [67]

8. Distributed Denial of Service ("DDoS") Attacks:

A final method hackers have used to wreak havoc on U.S. and UK companies and financial institutions is the DDoS attack. Over the last several months these attacks have become more prevalent, more powerful, more dangerous, and more thought-provoking.

In a DDoS attack, a hacker, through the use of massive botnets,[68] creates an "army of computers" that then attack a particular website, with a typical bandwidth and a typical duration. Botnets, a very typical threat vector in the financial services and retail spaces, can tie up a computer network for hours (and sometimes days), throwing the company offline and frustrating users and customers. Many financial institutions were attacked in 2015 and 2016.[69] Brian Krebs and OVH were attacked with DDoS botnet attacks of epic proportions called "Mirai" in September 2016, displaying the potential vulnerabilities caused by IoT devices.[70] These attacks were extremely powerful — double the size of previously recorded DDoS attacks (quadruple the size in OVH's case). Then on October 24, 2016, lightning struck again. A lot of lightening. A major attack struck the domain name server company Dyn, purportedly commenced by hundreds of thousands of IoT enabled devices — like Internet enabled cameras and DVRs — that flooded Dyn's servers at three different times during the day. The largest attack registered at about 1,200 gigabytes. These attacks were powerful and Dyn understandably could not handle the tremendous volume of Internet traffic. The attacks not only took down Dyn, but companies that relied upon Dyn for their domain name services (like customer traffic aimed at websites such as Twitter.com). In total, about 70 companies in the U.S. lost Internet connectivity. Imagine no Twitter feed for one day! The Dyn attack is a game changer. Unfortunately, these Mirai-inspired botnet attacks continue today.

The most famous botnet attack of 2014 was the "Grinch-like" attack by the Lizard Squad on the Sony and Microsoft gaming networks on Christmas Day, knocking users offline for hours.[71] Other DDoS attacks have targeted financial institutions.[72] One very large scale DDoS attack was recently launched against the Rio Olympics' online presence (which televised the Olympics on a streaming basis).[73] Indeed, the Lizard Squad has been very active, taking down the UK National Crime Authority website for a period of time with a DDoS attack.[74] A recent report issued by cyber security company Akamai noted that:

> For the past three quarters, there has been a doubling in the number of DDoS attacks year over year. And while attackers favored less powerful but longer duration attacks this quarter, the number of dangerous mega attacks continues to increase. In Q2 2015, there were 12 attacks peaking at more than 100 Gigabits per second (Gbps) and five attacks peaking at more than 50 Million packets per second (Mpps). Very few organizations have the capacity to withstand such attacks on their own.
>
> The largest DDoS attack of Q2 2015 measured more than 240 gigabits per second and persisted for more than 13 hours. Peak bandwidth is typically constrained to a one to two hour window. Q2 2015 also saw one of the highest packet rate attacks ever recorded across

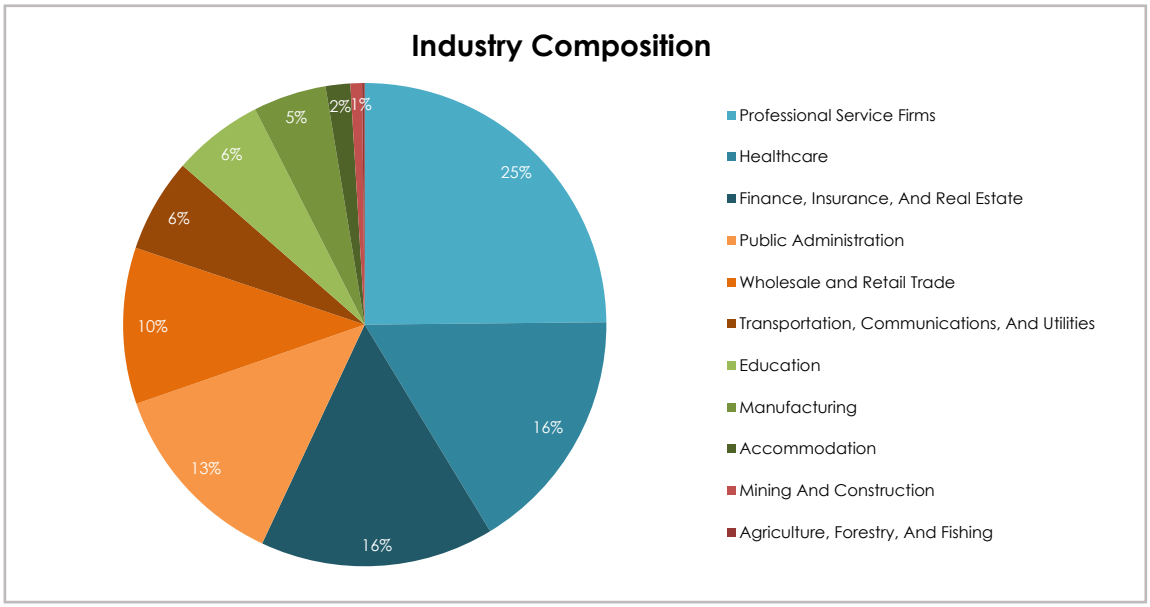
the Prolexic Routed network, which peaked at 214 Mpps. That attack volume is capable of taking out tier 1 routers, such as those used by Internet Service Providers (ISPs). The strength of attacks increased throughout 2016, with the largest attacks being registered in the fourth quarter.[75]

One final variant on the DDoS attack is the "smokescreen DDoS" attack: while the company is taking steps to mitigate the DDoS attack, hackers strike with another piece of malware aimed at stealing data. A recent article noted:

> In many cases, it may be a coordinated effort, but even if these attacks originate from different sources, IT staff have to allocate resources to solve two problems at the same time, under a lot of stress.

While many attackers do use DDoS as a smokescreen to hide data stealing or network damaging attempts, it's difficult to attribute them. For sure…. But even if they are unrelated, the fact that they arrive simultaneously — even by chance — a high percentage of the time means security staff should make sure their DDoS-mitigation plan includes resources to look for other incursions."[76]

WHO ARE THE TARGETS OF THE CYBER ATTACKS?



The Verizon DBIR gives a very good summary of the industry segments most affected by cyber incidents and data breaches in calendar year 2015. Setting aside the number of cyber breaches affecting the public sector (like federal and state governments), here are the industry segments suffering the highest number of security incidents with confirmed data losses:

1. **FINANCE** — No surprise here. Financial organizations hold high value personal and business information and high proprietary trading data, algorithms, and M&A data. These organizations faced cyber threats from both malicious insiders and third parties.[77]

2. **RETAIL** — Also no surprise given the prevalence of POS attacks. Retailers hold high value personal information and credit card data, as we saw in the Target and Neiman Marcus breaches.

3. **ACCOMMODATION (HOTELS, MOTELS)** — Similar to retail, these businesses hold high value personal information and credit card data.[78]

5. **PROFESSIONAL SERVICE FIRMS (LIKE LAW FIRMS, ACCOUNTING FIRMS, AND CONSULTANTS)** — Perceived to be "soft targets" not necessarily concerned about cyber-attacks, but an industry segment that typically stores a high volume of both intellectual property and confidential business data of its clients.

6. **HEALTHCARE** — No surprise, as healthcare organizations hold high value personal information. Well known breaches include Anthem, Premera, Carefirst, UCLA Healthcare System, Excellus Healthcare, and Banner Healthcare.[79] There were also an untold number of ransomware attacks against hospital and healthcare organizations in 2016.

7. **EDUCATIONAL INSTITUTIONS** — Hackers have recently mined data at institutions such as Harvard, Penn State, the University of Virginia, University of Georgia, Michigan State University and Rutgers University.[80]

Well, enough of the good news. As we noted above, cybersecurity breaches affect everyone. Governments (state and federal), public companies, private companies, healthcare institutions — everyone. And the threats grow every day. The question is, "So what are you going to do about it?"

The answers to that deceptively simple question will be found throughout the chapters in this book, through insurance and advanced technical solutions, through better communication and better security investments, and through the integration of cybersecurity into the organization's overall risk management. A "failure to communicate" is no longer a tolerable excuse. It is time for action.

ENDNOTES:

[1]See "DNC breach was likely Russia, not 400-pound hacker, law enforcement says," available at http://www.cnbc.com/2016/09/27/dnc-breach-was-likely-russia-not-400-pound-hacker-law-enforcement-says.html.

[2]See "How Hacked Cameras Are Helping Launch The Biggest Attacks The Internet Has Ever Seen," available at http://www.forbes.com/sites/thomasbrewster/2016/09/25/brian-krebs-overwatch-ovh-smashed-by-largest-ddos-attacks-ever/#52a6f29e6fb6; "Amateurs were behind the Dyn Inc. DDoS attack, report says," available at http://www.csoonline.com/article/3134721/security/amateurs-were-behind-the-dyn-inc-ddos-attack-report-says.html.

[3]See e.g. "Vera Bradley says payment system hacked, sales could be affected," available at http://www.cnbc.com/2016/10/12/vera-bradley-says-payment-system-hacked-sales-could-be-affected.html.

[4]See "Hackerpocalypse: A Cybercrime Revelation," available at http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[5]See "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating," available at http://www.latimes.com/business/technology/.

[6]See "Sage Employee Arrested for Insider Breach," available at http://www.esecurityplanet.com/network-security/sage-employee-arrested-for-insider-breach.html; "The Biggest Cybersecurity Threats Are Inside Your Company," available at https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company (noting "In the 2016 Cyber Security Intelligence Index, IBM found that 60% of all attacks were carried out by insiders.).

[7]See e.g. "Putin denies that Russia hacked the DNC but says it was for the public good," availa-ble at https://www.washingtonpost.com/world/putin-denies-that-russia-hacked-the-dnc-but-says-it-was-for-the-public-good/2016/09/02/d507a335-baa8-40e1-9805-dfda5d354692_story.html.

[8]See "ISIL aims to launch cyberattacks on U.S.," available at http://www.politico.com/story/2015/12/isil-terrorism-cyber-attacks-217179.

[9]See e.g. "Research Finds Malware In 75% Of The Top 20 Banks In The U.S," available at http://virusguides.com/research-finds-malware-75-top-20-banks-u-s/ ("As banks continue to grow through acquisition, legacy IT systems and their vulnerabilities are also acquired. In many cases, they remain in place for years. Despite major financial institutions spending billions of dollars on cybersecurity annually, this report suggests the financial industry may not be spending those dollars as effectively as possible. A greater level of protection is required, which should be a concern for their customers and partners").

[10]See "The Internet of Things: A "National Treasure," or a Worldwide Problem of Epic Propor-tions?" available at http://levick.com/blog/public-affairs/the-internet-of-things/; "The Dyn report: What we know so far about the world's biggest DDoS attack," available at http://www.zdnet.com/article/the-dyn-report-what-we-know-so-far-about-the-worlds-biggest-ddos-attack/.

[11]See e.g. "How Bitcoin helped fuel an explosion in ransomware attacks," available at http://www.zdnet.com/article/how-bitcoin-helped-fuel-an-explosion-in-ransomware-attacks/.

[12]See "Russian government hackers penetrated DNC, stole opposition research on Trump," available at https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html. (It is suspected that the hack "may have targeted DNC employ-ees with "spear phishing" emails. These are communications that appear legitimate — often made to look like they came from a colleague or someone trusted — but that contain links or at-tachments that when clicked on deploy malicious software that enables a hacker to gain access to a computer.")

[13]See "Hackers Target Anti-DDoS Firm Staminus," available at http://krebsonsecurity.com/tag/ddos/; "Massive Email Bombs Target .Gov Addresses," available at http://krebsonsecurity.com/ (describe a personal DDoS attack upon the mailbox of noted Cy-bersecurity intelligence gatherer and blogger, Brian Krebs).

[14]See "U.S. official blames Russia for power grid attack in Ukraine," available at http://www.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/; see also "FERC Takes Action on Cybersecurity in Response to Ukrainian Cyber Attacks," available at http://www.jdsupra.com/legalnews/ferc-takes-action-on-cybersecurity-in-87475/ (describing the Federal Energy Regulatory Commission's proposed response to the Ukrainian grid attack for US electric companies).

[15]See Speech by James B. Comey, Director, Federal Bureau of Investigation, Symantec Gov-ernment Symposium, Washington, D.C., August 30, 2016, available at https://www.fbi.gov/news/speeches/the-fbis-approach-to-the-cyber-threat.

[16]Testimony of Admiral Michael Rogers, head of both US Cybercommand and the National Se-curity Agency before the Senate Armed Services Committee, dated September 13, 2016, availa-ble at http://www.executivegov.com/2016/09/adm-michael-rogers-ai-human-analytics-integration-can-aid-natl-security-programs/.

[17]See "2016 Financial Stability Oversight Council Report," available at https://www.treasury.gov/initiatives/fsoc/studies-reports/Pages/2016-Annual-Report.aspx.

[18]See "ISIL Keeps FBI Director Awake At Night," available at http://www.refinery29.com/2015/07/91202/james-comey-isis-biggest-fears.

[19]See "FireEye Releases Annual Mandiant Threat Report on Advanced Targeted Attacks," found at http://www.fireeye.com/news-events/press-releases/read/fireeye-releases-annual-mandiant-threat-report-on-advanced-targeted-attacks.

[20]See "Theft of F-35 design data is helping U.S. adversaries –Pentagon," found at http://www.reuters.com/article/2013/06/19/usa-fighter-hacking-idUSL2N0EV0T320130619; "Chinese Hacked U.S. Military Contractors, Senate Panel Says," available at http://www.wsj.com/articles/chinese-hacked-u-s-military-contractors-senate-panel-says-1410968094.

[21]See "Attorney General Eric Holder Speaks at the Press Conference Announcing U.S. Charges Against Five Chinese Military Hackers for Cyber Espionage," available at http://www.justice.gov/opa/speech/attorney-general-eric-holder-speaks-press-conference-announcing-us-charges-against-five.

[22]See "Nation-State Cyber Espionage, Targeted Attacks Becoming Global Norm," available at http://www.darkreading.com/attacks-breaches/nation-state-cyber-espionage-targeted-attacks-becoming-global-norm/d/d-id/1319025.

[23]See "FBI Probes 'Hundreds' of China Spy Cases," available at http://www.thedailybeast.com/articles/2015/07/23/fbi-probes-hundreds-of-china-spy-cases.html (one FBI official recently noted that "The predominant threat we face right now is from China,").

[24]See "Russia More Prey Than Predator to Cyber Firm Wary of China," available at http://www.bloomberg.com/news/articles/2016-08-25/russia-more-prey-than-predator-to-cyber-firm-wary-of-china.

[25]See "First on CNN: FBI investigating Russian hack of New York Times reporters, others," available at http://www.cnn.com/2016/08/23/politics/russia-hack-new-york-times-fbi/.

[26]See "Cyber 'Smear': Hackers Publish Olympians' Medical Records," available at http://abcnews.go.com/International/anti-doping-agency-russian-hackers-published-athletes-medical/story?id=42063565.

[27]See "Obama administration accuses Russian government of election-year hacking, available at: http://www.politico.com/story/2016/10/obama-administration-accuses-russian-government-of-election-year-hacking-229296#ixzz4OCdWBp8y.

[28]See "Update on Sony Investigation," available at http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation; "FBI: North Korea to Blame for Sony Hack," available at http://krebsonsecurity.com/2014/12/fbi-north-korea-to-blame-for-sony-hack/.

[29]See "Now at the Sands Casino: An Iranian Hacker in Every Server," available at http://www.businessweek.com/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas; "Iran hackers targeted airlines, energy firms: report," available at http://www.reuters.com/article/2014/12/02/us-cybersecurity-iran-idUSKCN0JG18I20141202; "Iran-Linked Espionage Group Continues Attacks on Middle East," available at http://www.securityweek.com/iran-linked-espionage-group-continues-attacks-middle-east; "U.S. charges Iranians for cyberattacks on banks, dam," available at http://www.cnn.com/2016/03/23/politics/iran-hackers-cyber-new-york-dam/.

[30]See "Syrian Electronic Army Claims to Have Hacked U.S. Army Website," available at http://www.newsweek.com/syrian-electronic-army-claims-have-hacked-us-army-website-340874.

[31]See "Cyberterrorist Attacks Unsophisticated but Effective: Former FBI Agent," available at http://www.securityweek.com/cyberterrorist-attacks-unsophisticated-effective-former-fbi-agent; "Isil plotting deadly cyber-attacks against Britain, George Osborne warns," available at http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11999607/islamic-state-cyber-attack-plot-britain-george-osborne-warns.html.

[32]See "Nation-State Cyber Espionage, Targeted Attacks Becoming Global Norm," available at http://www.darkreading.com/attacks-breaches/nation-state-cyber-espionage-targeted-attacks-becoming-global-norm/d/d-id/1319025.

[33]See e.g., "Berkshire-owned Dairy Queen says customer data hacked in 46 states," found at http://www.reuters.com/article/2014/10/10/us-usa-dairy-queen-cybersecurity-idUSKCN0HZ1TM20141010; "Target Now Says 70 Million People Hit in Data Breach,' availa-ble at http://www.wsj.com/articles/SB10001424052702303754404579312232546392464.

[34]See "2014 Cost of Data Breach Study: Global Analysis," available at http://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf.

[35]See 2013 Ponemon Cost of Breach Report Study, found at https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

[36]See "Target's data breach fraud cost could top $1 billion, analyst says," available at http://www.bizjournals.com/charlotte/news/2014/02/03/targets-data-breach-fraud-cost-could-top-1-billion.html. The cost of replacing the compromised credit cards could alone total $400 million or more. See "Banks' Lawsuits Against Target for Losses Related to Hacking Can Continue," available at http://bits.blogs.nytimes.com/2014/12/04/banks-lawsuits-against-target-for-losses-related-to-hacking-can-continue/?_r=0.

[37]See "2016 FireEye M-Trends Report, available at https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf (noting that according to Mandiant, in 2015 it took companies an average of 146 days to detect a breach.

[38]Id. The Mandiant report further reports that only 31% of companies were able to discover breaches on their own.

[39]See "Dairy Queen Confirms Breach at 395 Stores," available at http://krebsonsecurity.com/2014/10/dairy-queen-confirms-breach-at-395-stores/.

[40]Available at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

[41]See "New point-of-sale malware distributed by Andromeda botnet," available at http://www.cio.com/article/2949334/new-point-tofsale-malware-distributed-by-andromeda-botnet.html.

[42]See e.g. "Credit Card Breach Hits All Eddie Bauer Stores in U.S., Canada," available at http://www.esecurityplanet.com/network-security/credit-card-breach-hits-all-eddie-bauer-stores-in-u.s.-canada.html.

[43]Id. ("What's more, these ongoing attacks against retailers, hoteliers and food chains indicate that it's likely that there are many more businesses that leverage PoS systems that have been at-tacked but don't yet know it because of a lack of insight into their risk and security posture").

[44]See "Anatomy of an Attack: From Spear phishing Attack to Compromise in Ten Steps," found at https://www.mandiant.com/threat-landscape/anatomy-of-an-attack/.

[45]See "Nearly half of all web application cyber attacks target retailers, study shows," found at http://www.computerweekly.com/news/2240235253/Nearly-half-of-all-web-application-cyber-attacks-target-retailers-study-shows.

[46]See "BlackEnergy Malware Plug-Ins Leave Trail of Destruction," https://threatpost.com/blackenergy-malware-plug-ins-leave-trail-of-destruction/109126#sthash.2zz6Trah.dpuf; see also "Sandworm APT Team Found Using Win-dows Zero Day Vulnerability," https://threatpost.com/sandworm-apt-team-found-using-windows-zero-day-vulnerability/108815#sthash.n3Mr8nBo.dpuf.

[47]See "Recent Zero-Day Exploits," available at https://www.fireeye.com/current-threats/recent-zero-day-attacks.html.

[48]See "Vulnerabilities in 2015: 0-days, Android vs iOS, OpenSSL," available at http://www.net-security.org/secworld.php?id=18732.

[49]See "Common Vulnerability Scoring System, V3 Development Update," available at https://www.first.org/cvss.

[50]See "Setting priorities with July's huge Patch Tuesday," available at http://www.computerworld.com/article/2947756/application-security/huge-july-patch-update-with-critical-update-to-ie-and-windows.html.

[51]See "Sixty Percent of Enterprise Application Vulnerabilities Go Unmitigated," available at http://darkmatters.norsecorp.com/2015/07/13/sixty-percent-of-enterprise-application-vulnerabilities-go-unmitigated\ (noting that many organizations take three to six months to re-mediate a known vulnerability).

[52]See "When Good Code Goes Bad," available at http://www.infosecurity-magazine.com/blogs/when-good-code-goes-bad/.

[53]In this section, we have not used the acronym "APT" or "advanced persistent threat" for a reason. An APT is not a per se "vector." It is a type of actor (very often nation-state sponsored) that makes a concerted effort to dig deep into a Company's network to collect sensitive infor-mation about a person, place, or secret (like the plans to the F-35 Fighter Jet) by silently moving laterally through a Company's network. See "Catch Me If You Can: How APT Actors Are Moving through Your Environment Unnoticed," available at http://blog.trendmicro.com/catch-me-if-you-can-how-apt-actors-are-moving-through-your-environment-unnoticed/?utm_source=twitterfeed&utm_medium=twitter&utm_campaign=information_security.

[54]See "Yahoo Malvertising Attack Points To More Flash Problems," available at http://www.informationweek.com/software/enterprise-applications/yahoo-malvertising-attack-points-to-more-flash-problems/a/d-id/1321626; See also "Cyphort Labs Issues Special Report on the Rise in Malvertising Cyber Attacks," available at http://www.darkreading.com/attacks-breaches/cyphort-labs-issues-special-report-on-the-rise-in-malvertising-cyber-attacks/d/d-id/1321902 (noting that "Cyphort researchers found that malvertising campaigns carried out by hackers increased 325 percent in the past year.").

[55]See "BlackHat 2015: 2FA key to defense against cyber espionage groups," available at http://www.computerweekly.com/news/4500251145/BlackHat-2015-2FA-key-to-defence-against-cyber-espionage-groups.

[56]See "Symantec uncovers Morpho cyber espionage operation," available at http://www.computerweekly.com/news/4500249597/Symantec-uncovers-Morpho-cyber-espionage-operation.

[57]See, e.g., "Skimmer Innovation: "Wiretapping ATMs," found at http://krebsonsecurity.com/.

[58]A very recent study of IT decision makers reported that only 68% of the companies surveyed felt that their company was making an adequate investment in technology designed to monitor activities of users with elevated or privileged access rights. See "2015 Cyberthreat Defense Report, North America and Europe," available at http://www.brightcloud.com/pdf/cyberedge-2015-cdr-report.pdf.

[59]See e.g., "JP Morgan Found Hackers through Breach of Corporate Event Website," found at http://www.moneynews.com/Companies/JP-Morgan-Hackers-Breach-Website/2014/11/02/id/604663/.

[60]See "Spearphishing Attacks," available at https://www2.fireeye.com/rs/fireye/images/fireeye-how-stop-spearphishing.pdf.

[61]See 2016 Verizon DBIR

[62]See "IBM X-Force Threat Intelligence Quarterly, 3Q 2015," available at https://www-01.ibm.com/marketing/iwm/dre/signup?source=swg-WW_Security_Organic&S_PKG=ov38487&S_TACT=C41303YW&dynform=20131. "Ran-somware continues to grow very rapidly – with the number of new ransomware samples rising 58 percent in Q2." See "Ransomware jumps 127%, IoT malware on rise too: McAfee," availa-ble at http://www.firstpost.com/business/ransomware-jumps-127-iot-malware-on-rise-too-mcafee-2419582.html. The rise in ransomware activity led the FBI to issue a very good alert in January 2015 on how to avoid potential harm from a ransomware attack. See "Ransomware on the Rise: FBI and Partners Working to Combat This Cyber Threat," available at https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise.

[63]See "Spearphishing Attacks," available at https://www2.fireeye.com/rs/fireye/images/fireeye-how-stop-spearphishing.pdf.

[64]See "Sony Hack: Ties to Past 'Wiper' Attacks?" available at http://www.bankinfosecurity.com/sony-hack-ties-to-past-wiper-attacks-a-7644/op-1.

[65]Id.

[66]See "Details Emerge on Sony Wiper Malware," available at http://threatpost.com/details-emerge-on-sony-wiper-malware-destover/109727.

[67]See "Las Vegas Sands' network hit by destructive malware in Feb: Bloomberg," available at http://www.reuters.com/article/2014/12/12/us-lasvegassands-cybersecurity-idUSKBN0JQ04520141212.

[68]A "bot" is "a type of malware that allows an attacker to take control over an affected comput-er. Also known as "Web robots", bots are usually part of a network of infected machines, known as a "botnet", which is typically made up of victim machines that stretch across the globe" in-fecting thousands, if not hundreds of thousands of computers. See "Bots and Botnets—A Grow-ing Threat," available at http://us.norton.com/botnet/.

[69]See "Britain's HSBC Recovers from Massive DDoS Attack," available at http://www.securityweek.com/britains-hsbc-recovers-massive-ddos-attack.

[70]See "Krebs dropped by Akamai for record DDoS attack, OVH suffers 1100 Gbps DdoS," available at http://www.scmagazineuk.com/krebs-dropped-by-akamai-for-record-ddos-attack-ovh-suffers-1100-gbps-ddos/article/524556/.

[71]See "Lizard Stresser Runs on Hacked Home Routers," available at http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/.

[72]See "Cyber attack hits RBS and NatWest online customers on payday," available at http://www.theguardian.com/business/2015/jul/31/rbs-and-natwest-customers-complain-of-online-problems.

[73]See "How a Massive 540 Gb/sec DDoS Attack Failed to Spoil the Rio Olympics," available at http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/how-a-massive-540-gbsec-ddos-attack-failed-to-spoil-the-rio-olympics/#.V8m-xswwSDY.twitter.

[74]See "Stressed out: Lizard Squad takes down UK law enforcement website in latest DDoS at-tack," available at http://siliconangle.com/blog/2015/09/02/stressed-out-lizard-squad-takes-down-uk-law-enforcement-website-in-latest-ddos/.

[75]See "Akamai Releases Q2 2015 State of the Internet - Security Report," available at http://prwire.com.au/pr/53743/akamai-releases-q2-2015-state-of-the-internet-security-report.

[76]See "Under DDoS attack? Look for something worse," available at http://www.networkworld.com/article/2984648/security/under-ddos-attack-look-for-something-worse.html.

[77]See "Corporate Espionage Risk Management For Financial Institutions," available at http://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/corporate-espionage-risk-management-for-financial-institutions/; "The Damage of a Security Breach: Financial Institutions Face Monetary, Reputational Losses," available at https://securityintelligence.com/the-damage-of-a-security-breach-financial-institutions-face-monetary-reputational-losses/ (nothing that more than 500 million records have been stolen from financial institutions over the past 12 months as a result of cyberattacks.").

[78]See "Donald Trump's Hotels Have Reportedly Been Hacked," available at http://www.nationaljournal.com/tech/donald-trump-s-hotels-have-reportedly-been-hacked-20150701.

[79]See "Cyber breach hits 10 million Excellus healthcare customers," available at http://www.usatoday.com/story/tech/2015/09/10/cyber-breach-hackers-excellus-blue-cross-blue-shield/72018150/; "BREAKING: Massive Cyber Attack at Banner Health Affects 3.7M Individ-uals," available at http://www.healthcare-informatics.com/news-item/cybersecurity/breaking-massive-cyber-attack-banner-health-affects-37m-individuals. Don't forget that along with the problems and litigations associated with a data breach, healthcare organizations also face poten-tial HIPPA violations as well. See, e.g., "Health Care System to Pay Largest Data Breach Set-tlement Ever," available at https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/health-care-system-to-pay-largest-data-breach-settlement-ever.aspx.

[80]See "Harvard says data breach occurred in June," available at https://www.bostonglobe.com/metro/2015/07/01/harvard-announces-data-breach/pqzk9IPWLMiCKBl3IijMUJ/story.html; "Who hacked Rutgers? University spending up to $3M to stop next cyber attack," available at http://www.nj.com/education/2015/08/who_hacked_rutgers_university_spending_up_to_3m_to.html; "University of Georgia hit by cyberattack," available at http://www.ajc.com/news/local-education/university-georgia-hit-cyberat-tack/jeGZpeHnYViTSI5u62YhSN/.

CHAPTER 2:
FEDERAL REGULATION AND OVERSIGHT – TODAY AND TOMORROW

PURPOSE OF THIS CHAPTER:

1. **Identify the various Federal regulatory agencies that have cyber security oversight and/or regulatory authority over companies.**
2. **Identify, in particular, the regulatory role of the SEC and FINRA over cybersecurity for registered investment advisers, funds and broker dealers.**
3. **Identify, in particular, the regulatory role of the Department of the Treasury/Office of the Controller of the Currency, the Federal Trade Commission and the Department of Health and Human Services over cybersecurity cybersecurity for those entities regulated by these governmental bodies.**

The regulatory drumbeats out of Washington D.C. continue despite the dysfunction of Congress in actually doing anything to foster or strengthen cyber security procedures in the private industry sector:

> "The consequences of cyber incidents are serious. When credit card data is stolen, it disturbs lives and damages consumer confidence. When trade secrets are robbed, it undercuts America's businesses and undermines U.S. competitiveness. And successful attacks on our financial system would compromise market confidence, jeopardize the integrity of data, and pose a threat to financial stability. As it stands, our laws do not do enough to foster information sharing and defend the public from digital threats. We need legislation with clear rules to encourage collaboration and provide important liability protection. It must be safe for companies to collaborate responsibly, without providing immunity for reckless, negligent or harmful behavior. And we need legislation that protects individual privacy and civil liberties, which are so essential to making the United States a free and open society. We appreciate the bipartisan interest in addressing this important issue, and the Administration will continue to work with key stakeholders on the various bills that are developing in Congress."
>
> US Treasury Secretary Jacob J. Lew, July 16, 2014[1]
>
> "What we found, as a general matter so far, is that a lot of preparedness, a lot of preparedness, a lot of awareness but also but their policies and procedures are not tailored to their particular risks."
>
> US SEC Chairperson Mary Jo White, May 19, 2016[2]

The regulatory drumbeats have been further enhanced by messaging, policy directives and executive orders from the White House. Even though comprehensive legislation has not been passed, the Executive Branch has been vocal in the realm cybersecurity. As recently as February 9, 2016, President Barack Obama issued a Cybersecurity National Action Plan (CNAP) that:

> takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security…[3]

While CNAP does not break fundamentally new ground, in retrospect it may serve as the cybersecurity capstone for a presidency that has clearly recognized the significance of cybersecurity as a national security issue and actively raised awareness in both the public and private sectors. Including the Presidential Policy Directive of February 13, 2009 and the February 12, 2013 Executive Order - Improving Critical Infrastructure Cybersecurity, the White House has delegated industry specific guidance roles and responsibilities to a broad range of government agencies and regulatory bodies. The Obama administration has also very recently called for the government to prioritize basic and long-term research on the development and use of artificial intelligence.[4]

Thus, in the absence of comprehensive cyber legislation, the responsibility for the consequences of a cyber-attack to a U.S. public company clearly lay with its board of directors. Luis Aguilar, a Former Commissioner of the SEC, stated very clearly in a speech entitled "Cyber Risks in the Boardroom,"[5] that,

> [B]oards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. Boards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk **and there can be little doubt that cyber risk also must be considered as part of board's overall risk oversight**. The recent announcement that a prominent proxy advisory firm [Institutional Shareholders Services (ISS)] is urging the ouster of most of the Target Corporation directors because of the perceived "failure…to ensure appropriate management of [the] risks" as to Target's December 2013 cyber-attack is another driver that should put directors on notice to proactively address the risks associated with cyber-attacks.

Id. (alteration in original) (emphasis added) (footnotes omitted).

Without equivocation, Commissioner Aguilar stated that cyber security was a Board responsibility. Likewise, ISS signaled that directors could or should be held personally accountable for cyber security breaches if they fail to keep their eye on the ball.[6] And the plaintiffs' bar has recognized that cyber security breaches may become a lucrative addition to their class action litigation practices.[7]

We lastly note there is even a move afoot today to add a cybersecurity-savvy member to the Board of Directors today to improve the oversight function of the board. This move was contained in the not yet passed Cybersecurity Disclosure Act of 2015, which would force "every publicly held company in the United States - and there are thousands - to specify in their public filings which member of their board of directors is their designated cybersecurity expert (let's call this Director the "DCE"). If the board does not have a DCE the company must explain why it feels that it does not need one and what measures it is taking to protect itself from cybercrime and cyberattacks."[8]

As we have noted above, in the absence of some broad Congressional mandate regarding the imposition of a unified cyber security standard, we have instead veritable panoply of federal and state regulators who have all issued some sort of "cyber guidance" to regulated entities to help focus them on cyber security governance. In response to this quickly evolving area of regulation and oversight of cyber security, and the ever-increasing scrutiny by multiple regulators on the board of

directors, we provide here this short, non-exclusive list of how the U.S. government and its agencies are dealing with companies under their specific regulatory authority related to cyber security.[9]

THE UNITED STATES DEPARTMENT OF JUSTICE

The newest entrant into the field of regulatory "guidance" is the United States Department of Justice, who on April 29, 2015 issued a memo entitled "Best Practices for Victim Response and Reporting of Cyber Incidents."[10] Though not necessarily "regulatory" in nature, it certainly contains *suggestions* from the Department of Justice for companies dealing with cyberattacks. The suggestions were as a result of the nation-state attack against Sony Pictures, and the desire to change the public persona that a victim of a nation-state was truly "a victim," and deserved to be treated as such. It sets forth guiding principles for pre-breach conduct and post-breach conduct by companies. These principles include both reaching out to local enforcement before a breach to establish a working relationship with their local FBI or Secret Service Field office, as well as notifying local law enforcement of the breach early in the process if criminality is suspected.

Under the Cybersecurity National Action Plan, issued July 26, 2016, if there is a level 3 severity breach or greater, the responding federal agencies, at least in the first instance, would be the DOJ, by and through FBI and the National Cyber Investigative Joint Task Force (NCIJTF).[11] The cooperation both pre-and-post breach may likely garner the full support of the Department of Justice, FBI and Secret Service, as it helps the victim company investigate the breach and perhaps attribute it to a definite source, and may also engender favorable treatment of the breached company by the Federal Trade Commission. The April 29th Department of Justice Memo and the Cybersecurity National Action Plan are both very new, and we will watch closely to see how its principles play out in practice.

THE UNITED STATES SECURITIES AND EXCHANGE COMMISSION (THE "SEC")

Certainly a significant portion of the Federal activity on cyber security issues has come from the SEC. And given the SEC's role in generally overseeing the financial markets, there can be no doubt of the SEC's importance in controlling systemic risk throughout the financial markets.[12]

The most recent genesis of its involvement began on or about October 12, 2011, when the SEC issued guidance regarding the disclosure obligations of public companies to investors and the securities markets relating to cyber security risks and cyber incidents. The focus of this guidance was on whether information concerning cybersecurity and cyber incidents rose to the level of a disclosure obligation either as a risk factor under Regulation S-K Item 503(c) or in the MD&A Section of a Company's mandatory SEC disclosure. One of the critical determining factors for the SEC was whether:

> [T]he costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a **material** event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.[13] (emphasis added)

Id. (emphasis added). If the registrant does determine its cyber security risk or previous cyber incidents rise to the level of a disclosable event, the SEC guidance notes that such disclosure might contain information reflecting:

- Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; and
- Description of relevant insurance coverage.

Id.

The SEC's October 2011 cyber guidance was just that – guidance. The question of "materiality" is and was left within the discretion of the company. There was no discussion about when the risk of "potential incidents" rose to the level of disclosure. Fueled by continuing major cyber breaches, on March 26, 2014 the SEC organized a "cyber roundtable" among industry groups and public and private sector participants in order to consider, among other things, whether or not additional SEC guidance related to the level of disclosure in a company's public filings was necessary. It will be interesting to see how events develop at the SEC, particularly as cyber breaches continue to increase in number and scope. We see already today that SEC Division of Corporate Finance comment letters are pointing registrants towards more cyber security disclosure rather than less regarding past cyber incidents and information security measures. We do not see that trend changing. In fact, at a conference in February 2015, David Glockner, the Director of the SEC's Chicago Regional Office said that cybersecurity was effectively "high on [the SEC's] radar."[14] Note that some also theorize that the failure to safeguard assets may or could under some cases be a violation of Section 404 of the Sarbanes-Oxley Act of 2002.[15]

SEC OFFICE OF COMPLIANCE, INSPECTIONS AND EXAMINATIONS (OCIE)

On April 15, 2014, the OCIE issued a National Exam Program Risk Alert, entitled "OCIE Cybersecurity Initiative," announcing it would conduct examinations of more than 50 registered broker-dealers and investment advisors "designed to assess cybersecurity preparedness in the securities industry and to obtain information about the industry's recent experiences with certain types of cyber threats."[16] Importantly, this alert came with an extensive list of questions requiring registrants to respond to various areas of their cyber security preparedness. Some of the questions are as follows:

- Please identify any published cybersecurity risk management process standards, such as those issued by the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO), the Firm has used to model its information security architecture and processes.
- Please indicate which of the following practices and controls regarding the protection of its networks and information are utilized by the Firm, and provide any relevant policies and procedures for each item.
- Confirm that the Firm provides written guidance and periodic training to employees concerning information security risks and responsibilities. If the Firm provides such guidance and/or training, please provide a copy of any related written materials (e.g.,

presentations) and identify the dates, topics, and which groups of employees participated in each training event conducted since January 1, 2013

- Confirm that the Firm maintains controls to prevent unauthorized escalation of user privileges and lateral movement among network resources. If so, please describe the controls, unless fully described within policies and procedures.
- Confirm that the Firm restricts users to those network resources necessary for their business functions. If so, please describe those controls, unless fully described within policies and procedures.
- Confirm that the Firm has a process for ensuring regular system maintenance, including timely installation of software patches that address security vulnerabilities.
- Does the Firm maintain protection against Distributed Denial of Service (DDoS) attacks for critical internet-facing IP addresses? If so, please describe the internet functions protected and who provides this protection.
- Confirm that the Firm maintains a written cybersecurity incident response policy. If so, please provide a copy of the policy and indicate the year in which it was most recently updated. Please also indicate whether the Firm conducts tests or exercises to assess its incident response policy, and if so, when and by whom the last such test or assessment was conducted.

The OCIE list also required responses including information on employee training, vendor management, the firm's practices to detect "unauthorized activity on its networks and devices," and specific information, if applicable, concerning any cyber breaches which the registrant experienced since January 1, 2013.[17]

On February 3, 2015, the SEC published a summary of the initial 100 examinations.[18] The results were both good and not so good. In most cases, firms admirably performed comprehensive risk assessments and had written information security policies. Note that in some cases however, the regulated entities examined did not perform risk assessments of vendors and business partners. Very few of the entities examined maintained cyber insurance to transfer any risk of an attack to a third party. Clearly, the story of cybersecurity examinations of regulated investment advisers and funds "will be continued", and it will be interesting to see if more and more firms adopt best practice guidance set forth by SEC OCIE. And if the regulated entities and advisers do not take the implicit "hint" of the SEC it will be interesting to see if penalties will result. It is certainly possible that the SEC might file more enforcement actions related to alleged inadequate cybersecurity measures under Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)), which requires firms to have policies and procedures to address protection of customer records and information, regardless of whether a breach occurred.

On September 15, 2015, OCIE put out a second cybersecurity risk alert, entitled "OCIE's 2015 Cybersecurity Examination Initiative."[19] Though this Risk Alert is somewhat repetitive of the April 2014 Alert, OCIE set forth an additional area of emphasis: "Access Rights and Controls," which deals in general with how users access network servers, and, in particular, how firms "prevent unauthorized access to systems or information, such as multifactor authentication or updating access rights based upon personnel or system changes."[20] We assume that with respect to "access rights," OCIE is indicating that it will review how firm's monitor access privileges given to authorized users in order to assess whether firm's are "over-privileging" certain employees or groups of employees. Access and privilege rights have both emerged as pressing problems during 2014 and 2015 among many companies that have suffered significant breaches. In sum, this is important new

information for registered funds and advisers to consider as they prepare for their second round of cybersecurity examinations. What we don't know (yet) is with so much guidance now in existence, if examiners find funds or firms deficient in their compliance, will that result in fines, penalties or, at the very least, some form of adverse publicity.[21] Though we don't know yet, early indications are that, most certainly, the SEC is closely watching the cybersecurity efforts of its regulated entities based upon its recent decision in an administrative proceeding opinion entitled R.T. Jones Capital Equities Mgt., Inc.[22] Our view is that considering entities falling under OCIE's regulatory authority will be looked at in the rear view mirror for compliance after a disclosed cybersecurity breach or theft of information, compliance with OCIE's guidance should be strongly considered.

SEC REGULATION SYSTEMS, COMPLIANCE AND INTEGRITY ("REG SCI")

The U.S. Securities and Exchange Commission adopted Regulation Systems Compliance and Integrity and Form SCI in November 2014 to strengthen the technology infrastructure of the U.S. securities markets. Specifically, the rules are designed to:

- Reduce the occurrence of systems issues;
- Improve resiliency when systems problems do occur;
- Enhance the Commission's oversight and enforcement of securities markets' technology infrastructure.

Who Regulation SCI applies to

Regulation SCI applies to "SCI entities," a term which includes self-regulatory organizations ("SROs"), including stock and options exchanges, registered clearing agencies, FINRA and the MSRB, alternative trading systems ("ATSs"), that trade NMS and non-NMS stocks exceeding specified volume thresholds, disseminators of consolidated market data ("plan processors"), and certain exempt clearing agencies. The SEC has indicated that *at some point* it might extend the reach of Reg. SCI to other entities (for instance, other regulated funds and regulated entities like private equity firms).

Reg SCI Rule and Compliance Regulations

Reg SCI requires a detailed compliance rubric of policies and procedures that must be done by SCI entities. Some of which has been seen before in other SEC cybersecurity guidance, and some of which is new or now mandatory under Reg SCI. Under Reg SCI, an SCI Entity must:

(1) establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems and, for purposes of security standards, SCI security systems, have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets; and

(2) Include certain required elements in such policies and procedures. As proposed, these policies and procedures were required to provide for: (A) the establishment of reasonable current and future capacity planning estimates; (B) periodic capacity stress tests of systems to determine their ability to process transactions in an accurate, timely, and efficient manner; (C) a program to review and keep current systems development and testing methodology; (D) regular reviews and testing of systems, including backup systems, to identify vulnerabilities pertaining to internal and external threats, physical hazards, and natural or manmade disasters; (E) business continuity

and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse to ensure next business day resumption of trading and two-hour resumption of clearance and settlement services following a wide-scale disruption; and (F) standards that result in systems being designed, developed, tested, maintained, operated, and surveilled in a manner that facilitates the successful collection, processing, and dissemination of market data.

FINANCIAL INDUSTRY REGULATORY AUTHORITY (FINRA)

In January 2014, FINRA announced a "sweep" program, which in effect is very similar to OCIE's, whereby firms under FINRA's authority would be receiving targeted examination letters requiring them to respond to questions relating in general to their cyber preparedness.[23] FINRA's targeted examination letters seek information very similar to the OCIE cybersecurity initiative.

On February 3, 2015, FINRA issued its own report on the cybersecurity practices of the broker-dealer industry.[24] Rather than being a results-oriented report, the FINRA report was "best practices" based for broker-dealers to hold up against their own cybersecurity policies and procedures and see where there are gaps. The FINRA report provided extensive guidance to its entities on the following points:

- A sound governance framework with strong leadership is essential. Numerous firms made the point that board- and senior-level engagement on cybersecurity issues is critical to the success of firms' cybersecurity programs.
- Risk assessments serve as foundational tools for firms to understand the cybersecurity risks they face across the range of the firm's activities and assets—no matter the firm's size or business model.
- Technical controls, a central component in a firm's cybersecurity program, are highly contingent on firms' individual situations. Because the number of potential control measures is large and situation dependent, FINRA discusses only a few representative controls here. Nonetheless, at a more general level, a defense-in-depth strategy can provide an effective approach to conceptualize control implementation.
- Firms should develop, implement and test incident response plans. Key elements of such plans include containment and mitigation, eradication and recovery, investigation, notification and making customers whole.
- Broker-dealers typically use vendors for services that provide the vendor with access to sensitive firm or client information or access to firm systems. Firms should manage cybersecurity risk exposures that arise from these relationships by exercising strong due diligence across the lifecycle of their vendor relationships.
- A well-trained staff is an important defense against cyberattacks. Even well-intentioned staff can become inadvertent vectors for successful cyberattacks through, for example, the unintentional downloading of malware. Effective training helps reduce the likelihood that such attacks will be successful.

In early 2015, FINRA distributed a 33 question Risk Control Assessment (RCA) to all member firms. 23 of the 33 questions were related to cybersecurity, including:

- Does your firm manage or store any customer personally identifiable information (PII)?
- Does your firm have policies and procedures that define criteria for the protection of customer PII data stored?

- How frequently does your firm report to executive management on the implementation and effectiveness of the firm's cybersecurity program?
- Has your firm performed a cybersecurity risk assessment in the past year to identify key cybersecurity risks?
- Has your firm experienced a successful cyber-attack in the past 24 months?

To date, FINRA has not publicly shared the results of the RCA but given the breadth of the industry, nearly 4,000 member firms and ~160,000 branch offices, FINRA must have gathered a treasure trove of data and gained a much clearer picture of the level of cybersecurity resiliency in the broker dealer community.

FINRA has issued a voluntary 2016 RCA and explained how they intend to use the results:

> FINRA will use the results of the RCA to better understand the specific business models of individual member firms, the attendant risks of those business models, and the controls intended to manage those risks. We will also use this information to benchmark controls and get a better sense of industry-leading practices as they relate to risks and controls. FINRA will use this information to enhance the quality of our regulatory programs-particularly our surveillance and onsite examinations.

The 2016 RCA is much longer with over 200 questions, with 20 questions focused on cybersecurity including more in depth questions regarding cybersecurity incidents as well as access and authentication protocols.[25]

Certainly, we can see a trend here. Both OCIE and FINRA are looking not only at previous cyber-attacks, but at the infrastructure in place at their regulated entities to prevent such attacks. In connection with the RT Jones decision, Andrew Ceresney recently stated:

> Cyber is obviously a focus of ours, as I know it is for the other divisions, and we've brought a number of cases there relating to Reg S-P and failure to have policies and procedures relating to safeguarding information," Ceresney said, citing the case the commission brought against R.T. Jones, a St. Louis-based RIA, this past summer. "There'll be others coming down the pike," Ceresney cautioned.[26]

Guidance again is abundant. On to next year's cybersecurity examinations to see if people were watching and listening. We hope they were.

CYBERSECURITY RISK MANAGEMENT STANDARDS OF THE OCC

Of course, as we were preparing the final draft of our book, the Office of the Comptroller of the Currency (OCC) decided to issue (on 10/18/16) a 49 page release entitled "Enhanced Cybersecurity Risk Management Standards" which it stated will likely apply "to depository institutions and depository institution holding companies with total consolidated assets of $50 billion or more." [hereinafter referred to as the "OCC Release"]. As noted in the OCC Release this is not the first time the Department of the Treasury has issued cybersecurity guidance and assessment tools through or by another departmental agency, like, e.g., the FFIEC which has issued numerous releases and its Cybersecurity Assessment Tool that was designed to help banks to assess and improve their cybersecurity posture. Here are some of the major points in the OCC release (it currently is in a comment period so we don't know what the final rule will look like):

1. The OCC Release applies to entities with consolidated assets of $50 million or more. The figure listed here is due to systemic risk issues; if an entity like this goes under, it might affect other large entities as well as the banking market as a whole. The Wall Street Journal recently noted, "The draft plan would impose the toughest restrictions on firms considered to pose the greatest risk to the financial system. Those firms would have to prove they can get their core operations running within two hours of a cyberattack or major IT failure. The new rules also would apply to nonbank financial companies deemed systemically risky by a panel of regulators headed by Treasury Secretary Jacob Lew." [29]
2. Tremendous (though not unexpected) emphasis on the board of directors' role in setting a formal cyber risk management strategy and for holding senior management accountable for establishing appropriate policies and procedures relating to cyber risk management (this point is little different from the proposed FFIEC rules). Boards have continuing obligation to monitor and assess the bank's adherence to good cyber risk practices.
3. Banks would be required to perform continuous risk assessments across the enterprise.
4. Loosely speaking the new rules would require that Banks continue to adhere to best practices contained in the NIST cybersecurity framework.
5. The rules continue to require good vendor risk management, especially where they are outsourcing operations.
6. Finally, the banks affected by the rules must have battle-tested incident response and business continuity plans dealing with cyber resilience.

For the large banks affected or potentially affected by the new Department of Treasury rules, much of the guidance noted above is nothing new. Not many surprises here. The rules however will be mandatory, and woe be to the entity that decides that they don't want to comply with them.

Most recently, on October 25, 2015, the Financial Crimes Enforcement Network (FinCEN) of the Treasury Department issued an advisory to financial institutions pertaining to cybersecurity and cyber attacks.[30] For cyber attacks which involve the theft or suspected theft of $5,000 or more, financial institutions must report these attacks in a Suspicious Activity Report (or SAR). The memo further notes "When filing a mandatory or voluntary SAR involving a cyber-event, financial institutions should provide complete and accurate information, including relevant facts in appropriate SAR fields, and information about the cyber-event in the narrative section of the SAR—in addition to any other related suspicious activity." The hope here is that by sharing cyber threat intelligence information, "Financial institutions can work together to identify threats, vulnerabilities, and criminals. By sharing information with one another, financial institutions may gain a more comprehensive and accurate picture of possible threats, allowing for more precise decision making in risk mitigation strategies. FinCEN continues to encourage financial institutions to use all lawful means to guard against money laundering and terrorist activities presented through cyber-events and cyber-enabled crime."[31]

SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT

To be fair and impartial, the winner in the US cyber security regulatory enforcement space has clearly been the US Federal Trade Commission ("FTC") who to date has brought over 50 enforcement actions against US companies related to cyber security. "Since 2002, the FTC has pursued numerous investigations under Section 5 of the FTC Act against companies for failures to abide by stated privacy policies or engage in reasonable data security practices. It has monitored compliance with consent orders issued to companies for such failures."[32] One recent report noted that:

> The FTC is gaining ground in the national cybersecurity debate due to an aggressive attempt to expand its authorities under Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive acts or practices. The agency's push for greater authority to regulate cybersecurity practices in the private sector won a major victory recently when a federal judge denied a motion to dismiss the FTC's case against Wyndham Worldwide Corp. for failing to protect consumer information. According to a Sept. 11 report by the Congressional Research Service, the judge's ruling effectively lends support to the FTC's position that it possesses jurisdiction to regulate data security under its unfair or deceptive practices authority. And as new massive data breaches make the news, experts warn of additional FTC enforcement actions on the horizon."[33]

The modus operandi of the FTC is simple: following the announcement of a cybersecurity breach, the FTC may swoop in and charge the Company with a Section 5 violation, like it did in Wyndham Worldwide, alleging that the failure of the Company to safeguard it's customers' data was an unfair practice.[34] To our knowledge, the majority of these cases have settled prior to a full hearing or trial.

The FTC's power to regulate cybersecurity was recently upheld by the Third Circuit Court of Appeals in August 2015. In FTC v. Wyndham Worldwide Corp., 799 F. 3d 236 (3d Cir. 2015), the Third Circuit affirmed that the FTC has authority to regulate cybersecurity. The Third Circuit held that Section 5 was not impermissibly vague. Congress had explicitly rejected the notion that specific "unfair" practices should be enumerated in the act. According to Section 5(n) of the FTC Act, to be deemed "unfair," (1) an act must be likely to cause "substantial injury" to consumers, (2) consumers cannot reasonably avoid the injury, and (3) the injury is not outweighed by benefits to consumers or competition. The language thus informs parties that the relevant inquiry is a cost-benefit analysis.

Regulation of cybersecurity was again evidenced in the recent LabMD decision. In a unanimous opinion and very broad opinion authored by FTC Chairwoman Edith Ramirez, the Commissioners held that LabMD's data security lapses were unreasonable and amounted to an unfair act or practice under Section 5 of the FTC Act, because they caused the unauthorized disclosure of patients' confidential medical data, amounting to a "substantial injury" to consumers. The Court noted in detail that:

> There is also broad recognition in federal and state law of the inherent harm in the disclosure of sensitive health and medical information. Section 5(n) expressly authorizes us to look to "established public policies" as additional evidence in support of a determination about whether a practice is unfair, including whether it causes substantial injury, and we do so here. Federal statutes such as HIPAA and the Health Information Technology for Economic and Clinical Health ("HITECH") Act, as well as state laws, establish the importance of maintaining the privacy of medical information in particular. See, e.g., HIPAA, 42 U.S.C. §§ 1320 et seq. (directing HHS to promulgate privacy and security rules for health information); 45 C.F.R. Parts 160 & 164 (privacy, data security, and related rules); HITECH Act, Pub. L. No. 111-5, 123 Stat. 226 (2009), codified at 42 U.S.C. §§ 300jj et seq.; §§ 17901 et seq.. [35]

OTHER FEDERAL REGULATIONS RELATED TO CYBER SECURITY

Gramm-Leach Bliley Act (GLBA)

Perhaps most famous for repealing part of the Glass-Steagall Act of 1933, the GLBA, also known as the Financial Services Modernization Act of 1999, has a cyber-data component and applies to "financial institutions," i.e., "any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust, or other financial account or relationship with the institution." This regulation is called Regulation S-P.[36] Under the Regulation S-P, financial institutions are required to "establish appropriate standards" to safeguard a customer's personal financial information, in order: "(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[37] Under Regulation S-P, financial institutions, in actions brought by the Department of Justice only (there is no private right of action), can be fined up to $100,000 for each violation, AND directors and officers of financial institutions could be held personally liable for civil penalties of up to $10,000 for each violation.

In April 2013, the SEC and CFTC jointly adopted a rule for the prevention of identity theft, called Regulation S-ID ("Reg S-ID" or "Rule"). "The Rule requires SEC or CFTC registrants (e.g., investment advisers, investment companies, broker-dealers, commodity pool advisors, futures commission merchants, retail foreign exchange dealers, commodity trading advisers, introducing brokers, swap dealers, and major swap participants) to establish and maintain programs that detect, prevent, and mitigate identity theft, if they maintain certain types of accounts for clients. These organizations must implement Reg S-ID policies and procedures by November 20, 2013."[38]

Payment Card Industry Data Security Standard (PCI DSS)[39]

The PCI DSS is not necessarily a "law" but a list of cyber security standards applied to any U.S. company that processes credit cards, such as retailers, resort and destination companies, or financial institutions. The list focuses on, among other general requirements, the need to "develop and maintain secure systems and applications," and the need to "track and monitor all access to network resources and cardholder data." These standards provide an "actionable framework for developing a robust payment card data security process – including prevention, detection and appropriate reaction to security incidents."[40] PCI DSS 3.0, adopted in November 2013, enlarges the scope of data security requirements upon retailers and financial institutions.[41]

It will be interesting to see whether "3.0," which was to be implemented by retailers on or about January 1, 2015, will have any material effect on an industry sector that continues to experience major cyber security breaches along the lines of Target, Home Depot, Kmart, P.F. Chang's or Neiman Marcus.[42]

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Among many other things, 2014 was also a year when the US saw a staggering number of cyber security breaches in the healthcare, managed healthcare and hospital sectors. For instance, in August 2014, Community Health Systems - with 206 hospitals in 29 states - reported that it had been hacked, with protected health information covering 4.5 million patients compromised as a result.[43] In February 2015, Anthem Healthcare suffered a tremendous cybersecurity breach which resulted in the loss of personal information on over 80 million of its customers. Indeed, one recent

KPMG survey noted that, "[i] n the past two years, 81 percent of hospitals and health insurance companies have had a data breach."[44]

Here is the basic problem for the healthcare industry when it comes to cyber - the information it stores on patients is a "gravy train" for cyber criminals:

- Medical identity theft is more lucrative than credit card theft. According to PhishLabs, a provider of cybercrime protection and intelligence services, stolen health credentials are worth about 10 to 20 times that of a U.S. credit card number.
- Forty-three percent of all identity theft is caused by medical records theft.
- The cost of a health care data breach averages $355 per record, well above the $201 per record for all industry segments combined, according to the Ponemon Institute's 2015 Cost of Data Breach Study.[45]

These facts show the lucrative target the healthcare industry provides to cyber thieves. Indeed, one senior healthcare cyber analyst at the Sans Institute noted:

> This level of compromise and control could easily lead to a wide range of criminal activities that are currently not being detected. For example, hackers can engage in widespread theft of patient information that includes everything from medical conditions to social security numbers to home addresses, and they can even manipulate medical devices used to administer critical care.[46]

HIPAA requires, in general, the protection and confidentiality of all electronically protected healthcare information that is created, received, maintained or transmitted. Under HIPAA, a healthcare facility must protect against any reasonably anticipated threat, or hazard, to the security or integrity of such healthcare information. Under HIPAA, fines can range from $50,000 to $250,000. There also can be civil litigation exposure as well, as demonstrated by the Anthem breach.

In particular, for directors and officers of healthcare related companies, HIPAA has three basic rules (also tons of minor ones which will not have the time to cover):

1. HIPAA Security Rule: Provides that covered entities (e.g. health care plans, health care insurers, HMO's and healthcare providers) and business associates must develop and implement policies and procedures to protect the security of ePHI (electronic personal health care information) that they create, receive, maintain, or transmit. Each entity must analyze the risks to the ePHI in its environment and create solutions appropriate for its own situation. Each entity must also conduct risk and security assessments to attempt to mitigate the risks associated with the confidentiality of the information being maintained.
2. HIPAA Privacy Rule: establishes standards for the protection of PHI held by covered entities and their business associates (defined below) and gives patients important rights with respect to their health information. Additionally, the Privacy Rule permits the use and disclosure of health information needed for patient care and other important purposes.

Protected Information

The Privacy Rule protects individually identifiable health information, called PHI, held or transmitted by a covered entity or its business associate, in any form, whether electronic, paper, or verbal. PHI includes information that relates to the following:

The individual's past, present, or future physical or mental health or condition;

The provision of health care to the individual; or

The past, present, or future payment for the provision of health care to the individual.

PHI includes many common identifiers, such as name, address, birth date, and Social Security Number.

HIPAA Breach Notification Rule: The Breach Notification Rule requires covered entities to notify affected individuals, HHS, and in some cases, the media of a breach of unsecured PHI. Most notifications must be provided without unreasonable delay and no later than 60 days following the discovery of a breach.[47]

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (THE HITECH ACT)

The HITECH Act expands the scope of the institutions covered under HIPAA to now include any organization or individual who handles protected healthcare information, which could now include banks, businesses, schools and other organizations.[48] Additionally, there is a requirement that HIPAA covered entities have a written contract with any business associate (BA) that handles PHI on behalf of the covered entities (i.e.: cloud service providers, etc.). The Act sets clear breach notification protocols if more than 500 PHI records are compromised, requiring notification of all affected individuals, the Secretary of Health and Human Services, and the media. The HITECH Act also increased the potential fine or penalty for a health care information cyber breach up to $1.5 million per violation.

HIPAA, HITECH AND THE NIST FRAMEWORK

One of the more interesting and in fact exciting developments over the past year is that the NIST is now in the healthcare security game. In order to assist organizations in properly aligning their cybersecurity to the HIPAA Security Rule, the NIST has mapped the Cybersecurity Framework to the HIPAA Security Rule in an organized and methodical way.[49] The "NIST Crosswalk" may be useful for any covered entity to assess its compliance with the Security Rule through an independent tool. The Crosswalk is not mandatory, but in our view an advisable suggestion especially to healthcare companies that do not have a mature cybersecurity profile.

CHILD ONLINE PRIVACY PROTECTION ACT OF 1998 (COPPA)

While we have deliberately avoided the very broad and controversial topic of privacy, COPPA is worth mentioning in this chapter as it sets very clear requirements for websites that target children or collect information from children. These requirements include enabling parents to review and delete any information from the site and clear disclosure in a readily available privacy statement of the uses (internal and external) of the data collected,

THE REGULATORY ENVIRONMENT: TODAY AND TOMORROW

Cyber security is the buzzword of the day, year, and maybe the decade. Well-publicized cyber breaches at major U.S. companies are now becoming the norm and have caused not only tremendous anxiety for executives, but reputational damage and material revenue loss for many

companies.[50] These breaches have not only caused both consumer and securities class and derivative actions, but have caught the eye of both federal and state regulators of many industries.

Given the broad regulatory spectrum we identified above, cyber security issues must continue to be omnipresent on the minds of corporate executives because any industry is at risk of having their IP, destroyed or stolen by hackers. In response to this ever changing landscape of increasingly complex threat vectors, plus increasing regulation, directors and officers, and their companies' CISOs and CIOs, must adapt daily and continue daily discussions about how to improve their company's cyber security procedures and detection/incident response plans of action. Adaptation means not just "checking the box" on some measure of an industry standard but having real discussions about allocating real physical and financial resources of the company to protect its most valuable IP and customer information. Adaptation means that companies and firms need to continue to adopt demonstrable and auditable processes and procedures which provide evidence to all constituencies (including their auditors) that they are paying attention and responding to the cyber security threat with actionable measures, and not just talking points. As we note above, one of the most important constituencies is "the regulators," where a fine or penalty could lead to further civil or reputational consequences. Whether that means adopting the NIST cyber security framework or continuing to improve upon their own cyber security procedures in a demonstrable fashion, directors and officers must consider the consequences of "failing to act". Even in the face of seemingly unimaginable technological threats to US businesses (e.g., Sony Pictures) directors and officers will likely be looked at with ever increasing scrutiny by regulators, customers, and investors in years to come.

ENDNOTES:

[1]See "In Call to Action, Treasury Secretary Lew Urges US Financial Sector to Redouble Efforts Against Cyber Threats," found at http://www.treasury.gov/press-center/press-releases/Pages/jl2571.aspx.

[2]See "5 Actionable Steps We Can Learn from the SWIFT Banking Attacks," available at http://www.tripwire.com/state-of-security/security-data-protection/5-actionable-steps-we-can-learn-from-the-swift-banking-attacks/. Apparently not much was learned in the aftermath despite all hands alerts to SWIFT member banks. "A group of hackers later attempted to replicate this attack with another foreign bank, Vietnam's Tien Phong Bank. Curiously, this second attack may have been structured by obtaining access to the computer system of a third-party vendor doing business with the Vietnam Bank. To those in the security community, that vector (a trusted vendor) sounds incredibly familiar." Id.

[3]See "The President's National Cybersecurity Plan: What You Need to Know," available at https://www.whitehouse.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-know.

[4]See "White House unveils new goals for AI," available at http://fedscoop.com/white-house-unveils-new-goals-for-developing-monitoring-ai; "The White House Meets WestWorld: The "Future of Artificial Intelligence" in the United States," available at https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-white-house-meets-westworld-the-future-of-artificial-intelligence-in-the-united-states/.

[5]Available at http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

[6]See Paul Ziobro & Joann S. Lublin, *ISS's View on Target Directors Is a Signal on Cybersecurity*, Wall St. J., May 28, 2014, available at http://www.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278.

[7]See Jeffrey Roman, *Supervalu Hit With Lawsuit After Breach*, Bank Info Security (Aug. 20, 2014), available here; see also the following recently filed complaints in *Davis v. Steinhafel*, Case Nos. 14-cv-00203-PAM-JJK *et seq.*, 2014 WL 3853976 (D. Minn. July 18, 2014) ; *Diana v. Horizon Healthcare Servs., Inc.*, Case Nos. 2:13-CV-07418-CCC-MF, 2:14-cv-00584-CCC-MF, 2014 WL 3351730 (D.N.J. June 27, 2014).

[8]See "Feds might force your board to be cyber-aware," available at http://www.csoonline.com/article/3102985/security/feds-might-force-your-board-to-be-cyber-aware.html.

[9]We leave for another day how various state agencies and authorities (e.g., the New York State Department of Financial Services ("DFS")) are simultaneously dealing with cyber security related issues. See e.g., New York State Department of Financial Services' Report on Cyber Security in the Banking Sector (2014), available at http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf/. It is, however, important to note that in September 2016, the NY Department of Financial Services recently issues a broad based mandate that entities under its regulatory authority take to improve their cybersecurity posture. See "CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES," available at http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf. Though very much consistent with other cybersecurity guidance and initiatives proposed by the NIST and SEC, among other things, the new DFS rules go one step further and require the appointment of a CISO.

[10]The Memo can be found at http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf.

[11]See "Countering the Cyber Threat: New U.S. Cyber Security Policy Codifies Agency Roles," available at https://www.fbi.gov/news/stories/new-us-cyber-security-policy-codifies-agency-role.

[12]See Statements of James Clapper, Director of National Intelligence, to the House Permanent Committee on Intelligence, dated September 10, 2015, where he noted cyber's potential effects on the financial markets, stating, "Successful cyber operations targeting the integrity of information would need to overcome any institutionalized checks and balances designed to prevent the manipulation of data, for example, market monitoring and clearing functions in the financial sector." These comments are available at http://fas.org/irp/congress/2015_hr/091015clapper.pdf.

[13]Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011), available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[14]See "U.S. SEC on the prowl for cyber security cases –official," available at http://www.reuters.com/article/2015/02/20/sec-cyber-idUSL1N0VU2AV20150220.

[15]See "Cybersecurity and Financial Reporting," available at http://www.mindthegaap.com/webarticle/In_Brief_Vol_12_Cybersecurity.pdf. ("According to the SEC's adopting release on ICFR…the safeguarding of assets is one of the elements of internal control over financial reporting. Because customer data is an asset, a company's failure to have sufficient controls to prevent the unauthorized acquisition, use, and/or disposition of customer data may constitute a weakness in ICFR."). See also "Understanding compliance -- Financial and technical standards," available at http://searchsecurity.techtarget.com/feature/Step-1-Understanding-compliance-Financial-and-technical-standards?SOX1.

[16]See "Office of Compliance Inspections and Examinations, 4 National Exam Program Risk Alert, no. 2, Apr. 15, 2014," available here.

[17]In large part, these questions mimic guidance issued by the SEC's Division of Investment Management in April 2015. See "Cybersecurity Guidance," available at http://www.sec.gov/investment/im-guidance-2015-02.pdf.

[18]See Cybersecurity Examination Sweep Summary," available at https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

[19]This Risk Alert can be found at http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

[20]Id.

[21] We lastly note here that in OCIE's 2016 Examination Priorities Memo, OCIE will continue its focus on cybersecurity. In this memo, it noted "in September 2015, we launched our second initiative to examine broker-dealers' and investment advisers' cybersecurity compliance and controls. In 2016, we will advance these efforts, which include testing and assessments of firms' implementation of procedures and controls." This memo can be found at https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2016.pdf.

[22] See "SEC's Regulatory Action against R.T. Jones: Did the Other Cybersecurity Shoe Just Drop?" available at http://www.dandodiary.com/2015/09/articles/cyber-liability/guest-post-secs-regulatory-action-against-r-t-jones-did-the-other-cybersecurity-shoe-just-drop/. A copy of the SEC's press release is available here, http://www.sec.gov/news/pressrelease/2015-202.html.

[23] See FINRA, Target Examination Letters re: Cybersecurity (Jan. 2014), available at http://www.finra.org/industry/cybersecurity-targeted-exam-letter.

[24] See "FINRA 2015 Cybersecurity Report," available at https://www.finra.org/industry/2015-cybersecurity-report.

[25] FINRA again stressed the importance of cybersecurity in its 2016 Priorities letter, noting "FINRA remains focused on firms' cybersecurity preparedness given the persistence of threats and our observations on the continued need for firms to improve their cybersecurity defenses. Given the evolving nature of cyber threats, this issue requires firms' ongoing attention." FINRA 2016 Examination priorities letter can be found here, http://www.finra.org/sites/default/files/2016-regulatory-and-examination-priorities-letter.pdf.

[26] See "SEC Warns More Cyber Enforcement Actions Coming," available at https://www.complianceweek.com/blogs/enforcement-action/sec-cyber-security-now-biggest-risk-facing-financial-system#.WAfZKk3rvcs.

[27] See "Agencies Issue Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards," available at https://www.occ.gov/news-issuances/news-releases/2016/nr-ia-2016-131.html.

[28] See "Cybersecurity Assessment Tool," available at https://www.ffiec.gov/cyberassessmenttool.htm.

[29] See "Regulators to Toughen Cybersecurity Standards at Nation's Biggest Banks," available at http://www.wsj.com/articles/regulators-to-toughen-cybersecurity-standards-at-nations-biggest-banks-1476885600.

[30] See "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," available at https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf.

[31] A nice summary of the FinCEN Memo can be found here, https://www.tripwire.com/state-of-security/latest-security-news/treasury-dept-tells-financial-orgs-report-computer-crime-attacks/.

[32] See "The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority," found at http://fas.org/sgp/crs/misc/R43723.pdf

[33] See "The FTC's expanding cybersecurity influence," found at http://fedscoop.com/ftcs-expanding-cybersecurity-influence/#sthash.HYQJfdC6.dpuf

[34] See e.g., FTC v. Wyndham Worldwide Corp., Civil Action Number: 212-cv-01365-SPL (June 25, 2012), found at http://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation

[35] The LabMD decision can be found here, https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf

[36] See Regulation S-P, available at http://www.sec.gov/rules/final/34-42974.htm#P41_3349. Regulation S-P also applies to investment advisers registered with the SEC ("registered advisers"), brokers, dealers (collectively, "broker-dealers"), and investment companies ("funds") and requires them to adopt appropriate policies and procedures that address safeguards to protect this information. Id.

[37] 15 U.S.C. § 6827(4)(a); 15 U.S.C. § 6801(b)(1)-(3).

[38] See generally "Identity Theft Regulation: Are you under the SEC/CFTC microscope?" available at http://www.pwc.com/us/en/financial-services/regulatory-services/publications/identity-theft-regulation.jhtml.

[39] The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The PCI Security Standards Council's mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards. See https://www.pcisecuritystandards.org/.

[40] PCI Security Standards Council, Navigating PCI DSS, Understanding the Intent of the Requirements, version 2.0 (Oct. 2010), available at https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf; PCI Security Standards Council, PCI SSC Data Security Standards Overview, available here.

[41] Available at https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

[42] For more specific information on the attributes of PCI DSS 3.0, see "How PCI DSS 3.0 Can Help Stop Data Breaches," available at http://www.darkreading.com/risk/compliance/how-pci-dss-30-can-help-stop-data-breaches/a/d-id/1318306.

[43] See generally, "Health care data breaches have hit 30M patients and counting," available at http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/ ("Since federal reporting requirements kicked in, the U.S. Department of Health and Human Services' database of major breach reports (those affecting 500 people or more) has tracked 944 incidents affecting personal information from about 30.1 million people).

[44] See "81 percent of hospitals and health insurance companies have had a data breach," available at http://www.csoonline.com/article/2978911/data-breach/study-81-of-large-health-care-organizations-breached.html.

[45] See "2016 Ponemon Cost of Data Breach Report," available at http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=BUL12370USEN&attachment=BUL12370USEN.PDF.

[46] Two excellent articles, "The Top U.S. Healthcare Story For 2014: Cybersecurity," and "New Cyberthreat Report By SANS Institute Delivers Chilling Warning To Healthcare Industry," which summarize the details of the Sans Institute Health Cyber Threat report are available here at http://www.forbes.com/sites/danmunro/2014/12/21/the-top-u-s-healthcare-story-for-2014-cybersecurity/ and here at http://www.forbes.com/sites/danmunro/2014/02/20/new-cyberthreat-report-by-sans-institute-delivers-chilling-warning-to-healthcare-industry/.

[47] More details concerning the provisions of the HIPAA Security, Privacy and Breach Notification Rules can be found at https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf.

[48] It should also be noted that federal legislation concerning cyber security has been promulgated to protect government data. The Federal Information Security Management Act was enacted in 2002 namely to "enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services." E–Government Act of 2002, Pub. L. No. 107–347, 116 Stat. 2899.

[49] See HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework," available at http://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

[50] For example, Brian Yarbrough, a research analyst with Edward Jones, predicted that after Target's cyber breach, "Probably 5% to 10% of customers will never shop there again." Hadley Malcolm, *Target sees drop in customer visits after breach*, USA Today, Mar. 11, 2014, available at http://www.usatoday.com/story/money/business/2014/03/11/target-customer-traffic/6262059/

CHAPTER 3:

UNDERSTANDING AND IMPLEMENTING THE NIST CYBERSECURITY FRAMEWORK

PURPOSE OF THIS CHAPTER:

1. Identify the purpose of the National Institute of Standards ("NIST") Cybersecurity Framework.[1]
2. Identify the components of the NIST Cybersecurity Framework and its "Core Components."
3. Identify the reasons why adopting the NIST Cybersecurity Framework may benefit companies and their boards of directors.
4. Identify why using the NIST cybersecurity framework risk assessment will be beneficial to your company or business.

> "The NIST Cybersecurity Framework represents a tipping point in the evolution of cybersecurity, one that emphasizes and encourages a proactive risk-management approach that builds on standards and compliance…. "While the framework is voluntary, we believe that organizations — across industries — should adopt the guidelines as a key tool to manage and mitigate cyber risk to their business, in combination with other risk-management tools and processes such as cyber insurance."[2]

We had hoped we wouldn't have to include this chapter in Book Two. We had hoped we were so convincing the first time around that many of you would have decided to adopt the NIST Cybersecurity Framework hook, line, and sinker last year. We had hoped to get most of you landed on the cybersecurity life raft we are constructing, even though space is limited and is being filled quickly.

Well, we were partially right. In the year since we wrote our book, uptake on the Framework has been noteworthy, though not all of those right minded ladies and gentlemen have actually adopted the whole thing in real life. In one recent publicly available survey, the data "reveals that 70% of organizations view NIST's framework as a security best practice…"[3] The problem is cost: "Fifty-percent see the high level of investment that it requires as a barrier to adoption [though] [t]he NIST framework was the most popular choice of security frameworks to be implemented over the next year."[4] According to the same survey, "Twenty-nine percent of organizations leverage the NIST Cybersecurity Framework ("CSF") and overall security confidence is higher for those using this framework."[5] The survey concludes:

> While the survey indicates larger organizations (5,000 employees or more) are more likely to adopt the NIST CSF (37%), 17% of smaller organizations surveyed (100 to 1,000 employees) also rely on this framework to maintain their security posture. Larger organizations may be more likely to have a security framework in place if they have more staff and a bigger budget to secure a larger network.[6]

BACKGROUND

To combat these increasing and serious cybersecurity issues, the president on February 12, 2013 issued Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity."[7] The EO directed NIST, in cooperation with the private sector, to develop and issue a voluntary, risk-based Cybersecurity Framework that would provide U.S. critical infrastructure organizations with a set of industry standards and best practices to help manage cybersecurity risks.

In February 2014, through a series of workshops held throughout the country and with industry input, NIST released the "Framework for Improving Critical Infrastructure Cybersecurity" ("the Framework").[8] For the first time, the Framework provides industry with a risk-based approach for developing and improving cybersecurity programs. It also provides a common language regarding cybersecurity issues, allowing important discussions to take place between an organization's "IT" people and its "business" people, some of whom may cringe when hearing complicated terms like "APT" ("Advanced Persistent Threat"). The common sense, "English language" approach allows an organization and its directors to both identify and improve upon their current cybersecurity procedures. Though the Framework was developed for the 16 critical infrastructure sectors, it is applicable to all companies — albeit, at least today, on a voluntary basis.[9]

Without question, the Framework is not the only "standard" that exists right now for "best practices" in data security. ISO 27001 ("ISO") is an international standard that describes a "best practices" approach for information security management. Like the Framework, ISO provides a holistic, system-wide approach to information security that encompasses people, processes, and technology. And since it has been in the public domain for a longer period of time, many organizations have already adopted ISO.

For ease of reference, as the Framework incorporates by reference many of the ISO standards, we are going to refer mostly to the Framework in this section so there is no duplication of effort. The point of this chapter is not to discourage an organization from adopting *either* the Framework or ISO. The point is to emphasize the importance of a company or organization adopting *some* recognized standard for information management security based upon its own particular risk profile. The company or organization can point to such adoption, along with accompanying written policies and procedures implementing it, as evidence not only of compliance for regulatory purposes,[10] but also to demonstrate to regulators, the plaintiffs' class action bar, customers, and other third parties that it is paying attention to "best practices" in cybersecurity.

We also draw attention to a document that has not received a lot of airtime: the NIST cybersecurity risk assessment template, which overlays the Framework and adds a process for assigning risk value to certain core functions. This document is incredibly helpful because it is a starting point for determining, assessing, and then mitigating cybersecurity risk based upon an organization's own cybersecurity risk (not someone else's assessment, and not someone else's company). We like the risk assessment document a lot. Not because we wrote it. We didn't. We like it because it allows for discussions around cybersecurity risk that all stakeholders can take part in, from the most tech savvy to those executives still afraid to update iOS on their iPads.

WHAT IS THE CYBERSECURITY FRAMEWORK?

The Framework contains three primary components: The Core, Implementation Tiers, and Framework Profiles.

FRAMEWORK IMPLEMENTATION TIERS EXPLAINED

TIER 1 (PARTIAL): Here, the Organization's cyber risk management profiles are not formalized, and are managed on an ad hoc basis. There is a limited awareness of the Organization's cyber security risk at the Organization level, and an Organization-wide approach to managing cyber security risk has not been established.

TIER 2 (RISK INFORMED): Unlike Tier 1, Tier 2 Organizations establish a cyber risk management policy that is directly approved by senior management (though not yet on an Organization wide basis). There is some effort by senior management to establish risk management objectives related to cybersecurity, to understand the Organization's threat environment, and to implement cyber security procedures with adequate resources.

TIER 3 (REPEATABLE): Here, the organization is running with formal cyber security procedures, which are regularly updated based upon changes in risk management processes, business requirements, and a changing threat and technology landscape. Cyber-related personnel are well-trained and can adequately perform their duties. The Organization also understands its dependencies and business partners, and receives information from them which allows for collaboration and risk-based management decisions.

TIER 4 (ADAPTIVE): Here, the Organization adapts its cybersecurity practices "in real time" based upon lessons learned and predicative indicators derived from previous and current cyber security activities. Through a process of continuous improvement incorporating advanced cyber security technologies, real time collaboration with partners, and "continuous monitoring" of activities on their systems, the Organization's cyber security practices can rapidly respond to sophisticated threats.

The Framework Core

The Framework Core ("Core") is a set of cybersecurity activities and applicable references established through five concurrent and continuous functions – Identify, Protect, Detect, Respond and Recover – that provide a strategic view of the lifecycle of an organization's management of cybersecurity risk. Each of the Core Functions is further divided into Categories tied to programmatic needs and particular activities. The outcomes of activities point to informative references, which are specific sections of standards, guidelines, and practices that illustrate a method to achieve the outcomes associated with each subcategory. The Core principles can be thought of as the Framework's fundamental "cornerstone" for how an organization should be viewing its cybersecurity practices: (1) identifying its most critical intellectual property and assets; (2) developing and implementing procedures to protect them; (3) having both sufficient human and IT resources in place to timely identify a cybersecurity breach; and (4) having procedures in place to both respond to and (5) recover from a breach, if and when one occurs.

Now, the knee-jerk response to our explanation of the Core may be, "Oh, well, we do this already," or, "We had this discussion last year." Our response, very simply, is that cybersecurity is a living, breathing holistic concept for three main reasons:

1. Business processes change (and so do business practices) — Our best examples here are two of the most important discussions in this book: Big Data Analytics and the cloud. All three of these reasons hinge upon the accessibility and collection of data from many different systems and endpoints, and the security of data the company is collecting. As we discuss later in the book, we are collecting enormous amounts of data each business day. What is your plan for how to use this data, where do you store this data, and how long should you keep the data before it become stale? When is it safe to purge data from your storage facility? The "Identify" and "Protect" Elements of the Core allow a discussion around big data to occur not just yearly, but "as needed" as the methods and means of using and crunching big data are changing constantly.

2. Good cybersecurity must be instilled into a corporate culture by awareness, compliance, and employee training. What was OK last year, or even six months ago, might not be OK today. New business lines, methods, and processes may have incepted in the interim and created more data issues to deal with. Hackers have gotten more advanced in their threat vectors. Similarly each year firewalls, and data intrusion and incident response hardware get more advanced. Many now contain elements of AI, machine learning, deep learning, or cognitive computing. Good data security is not merely taken in snapshots every year. It is more like one continuous movie stream, where each frame shows a different picture at any given point in time. At least at the CIO or CISO level, data and information security discussions must happen frequently and be documented so as to be true to the principles contained in the Framework's Core, so that relevant information can be transmitted upstream to senior management and the board of directors.

3. Finally, we note that even the "Respond" element of the Framework continues to warrant discussion. Where two years ago most companies relied upon human incident responders to review all alerts based upon severity, cybersecurity hardware has changed dramatically, creating the genre of "cybersecurity automation and orchestration," where advanced hardware (taking its cue from sensors, machine learning, and its cousin, Deep Learning) is helping incident responders deal with the plethora of events and Alerts they get daily by separating false positives from real actionable alerts. Nothing stays the same in cybersecurity. That truly is the value of the Framework: keeping up with the Joneses, your own business people, and your tech.

THE "IDENTIFY" ELEMENT

At "the core" of the Framework's Core are discussions concerning what the organization's most important IP assets are. This is really one area that does not get enough attention in our view because not all information has the same significance to a corporation. To some companies, customer and credit card information is the key. For others, personally identifiable healthcare information is critical. And to others, it might be the plans to a new fighter plane or nuclear battleship. Without identifying these critical assets, it would be difficult if not impossible to determine:

1. What level of security to apply to each category of informational assets simply put, some categories of data are more valuable to your business then others.;

2. How and where to store back up copies of such data if you need to immediately invoke your business continuity plan; and

3. What categories of data, if stolen, lost or encrypted in a ransomware attack, would cause catastrophic suffering to your business, customers and stakeholders.

4. What data can be stored in the cloud; and what data must be stored on premises?

For the mission critical data (say e.g. the plans to the new F-40 advanced stealth fighter drone), more specific and severe strategies might be needed to make security for such data the equivalent of Fort Knox. Without identifying your critical information data sets, the allocation of security assets and resources to protect such assets will potentially turn into a fruitless exercise with no residual benefits to the organization. And today, with the construction of data lakes (i.e. "pools" of data that big data analytics are performed on), identifying the type of data you use, hold and store has never been more important. One excellent word of advice from a friend: "protect the most which matters the most."

PROTECTION

Now for a few words about the "protection" aspect of the Framework's Core. Previously, we mentioned this concept in connection with explaining the various pieces of a network server cybersecurity system, including hardware, software, and the new, next "best black box" that vendors urge upon organizations on every sales call. The point here, in today's cybersecurity ecosystem, is that cybersecurity "defensive" hardware is constantly changing to adapt to the hackers' next best threat vector. Though a CISO may say, "Everything is just fine," boards of directors must be asking in return, "Is there anything new out there we need to have?" or more simply put, "what can we be doing better?" The Framework provides the template and method-ology to have such discussions.

For instance, many companies, and even some portions of the U.S. government today, rely on signature-based intrusion detection systems, meaning they only attempt to block "known threat signatures." This would be akin to a firewall on steroids. What happens if the hacker uses a new variant of malware specifically designed to have no known threat signature, or one designed to evade current sandboxing technology?[11] In Chapter 6, we also note the plethora of AI and Machine Learning driven cybersecurity defensive technologies that have hit the market in the last six months. Boards must ask the hard questions in order to answer the simpler one, to wit, "Are we OK with what we have, or should we attempt to step up our game and be better than the average company?" The answer [hopefully] should be the latter. Low hanging fruit gets picked first. You don't want to be the low hanging fruit when the hackers climb over the orchard fence or the last runner in the pack of IT executives being chased by the Fancy Bear. Getting bitten is no fun, especially if the bite is life or company threatening.

DO WE HAVE ENOUGH HUMANS IN OUR IT DEPARTMENT?

Funny question, but not so much. Though we did not ask this question in Book One, it is front and center in Book Two because we are simply not educating and training enough people to fill even half of the cybersecurity jobs that exist in the United States. Why? That's a hard question to answer, but my educated guess is that the cybersecurity job shortage took us by surprise. Or perhaps it was complacency. Or both. Up until the Target breach, I could bet you a quarter that you would not find one cybersecurity story a day in the press: print or business media. Today, the number of articles, white papers, and presentations that get published every day is absolutely astounding. No human could keep up. We are now playing catchup in our high schools, universities, and business schools trying to educate cybersecurity professionals. This problem is not going away anytime soon.

But it is an important question for boards to ask because despite exponential gains in cybersecurity technology and hardware over the past year, most if not all security hardware needs human intervention, and human input. There are simply some blended threats that are very complex,

requiring a sharp, trained professional to discern whether it is merely a DDoS attack or if someone is also, at the same time, trying to steal data. Tech helps, but it's not the cure.[13] People are.

RECOVERY

The recovery aspect of the Framework's Core has been mentioned a few times already before, (and is mentioned a lot more in Book Two). Aside from the importance of an incident response plan, it is critical that companies have an information management business continuity plan ("BCP"). Not unlike the plan a major corporation along the Gulf of Mexico might have in the event of a hurricane, a BCP is designed so that a corporation can recover from a major loss of data. Think Saudi Aramco. Think Sony Pictures. Think "the dark ages" where business was done with typewriters and fax machines. Think "ransomware" leaving a hospital without scanners or CT scanners or MRIs or bar codes. And patients waiting to be operated on without their doctor's having access to their medical records. The corporation, company, or hospital should have a regular backup plan for data that it creates daily and weekly, and should keep that data ideally off premises (or even in the cloud). Many cloud service providers, too, have their own backup plans if for some reason access to their services is denied or unavailable. Unlike the 1930's, data is the lifeblood of most corporations. It needs to be ready to be restored or recovered to the mainframe instantaneously in the event network servers suffer catastrophic damage. Along with incident response plans, information management business continuity plans should be practiced quarterly, with a full "cut-over" to the backup material done in order to evidence the resiliency of an organization to even the worst cyber breach.

The Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") describe the level of sophistication and rigor an organization employs when applying its cybersecurity practices, and provide a context for applying the Core Functions. Consisting of four levels, from "Partial" (Tier 1) to "Adaptive" (Tier 4), the tiers describe approaches to cybersecurity risk management that range from "informal, reactive responses to agile and risk-informed." Think of the tiers as a "self-assessment" that takes place at the time the NIST Framework is adopted. When the directors and officers are meeting for the first or second time to go through the Framework, the organization might be a Tier 1 or Tier 2. The goal for any organization obviously is not to remain static in its cybersecurity practices, because, simply put, as the hackers get progressively better in their intrusion methods, the organization can fall even further behind the cybersecurity eight ball. A Tier 1 should strive to be a Tier 2. A Tier 2 should strive to be a Tier 3, and so on.

I am sure you noticed there is not a lot of "rah rah" here regarding the implementation tiers. Why? Well, they are really up to you and your company. They are a classic business judgment. For some companies, cybersecurity might not rank in the top 5 of important things to consider. For Intel, cybersecurity might rank in the top two.[14] But what we will say is that showing progression through the tiers, even in small, measured bites, arguably shows continuing attention to cybersecurity principles in general, and more specifically a desire to attain the highest cybersecurity standard possible (evidence of this might be especially useful if the company is later sued as a result of a data breach or investigated by the FTC).[15] Showing no attention means, well, showing no attention. That would not look good post-breach.

The Framework Profile

The Framework Profile ("Profile") is a tool that provides organizations a method for storing information regarding their cybersecurity program. A Profile allows organizations to clearly articulate

the goals of their cybersecurity program. The Framework is risk-based; therefore the controls, and the process for their implementation, change as the organization's risk changes. Building upon the Core and the tiers, a comparison of the Profiles (i.e. Current Profile versus Target Profile) allows for the identification of desired cybersecurity outcomes and gaps in existing cybersecurity procedures. Attention can then be focused on allocating time, resources, and people to close the gaps.

WHAT IS THE RELATIONSHIP BETWEEN THE FRAMEWORK AND NIST'S GUIDE FOR APPLYING THE RISK MANAGEMENT FRAMEWORK ("RISK ASSESSMENT GUIDE") TO FEDERAL INFORMATION SYSTEMS (SP 800-30 REV 1)?

Good question. Sort of like the relationship between peanut butter and jelly. If the Framework is the jelly, the Risk Assessment Guide is the peanut butter. We will not go too far into the Risk Assessment Guide here, save for a few sentences because, in sum, it only applies to federal agencies bound by Executive Order to apply the Framework to their Critical Infrastructure. If they are bound to apply the Framework, they are bound to apply the Risk Assessment Guide.[16]

But we are mentioning it here because it is very good. In a non-technical way, it walks an organization and its senior executives through the cybersecurity threats and vulnerabilities they face daily, along with identifying both the organization's most critical IT and IP assets, and the biggest risks, threats, and vulnerabilities it faces. Next, the organization assesses what compensating controls and other procedures it already has in place to reduce or eliminate the potential threat, risk, or vulnerability. The organization and its executives are next required to assess the likelihood of the risk happening to the network, and the likely impact. Using new math, the Risk Assessment puts numbers behind the risks and the impacts of breaches on an organization, from minimal to severe.[17] The Risk Assessment Guide is company-neutral, meaning what might be a high risk to a small company would be a low risk to a high-end company with a lot of compensating controls.

So, you say, why is the Risk Assessment Guide so important? Because at the end of the day it allows an organization to prioritize its risks, vulnerabilities, and threats, and allows it to then spend its budget dollars wisely where the impact of a cybersecurity breach is the greatest. It is like the Framework on steroids. The Risk Assessment is very useful when used more than once a year because cybersecurity is not static, and what might be a low risk item one quarter could be a high risk item at year end. But please don't get the impression that the Risk Assessment Guide is the beginning and the end. It is just a guide. Whether you use the Risk Assessment Guide, or decide to otherwise wing it, is completely up to you and your organization.

WHY DIRECTORS SHOULD CARE ABOUT THE FRAMEWORK

> "Our critical infrastructure networks are extremely vulnerable to such a damaging attack, and we can't count on deterrence if we're already in a shooting war with a nation like China or Russia…. It's not hard to understand how difficult it would be if the power or water was shut off, but imagine if one of our adversaries were able to shutdown key American financial transactions. Our economy would grind to a halt." -Rep. Mike Rogers, (R.-Mich.), chairman of House Intelligence Committee.[18]

When the Framework was originally announced, Tom Wheeler, Chariman of the Federal Communications Council ("FCC"), stated that an industry-driven cybersecurity model is preferred over prescriptive regulatory approaches from the federal government.[19] Nonetheless, we continue

to see, almost daily, successful attacks on critical infrastructure organizations like financial institutions, major corporations, and the healthcare sector.

As we noted above, the NIST Framework is not the only risk-based cybersecurity framework in existence. For U.S. financial institutions, an important framework to consider is the one put out by the The Federal Financial Institutions Examination Council ("FFIEC"), which is essentially the governing body that "prescribes uniform principles, standards, and report forms for the federal examination of financial institutions by the board of governors of the Federal Reserve System ("FRB"), the Federal Deposit Insurance Corporation ("FDIC"), the National Credit Union Administration ("NCUA"), the Office of the Comptroller of the Currency ("OCC"), and the Consumer Financial Protection Bureau ("CFPB") and to make recommendations to promote uniformity in the supervision of financial institutions."[20] As of June 2015, these uniform principles and standards now include standards and principles for cybersecurity as well. We are not going to do a deep dive into the FFIEC framework in any detail because is mostly derived from the NIST Framework.[21]

At some point, if critical infrastructure organizations do not demonstrate that a voluntary program can provide cybersecurity standards that are the same as, if not better than, federal regulations, regulators will likely step in with new measures. In fact, according to former SEC Commissioner Luis Aguilar, the Framework has already been suggested as a potential "baseline for best practices by companies, including in assessing legal or regulatory exposure to these issues or for insurance purposes. At a minimum, boards should work with management to assess their corporate policies to ensure how they match up to the Framework's guidelines — and whether more may be needed."[22] If the SEC OCIE guidance, or other proposed federal regulation of cybersecurity, becomes a reality, implementing the Framework could be a mandatory exercise.

In addition to staying ahead of federal and state regulators and potential Congressional legislation, the Framework provides organizations with a number of other benefits, all of which support a stronger cybersecurity posture for the organization. These benefits include a common language, collaboration opportunities, the ability to verifiably demonstrate due care by adopting the Framework, ease in maintaining compliance, the ability to secure the supply chain, and improved cost efficiency in cybersecurity spending. Though it would be Herculean to accurately summarize all benefits of the Framework and how to implement them, we stress its key points below.

Common Language

The Framework, for the first time, provides a common language to standardize the approach for addressing cybersecurity concerns. As we have noted a few times in other chapters, many cybersecurity principles are not intuitive. They are not based upon well-established principles that directors (especially audit committee members) are used to hearing, like "revenue recognition." The Framework allows for cybersecurity programs to be established and shared within an organization and with organizational partners using a common, easy-to-understand language. For example, the Framework allows for the creation of several types of Profiles: Profiles that provide strategic enterprise views of a cybersecurity program, Profiles that are focused on a specific business unit and its security, and Profiles that describe technologies and processes used to protect a particular system. Despite the number of Profiles that may exist for an organization, directors can quickly and easily understand how corporate guidance is implemented in each Profile since they have a standard language and format for describing an organization's cybersecurity programs.

Collaboration

NIST and participants from industry that assisted in the Framework development envision the

Framework Profiles as a way for organizations to share best practices and lessons learned. By leveraging the common language and increased community awareness established through the Framework, organizations can collaborate with others through programs such as the Cybersecurity Forum ("CForum").[23] CForum provides an online forum for organizations to share lessons learned, post questions regarding their cybersecurity challenges, and maintain the conversation to continually improve cybersecurity capabilities and standards.

Demonstrating Due Care

By choosing to implement the Framework (or some part of it) sooner rather than later, organizations can potentially avoid the inevitable conclusion (or parallel accusation by a plaintiff's attorney) following disclosure of a cyber breach that they were "negligent" or "inattentive" to cybersecurity best practices. Indeed, a recent NYSE board survey made the following statement:

> "Overall, industry data shows global cyber risk is growing both in scope and severity, yet the survey demonstrates that in practice, boards are not always addressing it as a top priority. Indeed, when asked how often the board discusses topics related to risk and enterprise value, 42% admitted their board only occasionally discusses cyber/ IT security (Figure 6)."[24]

FIGURE 6

How often does your board discuss the following topics to oversee risk and enhance enterprise value?

	Regularly	Occasionally	Never
Cyber/IT security	54.85%	41.75%	3.4%
Emerging technologies	35.44%	54.37%	10.19%
Post-merger transaction integration	46.19%	36.55%	17.26%
Operational technology	53.40%	42.72%	3.88%
Compliance systems	71.84%	26.21%	1.94%
Social media	16.99%	65.63%	17.48%

Source: NYSE Board Survey

These figures from the NYSE survey are discouraging at best, and will potentially serve as fodder for future shareholder derivative lawsuits if they remain constant. Organizations using the Framework as a common language for board discussions should be more easily able to demonstrate their due care in the event of a cyber attack by providing key stakeholders with information regarding their cybersecurity program via their Framework Profile and the active steps the company took to elevate that Profile to a higher level. At the same time, directors can point to their request that the organization consider implementing the Framework (or using it as guidance) in defense of any claim that they breached their fiduciary duties by failing to oversee the cybersecurity risk inherent in their organization.

Maintaining Compliance

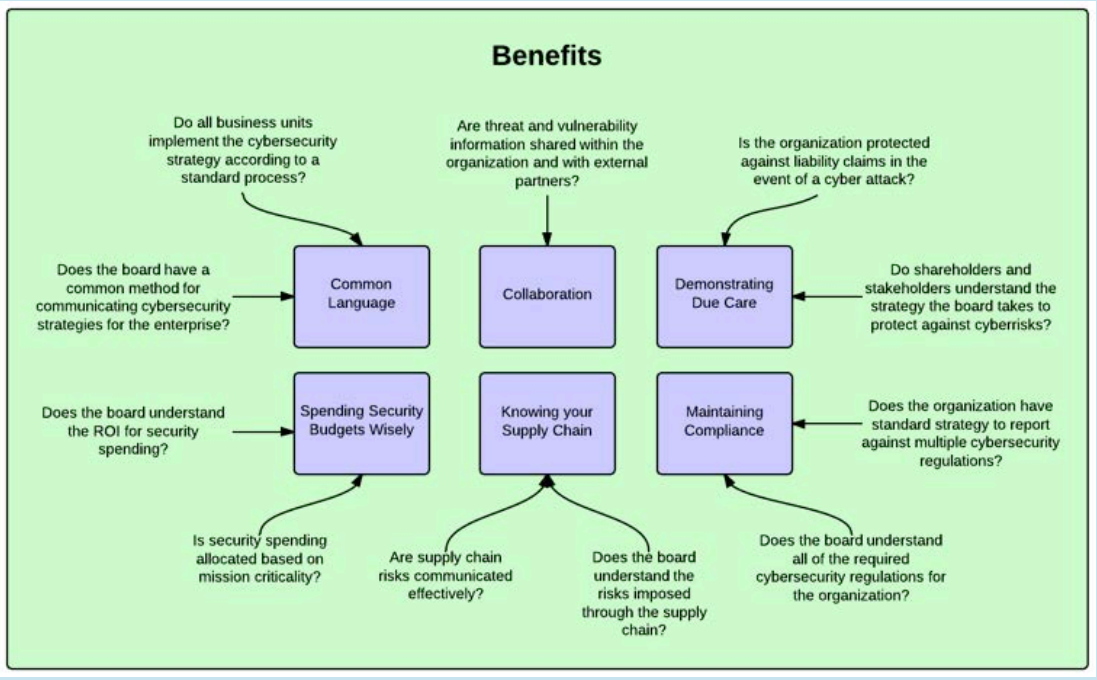
Many critical infrastructure organizations (e.g. financial institutions) must comply with multiple regulations with overlapping and conflicting requirements. In order to avoid fines and additional fees from regulatory bodies, many operators are forced to maintain multiple compliance documents describing how the organization complies with each requirement. The standard developed by the Framework enables auditors to evaluate cybersecurity programs and controls in a single format, eliminating the need for multiple security compliance documents.

Knowing Your Supply Chain/Good Vendor Management Practices

The Framework also provides an opportunity for organizations to better understand the cybersecurity risks imposed through their supply chains. Chinks in the armor of major corporations' vendors have proved catastrophic to at least two major retailers this year alone. Organizations purchasing IT equipment or services can request a Framework Profile, providing the buying organization an opportunity to determine whether the supplier has the proper security protections in place. Alternatively, the buying organization can provide a Framework Profile to the supplier or vendor to define mandatory protections that must be implemented by the service provider's organization before it is granted access to the buying organization's systems.

Spending Security Budgets Wisely

In an environment where cyber threat information is not readily available, organizations struggle with understanding how much security is enough security, leading to organizations implementing unnecessary cybersecurity protections. Through the use of the Framework, standards for care can be established for each critical infrastructure sector. Organizations can leverage these standards to determine the appropriate level of security protections required, ensuring efficient utilization of security budgets.



The diagram above provides questions to help determine if and how an organization can benefit from implementing the Framework. Discussing these questions and their responses will help organizations determine how well their current cybersecurity efforts are protecting them against cyber attacks. Based on the answers to these questions, they will better understand which of the benefits presented in this article will apply to their organization should they implement the Framework.

WHERE DO YOU START WITH IMPLEMENTING THE FRAMEWORK? WITH DISCUSSION AND ACTION STEPS!

A major challenge in adopting the Framework is simply getting started. Yes, the Framework (when drilled down into) can be a large task and take hundreds of hours to implement. And yes, we know there are 20 allegedly more important things on the board of director's quarterly meeting calendar than taking two or three hours to talk about the Framework.

We cannot make this judgment for you. But with 20 years experience of being corporate counselors and practitioners, we can only tell you one thing: the feeling you get when you walk onto the corporate campus for the first time after receiving the phone call that "something really bad happened" is not fun. You walk into the corporate offices and the employees are shocked and sometimes panicked with the inability to conduct their affairs. They might have even lost thousands when the company's stock price fell after the announcement of the bad news, and thus their pension plans dropped off a cliff. If you thought the employees were in bad shape, the first time you walk into the general counsel's office or CEO's office, you truly get the sense that they are not only upset, but panicked and maybe even guilt ridden for not paying enough attention to the situation before it happened. That look in their eyes is as if someone died. It is awful. And you imagine to yourself, "What if someone in the company had looked at the Framework six months or one year ago?" What a waste.

That is why we urge you to spend the time to adopt the Framework. Some organizations, maybe those in Implementation Tier 1, may have limited resources and familiarity with the Framework (or the ISO 27001 standard), and how it could help them leverage their existing cybersecurity, compliance, and audit programs, policies, and processes. But coming to grips with the Framework is certainly worth the effort and expense for any organization, especially when considering that a major cybersecurity breach could conceivably wipe out the entire organization.

At a minimum, directors and their management should become familiar with the Framework. First up on the discussion table is "Identify and Protect." Ask the officers and directors to answer those questions right off the bat. That is the easiest place to start because the directors and officers can honestly be involved in the discussion and participate. The NIST Framework pays benefits if and when it is adopted. The NIST Framework pays tremendous benefits when the directors and corporate executives lead and personalize the discussion. Then hit on the last two items: does the company have an incident response, business continuity, and crisis communications plan? Those are also easy for directors to understand, and those plans may already exist in different forms for other corporate catastrophes, like fire or hurricanes.

Additionally, directors (or some committee thereof) should have a deep discussion with management about the organization's Implementation Tiers. The Implementation Tiers allow an organization to both consider its current cyber risk management practices, the present threat environment, legal and regulatory requirements (e.g., those imposed by the SEC, FINRA, FTC, FFIEC, GLBA or HIPPA), business/mission objectives, and organizational constraints, and set a goal to ascend to a higher Implementation Tier.

Educating managers and staff on the Framework to ensure everyone in the organization is on the same page is also an important step toward the successful implementation of a robust cybersecurity program. The previously mentioned Forum is a source for success stories, lessons learned, questions, and information useful to organizations implementing the Framework. This information about existing Framework Implementations may help organizations with their own approaches. Additionally, organizations can seek out cybersecurity service providers skilled in helping organizations with the education, awareness, and planning required to implement the Framework across an entire enterprise.

Though "voluntary," it cannot be overstated that the Framework is "a National Standard" developed with input from industry experts, collaborators, and businesses (and our own government) with years of cyber experience. As stated by the Chairman of the House of Intelligence, Mike Rogers, "There are two kinds of companies: those that have been hacked and those that have been hacked but don't know it yet."[25] Given that it is almost inevitable that an organization will be hacked, there will be a time and a place where it may need to demonstrate to customers, investors, regulators, and plaintiff's attorneys that it gave thought to, and implemented, cybersecurity measures in order to defend its most critical intellectual property assets, and its most critical business and customer information. Implementing the Framework will not only allow organizations to improve cybersecurity measures, but also to effectively demonstrate due care when it comes to protecting its most valuable data and IP assets.

ENDNOTES:

[1] Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. inno-vation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

[2] See "Getting Inside the Insider Threat," found at http://www.nxtbook.com/nxtbooks/kmd/hst_20141011/#/44

[3] See "NIST Cybersecurity Framework Adoption Hampered By Costs, Survey Finds," available at http://www.darkreading.com/attacks-breaches/nist-cybersecurity-framework-adoption-hampered-by-costs-survey-finds/d/d-id/1324901

[4] ID.

[5] See "NIST Cybersecurity Framework Adoption on the Rise," available at https://www.tenable.com/blog/nist-cybersecurity-framework-adoption-on-the-rise.

[6] Id.

[7] Executive Order 13636 of February 12, 2013, *Improving critical Infrastructure Cybersecurity*, available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[8] The National Institute of Technology and Standards (NIST) "Framework for Improving Critical Infrastructure Cy-bersecurity version 1.0", February 12, 2014,available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[9] G2, Inc. was engaged by the National Institute of Standards and Technology (NIST) as the prime contractor to assist in the development of the Framework for Improving Critical Infrastructure Cybersecurity. We thank Tom Conkle, a former Commercial Cybersecurity Lead at G2, Inc. for his assistance with this Chapter.

[10] Indeed, regulatory guidance issued by the SEC's Office of Compliance, Inspections and Examination requests information from regulated entities as to whether they have adopted "any published cybersecurity risk management process standards, such as those issued by the National Institute of Standards and Technology (NIST) or the Interna-tional Organization for Standardization (ISO)." See also, "3 ways healthcare CIOs can avoid an FTC lawsuit over security," available at http://www.fiercehealthit.com/story/3-ways-healthcare-cios-can-avoid-ftc-lawsuit-over-security/2015-09-01 (noting that "Having [NIST cyber security framework] in place is one way a CIO can show the FTC that the company took serious steps to keep data safe.").

[11] See "Data explosion offers challenges, opportunities to security pros," available at http://www.csoonline.com/article/2949007/data-protection/data-explosion-offers-challenges-opportunities-to-security-pros.html (noting that "[Many] cybercriminals have learned how to evade traditional approaches that use standard rules, signatures and sandboxing.")

[12] See, e.g., "FireEye Adaptive Defense," available at https://www.fireeye.com/products/fireeye-adaptive-defense-cyber-security.html.

[13] One idea that has gotten a lot of air time is Security as a Service or "SECaaS." Security as a Service is a new method of managed services where a large security company offers to provide its own security services and sensors within the Company's corporate network infrastrcture and manage those services as if they were the Company. This is an incredibly effective was for many companies to secure themeselves without the need to buy millions of dollars of security hardware. SECaaS has been used by many small and large companies very effectively and certainly must be considered an option for companies that do not have sufficient IT staff.

[14] See "Intel comments in response to NIST's Solicitation for Comments on 'Views on the Framework for Improving Critical Infrastructure Cybersecurity,'" available at http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160218_Intel.pdf.

[15] See "How FTC Data Security Aligns with NIST Cybersecurity Framework," available at http://healthitsecurity.com/news/how-ftc-data-security-aligns-with-nist-cybersecurity-framework (""By identifying different risk management practices and defining different levels of imple-mentation, the NIST Framework takes a similar approach to the FTC's long-standing Section 5 enforcement,).

[16] The NIST Risk Assessment Guide can be found at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf).

[17] See NIST Risk Assessment Guide, available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf)

[18] See "US Cybersecurity Practices Fail to Keep Pace with Cyber Adversaries," found at http://www.hstoday.us/channels/dhs/single-article-page/us-cybersecurity-practices-fail-to-keep-pace-with-cyber-adversaries.html.

[19] (Sarkar, 2014), available at http://www.fiercegovernmentit.com/story/fcc-chairman-pitches-new-industry-driven-regulatory-model-enhance-cybersecu/2014-06-13.

[20] See "About the FFIEC," available at https://www.ffiec.gov/about.htm.

[21] Obviously if you are a bank or financial institution should review the FFIEC Framework in detail to make sure that your organization is com-plaint with any specific provision of the FFIEC Framework that is not included in the NIST Framework.

[22] See "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," available at http://www.sec.gov/News/Speech/Detail/Speech/1370542057946 ; It has also been discussed that the Framework may be used by other countries who are mindful of the need for great global alignment with respect to cybersecuriy issues and standards. See "The Global Update of the NIST Cybersecurity Framework," available at https://www.crowell.com/files/20160215-The-Global-Uptake-of-the-NIST-Cybersecurity-Framework-Wolff-Lerner-Miller-Welling-Hoff.pdf.

[23] The Cybersecurity Forum (CForum) is a not-for-profit, publically available site dedicated to the evolution and implementation of the Cybersecurity Framework, available at http://Cyber.securityFramework.org.

[24] See "Managing Cyber Risk: Are Companies Safeguarding Their Assets?" available at https://www.nyse.com/corporate-services/nysegs/CBM_1Q15_Special_Report.

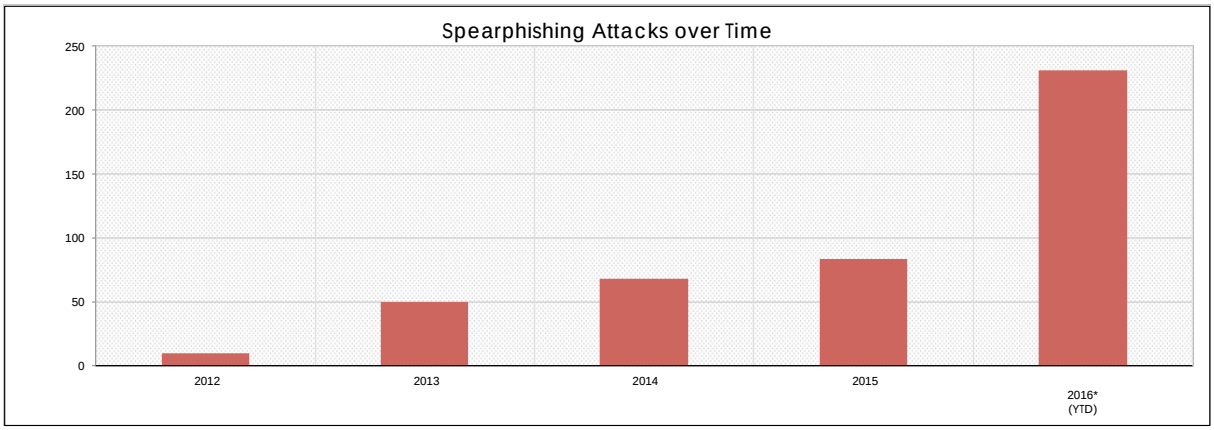
[25] Graham, Scott, Interview: Greg Toughill, DHS, USA on Cybersecurity, July 28, 2014, available at http://www.globalgovernmentforum.com/brigadier-general-greg-touhill-cybersecurity-department-of-homeland-security-interview/,.

CHAPTER 4:

SPEARPHISHING ATTACKS – DON'T TAKE THE BAIT! DON'T CLICK ON THE LINK![1]

PURPOSE OF THIS CHAPTER:

1. Identify the nature and identity of social media scams;
2. Identify the nature and identity of various spearphishing and related email scams;
3. Identify proactive steps that a company may take to attempt to defeat spear-phishing and email-related scams through employee awareness and automated training



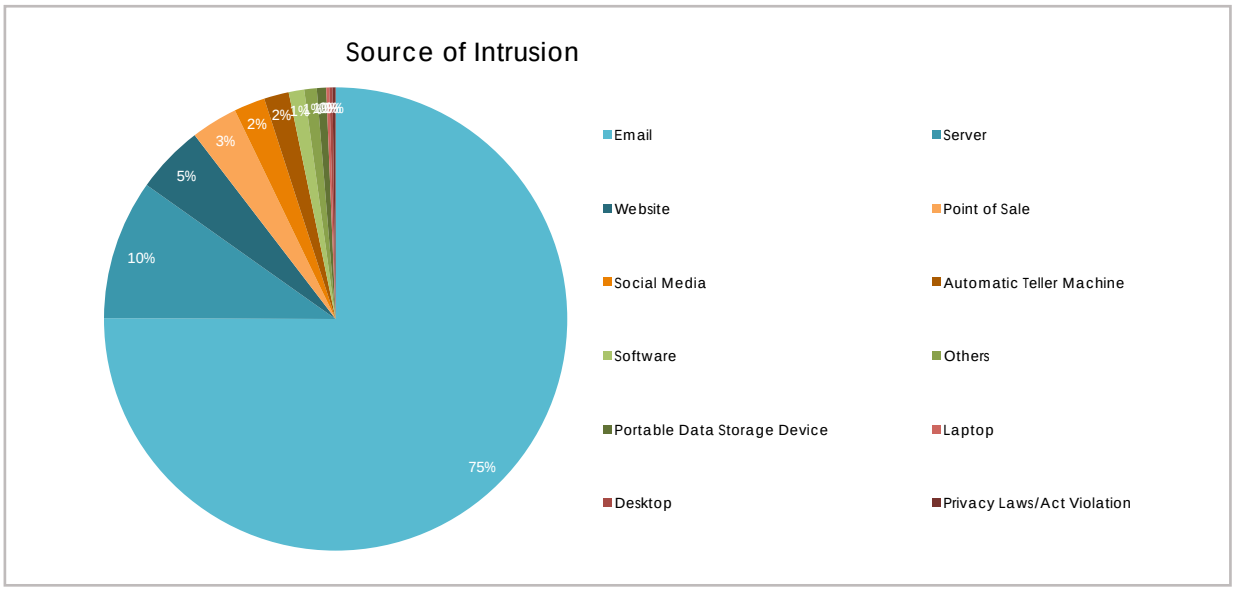
It seems that just like in old times (in cyberspace that means last year) the existence of "snake-oil" salesmen[1] on the Internet is getting worse, not better. Rather than selling something medicinal or at the very least useful, these snake-oil salesmen of today have only one intent: to steal your personal information or worse, to distribute malware to your computer.[2] One recent FireEye report noted the following:

> 84% of organizations said a spear-phishing attack successfully penetrated their organization in 2015. The average impact of a successful spear-phishing attack: $1.6 million. Victims saw their stock prices drop 15%.[3]

The 2016 Verizon Data Breach Investigations Report gave similar ominous statistics:

> In this year's dataset, 30% of phishing messages were opened by the target across all campaigns. But wait, there's more! About 12% went on to click the malicious attachment or link and thus enabled the attack to succeed. That indicates a significant rise from last year's report in the number of folks who opened the email (23% in the 2014 dataset) and a minimal increase in the number who clicked on the attachment (11% in the 2014 dataset).[4]

Why do people continue despite training, educational efforts and online training still want to click on the link? As FireEye puts it, because these emails are believable. "People open 3% of their spam and 70% of spear-phishing attempts. And 50% of those who open the spear-phishing emails click on the links within the email—compared to 5% for mass mailings—and they click on those links within an hour of receipt. A campaign of 10 emails has a 90% chance of snaring its target."[5]



We spend this chapter discussing spearphishing attacks, not out of morbid curiosity about the utter gall of these modern day snake-oil salesmen, but to hopefully inform and prevent the inadvertent "click on the link" circumstances which you and your company would rather avoid. And this threat is really hard to avoid. The Verizon Data Breach Investigations Reports also notes the following about an employees' propensity to click on the link:

> The median time for the first user of a phishing campaign to open the malicious email is 1 minute, 40 seconds. The median time to the first click on the attachment was 3 minutes, 45 seconds!

We also point to recently issued reports noting that other scams like phishing and spear phishing continue to be a bothersome and dangerous component not only of company emails, but emails sent to US government agencies, officials and employees.[6] And spear phishing attempts by nation-states, cyber criminals and others will likely continue, and worsen, given the large amount of personal information already stolen by other cyber-attacks. This information will no doubt be used for malicious purposes, like e.g. the Ukrainian Power Grid attack in 2015 which was allegedly started by a spearphish.[7] At the end of the day, continuous and thorough employee training and awareness programs (including online training) outlining these sorts of scams must be considered an essential part of the "Holy Grail" of cybersecurity, along with certain network hardware components that can help stop "bad" emails before they get to your employees' desktops.

SOCIAL MEDIA SCAMS

"Where attacks of yesteryear might have involved a foreign prince and promises of riches through shady exchanges of currency,…today's phishers scan social media for birthdays, job titles and anything else that can be used to create the appearance that an email request is coming from a legitimate source."[8] As the Symantec Report points out, a lot of these email scams and offers are now generated through the explosive growth of social media sites such as Facebook, Twitter, and Pinterest. Here are some of them:

- **MANUAL SHARING** – These rely on victims to actually do the work of sharing the scam by presenting them with intriguing videos, fake offers, or messages that they can then share with their friends;
- **FAKE OFFERINGS** – These scams invite social network users to join fake events or groups with incentives such as free gift cards. Joining often requires the users to share credentials with the attacker or to send a text message to a premium rate number;
- **LIKEJACKING** – Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, thereby spreading the attack;
- **FAKE APPLICATIONS** – Users are invited to subscribe to an application that appears to be integrated for use with a social network, but is not as described and may be used to steal credentials or harvest other personal data; and
- **AFFILIATE PROGRAMS** – When you click on the link, these might allow you to get a free smartphone, airline ticket, expensive vacation or gift card to your favorite store. Especially when you did not initiate any activity to receive one of these fine offers. Caveat emptor: Nothing in life is free, especially when malware is attached thereto.

PHISHING ATTACKS – EMAIL SCAMS – EMAIL HIJACKING

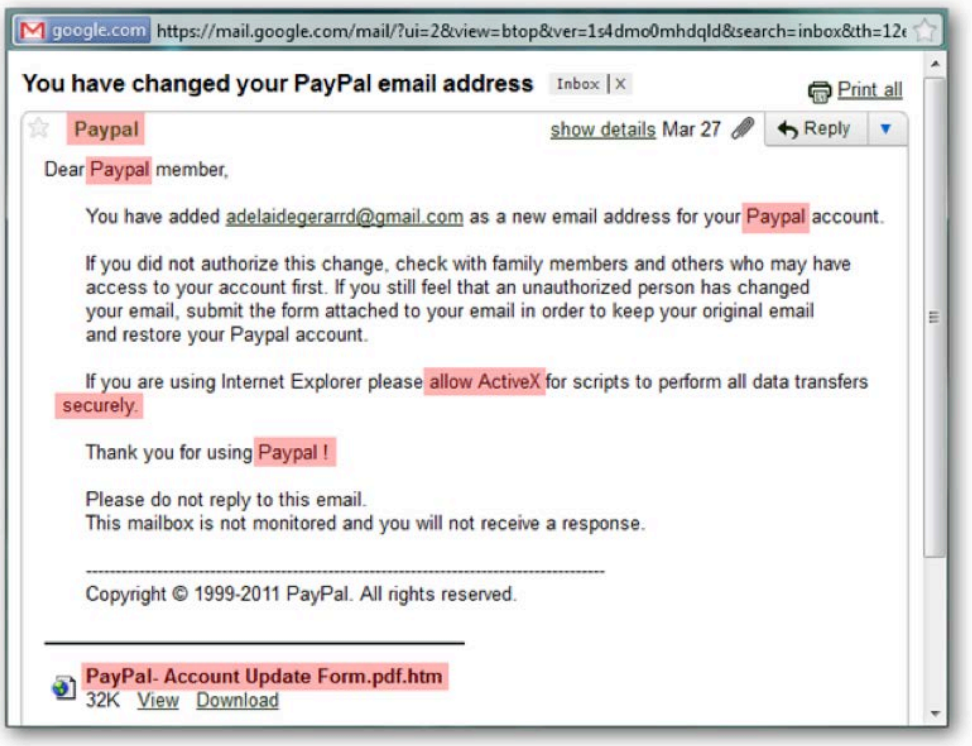
We have previously pointed out the prevalence of phishing or spear phishing attacks against U.S. public companies. As noted in the recently issued 2015 Verizon Data Breach Investigation Report,[11]

> Social engineering has a long and rich tradition outside of computer/network security, and the act of tricking an end user via e-mail has been around since AOL installation CDs were in vogue.
>
> The first "phishing" campaigns typically involved an e-mail that appeared to be coming from a bank convincing users they needed to change their passwords or provide some piece of information, like, NOW. A fake web page and users' willingness to fix the nonexistent problem led to account takeovers and fraudulent transactions.[12]

Phishing campaigns have evolved in recent years to incorporate installation of malware as the second stage of the attack. Lessons not learned from the silly pranks of yesteryear and the all-but-mandatory requirement to have e-mail services open for all users has made phishing a favorite tactic of state-sponsored threat actors and criminal organizations, all with the intent to gain an initial foothold into a network.

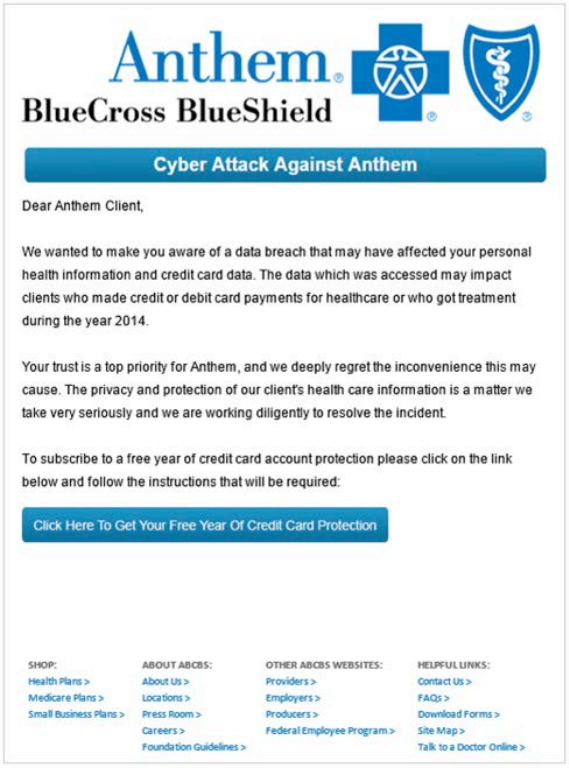
Here are some publically available examples of spear phishing emails that unfortunately had some success in tricking employees and customers to click on the link:

If you had a HSBC account, this would certainly look like a link that you should click on to keep your banking services continuous?



If you shop on Ebay and thus have a PayPal account, might you want to click on this link to make sure that an unauthorized person is not using your PayPal account?

Finally, if you had your healthcare insurance provided for by Anthem Healthcare, this link looks like "you have to" click on it to get free credit monitoring. But many probably did not know that Anthem notified its customers in writing by mail of this free credit protection offer. That is the problem with socially-engineered spearphishing. By some business, personal or emotional connection, they force you to want to click on the link to investigate further. But we urge you not to![13]


Anthem
BlueCross BlueShield

Cyber Attack Against Anthem

Dear Anthem Client,

We wanted to make you aware of a data breach that may have affected your personal health information and credit card data. The data which was accessed may impact clients who made credit or debit card payments for healthcare or who got treatment during the year 2014.

Your trust is a top priority for Anthem, and we deeply regret the inconvenience this may cause. The privacy and protection of our client's health care information is a matter we take very seriously and we are working diligently to resolve the incident.

To subscribe to a free year of credit card account protection please click on the link below and follow the instructions that will be required:

Click Here To Get Your Free Year Of Credit Card Protection

SHOP:
Health Plans >
Medicare Plans >
Small Business Plans >

ABOUT ABCBS:
About Us >
Locations >
Press Room >
Careers >
Foundation Guidelines >

OTHER ABCBS WEBSITES:
Providers >
Employers >
Producers >
Federal Employee Program >

HELPFUL LINKS:
Contact Us >
FAQs >
Download Forms >
Site Map >
Talk to a Doctor Online >

HOW DO YOU STOP MALICIOUS SOCIAL MEDIA/SPEAR PHISHING/EMAIL CAMPAIGNS

Obviously there are no good answers to these questions - especially in an era when the bad guys are sending such realistic socially engineered emails that they look like they could come from your husband, wife, son, or daughter, or your company, school or church. They are that good.

A recent, very well written Harvard Business Review article, entitled "Cybersecurity's Human Factor: Lessons from the Pentagon",[14] accurately summarizes the problem and "a" potential solution:

> Companies need to address the risk of human error too.… The exfiltration of 80 million personal records from the health insurer Anthem, in December 2014, was almost certainly the result of a "spear phishing" e-mail that compromised the credentials of a number of system administrators. These incidents underscore the fact that errors occur among both IT professionals and the broader workforce. Multiple studies show that the lion's share of attacks can be prevented simply by patching known vulnerabilities and ensuring that security configurations are correctly set.
>
> The clear lesson here is that people matter as much as, if not more than, technology. (Technology, in fact, can create a false sense of security.) Cyber defenders need to create "high-reliability organizations"—by building an exceptional culture of high performance that consistently minimizes risk. "We have to get beyond focusing on just the tech piece here," Admiral Mike Rogers, who oversees the U.S. Cyber Command, has said. "It's about ethos. It's about culture. [It's about] how you man, train, and equip your organization, how you structure it, the operational concepts that you apply.

Clearly, the human element of cybersecurity is one of the most important elements (if not the most important element) of the cybersecurity ecosystem. But what do we do with "us humans" to help us navigate such a very difficult cybersecurity environment highly charged with socially engineered spear phishing emails? Here are some points to consider:

1. **IT IS EVERYONE'S RESPONSIBILITY:** Spear phishing is a tremendous problem with no 100% solution. And its results, if successful, could be devastating, ranging from ransomware to worse effects on your company and organization. Your employees are your first line of defense in defeating spearphishing attacks. Be sure to emphasize in training that they are at

the make or break point for this vector. Whether it's their laptop, IPad or smartphone, one false move towards a link could spell doom and gloom for a company. Ask them to understand that in the overall scheme of things they are critical. They should view emails they receive with healthy skepticism, especially from senders who they don't know or where the email or advertisement they see looks off. If they didn't buy anything recently, there is no reason for "FedEx" to be sending you an email asking you to pick up a package. That package you receive will not be something good like a new watch or shirt from Vineyard Vines. It will be malware instead.

2. **ANTI-PHISHING TRAINING:** Many argue that the weakest link in cybersecurity is the person who is sitting in the chair in front of his or her computer. In a recent study, "Just 23% of respondents rated their organizations' cybersecurity education and training methods as being extremely effective. That's not an encouraging harbinger, especially when you consider that no letup is in sight.[15] And no let up in sight to the continuing ransomware plague.

As such, we strongly advocate a consistent training program, as provided by various organizations,[16] which can provide tailored solutions to your employee base, or specific sections of your employee base (like your IT department or your finance department), to help them change their behavior and discern between "good" emails and potential "really, really bad" emails which may contain malware packages just waiting to go off when someone opens the email or clicks on the link. Choose a program which can provide metrics and reports to either your compliance or IT security department, which might point out areas of risk such as divisions, departments, or employees who need further training. A recent report noted:

> The infamous Sony hack, the systematic attacks of Heartbleed and Shellshock targeting core internet services and technologies, and the new wave of mass mobile threats have placed the topic of security center stage. Companies are dramatically increasing their IT budgets to ward off attack but will continue to be vulnerable if they over-invest in technology while failing to engage their workforce as part of their overarching security solution. If we change this paradigm and make our workforce an accountable part of the security solution, we will dramatically improve the defensibility of our organizations.[17]

3. **INCREASE USER TRAINING AND ADVISE WORKERS ON SAFE PRACTICES WHEN USING FACEBOOK, TWITTER, SNAPCHAT, AND OTHER ONLINE SERVICES:** Simply put, there are bad actors out there who will attempt to lure your employees into doing things or sharing information which may, at its core, contain or share malicious code with others. Adopt policies and procedures to educate your employees on social media website scams, which may include limiting use of such sites to their own devices. "It is key that all staff receive security awareness training covering your acceptable usage policy for social networking. Promoting good practice and improving user behavior are the best methods of reducing the risks from this form of communication."[18]

4. **EMPLOY DMARC BASED TECHNOLOGY:** Many companies have chosen to employ a technology-based solution founded on DMarc, or "Domain-based Message Authentication, Reporting & Conformance."[19] "DMarc is an Internet protocol specification that… provides visibility into email flows, and can tell receiving servers to delete spoofed messages from spooked addresses immediately upon receipt, thus ensuring that only legitimate emails are delivered to inboxes."[20] DMarc allows companies to "pre-qualify" email providers who are "approved" to send your employees emails from those who may be attempting to spoof or clone domain names to send your employees malicious emails. Other vendors provide email spear phishing protection as well. As noted in the 2016 Data Breach Report:

An ounce of prevention is worth a pound of cure." It was good advice said it and so it remains. The first opportunity to defend against email borne threats is (thankfully) before a human can interact with it. Email filtering is your buddy in this fight and you need to have an understanding of your current solution, and test its implementation.

5. **SANDBOXING:** Deploy a solution that checks the safety of an emailed link when a user clicks on it. The hardware solution that is employed[21] examines the link-driven email and analyzes it against known malicious email threats and URLs and then "quarantines" them using anti-spam and anti-virus threat engines to see if those emails exhibit "bad" characteristics. These solutions can be used both "on premises" and if your email is handled by cloud mailboxes.[22] It is better to check and stop the email before it gets to an employee's desk where it could be inadvertently opened and spread malware to your network. Beware that not all sandboxing technology works the same, and it may not be 100% effective against all threat vectors, especially as bad actors get more and more sophisticated in masking their attacks.[23]

6. **KNOW YOUR ENDPOINTS:** Here we assume that the employee is going to click on the link from his home computer. Can you see his home computer? Can you generally see all your endpoints, meaning your smart phones, iPhones and iPads? According to one expert, David Bisson of Tripwire, "Digital attackers are constantly looking for ways to infiltrate organizations' IT environments. One of the easiest modes of entry is for an actor to exploit a weakness in an endpoint, a network node which according to Dark Reading remains "the most attractive and soft target for cyber criminals and cyber espionage actors to get inside."[24] Several endpoint solutions exist whereby your network commander can see, hear and sniff if something is amiss at an endpoint, and cut it off at the pass within seconds before it can do damage to the entire network.[25] Many are combined with other AI or automated products to make sure there is 100% visibility on the network.

7. **CHECK BEFORE YOU WIRE:** Given the vast increase in business email compromise (or "BEC") scams, there should be checks and balances in place before large, unexpected wire transfers take place, including secondary sign-offs within the company if the amount to be wired is over a pre-set threshold.

High profile attacks in 2014, 2015 and 2016 all have seemed to contain one common element: some employee, either high-level, low-level, or one targeted specifically for his or her password and administrative privileges information, opened a malicious email which set off a catastrophic set of consequences for a company. Though there are many solutions that can be potentially employed to stop this pattern of doom and gloom, not one can be said to be entirely effective. Instead, the set of proactive approaches described above, when used jointly, may help companies reduce the risk of potentially being spear phished "to death" by bad actors. In sum, please don't click on the link!

ENDNOTES:

[1] The author thanks Randi Singer, for co-authoring a related article with her on cybersecurity employee training in a Weil Gotshal & Manges LLP Client alert.

[2] The existence of the first "snake-oil salesmen" date back at least to the time of the First Intercontinental Railroad in 1863.

[3] See "Spearphishing Attacks," available at https://www2.fireeye.com/rs/fireye/images/fireeye-how-stop-spearphishing.pdf.

[4] See 2016 Verizon Data Breach Investigations Report, available at http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

[5] See "The Best Defense Against Spearphishing Attacks," available at https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html/.

[6] See e.g., "Phishing Email Baits Indiana Medical Center, Health Data Exposed," available at http://www.nextgov.com/cybersecurity/threatwatch/2015/04/breach/2233/; "SendGrid: Employee Account Hacked, Used to Steal Customer Credentials," available at https://krebsonsecurity.com/2015/04/sendgrid-employee-account-hacked-used-to-steal-customer-credentials/.

[7] See "China and Russia are using hacked data to target U.S. spies, officials say," available at http://www.latimes.com/nation/la-na-cyber-spy-20150831-story.html.

[8] See "Data Breach Methods Getting More Sophisticated, Report Says," available at http://www.govtech.com/data/Data-Breach-Methods-Getting-More-Sophisticated.html.

[9] See "Beware of Nepal charity scams," available at http://www.usatoday.com/story/money/personalfinance/2015/05/03/weisman-nepal-charity-scams/26755507/ (highlighting that "Email and text message solicitations for charities as well as solicitations you find on social media are also not to be trusted. Once again, you cannot be sure as to who is actually contacting you and these solicitations carry the additional danger of having links or attachments that, if clicked on or downloaded, will install malware on your computer or smartphone that will steal the personal information from your device and use it to make you a victim of identity theft.").

[10] See "5 Scams to Watch for in 2015," available at https://www.allclearid.com/blog/5-scams-to-watch-for-in-2015.

[11] See 2015 Verizon Data Breach Investigations Report," available at http://www.verizonenterprise.com/DBIR/2015/ (hereinafter, the "Verizon Report").

[12] See "Banking Malware Taps Macros," available at http://www.databreachtoday.com/banking-malware-taps-macros-a-8186 (describing the Bartalex macro malware scheme, in which a social-engineering attack tells recipients that their Automated Clearing House electronic-funds transfer was declined, and invites the recipient to click a link to "view the full details," which leads to a Dropbox page that lists specific instructions, including the need to enable Microsoft Office macros).

[13] There are scores of other scams too. Most recently, a network technology manufacturer overseas was caught in a "CEO email hijacking" scam in which an overseas subsidiary was tricked through employee impersonation into sending money to several offshore accounts. Very little of that money was recovered. See "Networking Manufacturer Ubiquiti Lost $46.7M after Falling for Elaborate Impersonation Scam," available at http://www.nextgov.com/cybersecurity/threatwatch/2015/08/breach/2438/. Another term for this scam is a "business email compromise," where the attacker impersonates a legitimate person or vendor and requests money be wired to another location (likely outside of the US). This scam has resulted in the loss of approximately $750 million in the past two years. See FBI: Social Engineering, Hacks Lead to Millions Lost to Wire Fraud – available at https://threatpost.com/fbi-social-engineering-hacks-lead-to-millions-lost-to-wire-fraud/114453#sthash.lmnaJHc7.dpuf

[14] This article is available at https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon.

[15] See Avoiding a bleak cybersecurity scenario," available at http://www.csoonline.com/article/3110785/techology-business/avoiding-a-bleak-cybersecurity-scenario.html.

[16] See, e.g., the comprehensive anti-phishing training services offered by www.phishme.com.

[17] See "The Weakest Link Is Your Strongest Security Asset," available here.

[18] See "Social networking best practices for preventing social network malware," available at http://searchsecurity.techtarget.com/answer/Social-networking-best-practices-for-preventing-social-network-malware.

[19] See "DMARC – What is it?" available at http://dmarc.org/.

[20] See "How To Reduce Spam & Phishing With DMARC," available at http://www.darkreading.com/application-security/how-to-reduce-spam-and-phishing-with-dmarc/a/d-id/1319243.

[21] For instance, one of these solutions is the FireEye EX prevention series. See "Threat Prevention Platforms that Combat Email-Based Cyber Attacks," available at https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/fireeye-ex-series.pdf.

[22] See e.g., "Email Threat Prevention Cloud," available at https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/fireeye-email-threat-prevention-cloud.pdf.

[23] See "'SandBlast' A Different Spin On Sandboxing," available at http://www.darkreading.com/attacks-breaches/sandblast-a-different-spin-on-sandboxing/d/d-id/1322076 (noting that as attackers are using new techniques to avoid having their malware play in the sandbox, forensic consultants are devising new techniques to find malware laying dormant on their servers ready to spring into action).

[24] See 3 Principles and Challenges of Endpoint Discovery, available at http://www.tripwire.com/state-of-security/security-data-protection/3-principles-and-challenges-of-endpoint-discovery/

[25] See "Tanium Endpoint Security," available at https://www.tanium.com/products/endpoint-security/

CHAPTER 5:
INCIDENT RESPONSE – PLANS, REALITY, AND LESSONS LEARNED

"The days of the IT guy sitting alone in a dark corner are long gone. Cybersecurity has become an obvious priority for C-Suites and boardrooms, as reputations, intellectual property, and ultimately lots of money [are] on the line."

– Priya Ananda, "One Year after Target's Breach: What have we learned?" November 1, 2014.[1]

"Resiliency is the ability to sustain damage but ultimately succeed. Resiliency is all about accepting that I will sustain a certain amount of damage."

– NSA Director and Commander of U.S. Cyber Command Mike Rogers, September 16, 2014.[2]

PURPOSE OF THIS CHAPTER:

1. **Identify the most important elements of a cyber incident response plan.**
2. **Identify the importance of compliance with the Department of Justice's April 29, 2015 memo on Incident Response Practices.**
3. **Identify the importance of proactive press and investor relations practices, as they relate to responding to a cyber incident, to preserve the company's reputation in the event of attack.[3]**
4. **Make the most of pen-tests and red-team exercises.**

The last few years of catastrophic cybersecurity breaches have taught us that throwing tens of millions of dollars at "prevention" measures is not enough. The bad guys are smart, very nimble, and can adapt their strategies to exploit network weaknesses and software vulnerabilities far quicker than companies have been able to eliminate them.[4] We have also learned there are no quick fixes in the cybersecurity world. The best approach is the holistic approach. Basic blocking and tackling like password protection, encryption, "ASAP" patching, employee training, and strong, multi-faceted intrusion detection and prevention systems[5] really trump reliance on the "50-foot-high firewall" alone.

But there are two additional things that are critical to a holistic cybersecurity approach: a strong, well-practiced incident response plan, and, as Admiral Rogers noted, the concept of cyber resiliency, e.g., the ability to "take your cyber lumps" but continue your business operations as soon as possible after the breach is remediated. In fact, a September 2015 Ponemon study of more than 600 IT and security executives stated, "Seventy-five percent of U.S. organizations are not prepared to respond to cyber attacks, leaving them more vulnerable than ever against increasing intensity and volume of security breaches. Improving cyber resilience is found to be the most potent weapon organizations have in prevailing against the mounting threats they face."[6] A more recent study had

similar findings: "Sixty-two percent of organizations acknowledged they were breached in 2015. Yet only 34% believe they have an effective incident response plan."[7]

The questions we ask, and hopefully answer, in this article are: (1) What are the essential elements of a cyber incident response plan? And (2) Why are incident response plans so important to your organization?

Indeed, the NIST has its own booklet, the "Incident Handling Guide,"[8] which notes:

> Computer security incident response has become an important component of information technology (IT) programs. Cybersecurity-related attacks have become not only more numerous and diverse, but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

Note that each element of an effective incident response plan has multiple sub-elements and multiple levels of complexity. We also note that, for effective incident response plans, "one size does not fit all." Plans will likely be different based upon organization size, complexity, and industry sector, and on the types of personally identifiable information stored by the organization (and where that data is stored).

Directors and officers need to resist the urge to take a statement such as, "Yes, we're ready for the next attack" at face value. Instead, they must ask relevant questions about the company's incident response plan now, prior to finding out that the organization has been hacked. The goal of the incident response plan isn't to make a company immune to hacks. In 2016, no organization has managed such a feat, not even the federal government. The primary goal behind having a well-rehearsed incident response plan is to improve one's "cyber resiliency;" to "get back in the game (quickly and safely)" as soon as possible in order to keep your customers and investors happy, and your corporate reputation intact. And to show any regulators and federal law enforcement agencies in the mix (e.g. SEC, OCIE, FINRA, FTC) that you have paid attention and planned for the worst.

"By failing to prepare, you are preparing to fail."

"Never leave that till tomorrow which you can do today."

-Benjamin Franklin-

A cyber "event," according to NIST, is "an observable occurrence in an information system or network." A cyber "incident" is something more — "a violation of computer security policies, acceptable use procedures, or standard security practices."[9] In a recent book, co-authored by Kevin Mandia, the founder of security consulting firm Mandiant (now FireEye/Mandiant) and titled, "Incident Response and Computer Forensics," Mandia simplifies this definition for today's cyber environment:

An incident is "any unlawful, unauthorized, or unacceptable action that involves a computer system, cell phone, tablet, and any other electronic device with an operating system or that operates on a computer network."

In sum, cyber "events" *may* ultimately be OK if it is determined either by intrusion detection systems, along with trained cyber-technicians reviewing the logs, that the event is something akin to "normal." Cyber "incidents" need to be investigated, because if they are "bad," they could be very bad and have catastrophic results for an organization if not promptly addressed, properly and fully identified (network-wide), and remediated as quickly as humanly possible so the organization may continue its operations relatively unhindered.

Distinguishing between potentially harmless cyber events and potentially serious cyber events is not an easy task, as many companies get thousands, if not tens of thousands, of cyber alerts a day from their intrusion detection systems. Skill, experience, and hardware that can distinguish "noisy" or "abnormal"[10] events from potentially serious events are required for this task. And it is a daunting task.

The best response to, "We've been hacked" is not, "Now what?" The best response is, "Let's invoke our incident response plan immediately." Though there are literally hundreds of cybersecurity consultants in the marketplace today that could provide a very complex version of an incident response plan, here are the basics (as least as we and NIST see them):

1. Preparation, Ownership and Testing of the Incident Response Plan

Just as many high-rise buildings in New York City have their own emergency evacuation plan in the event of a fire or other catastrophic event — plans that tenants rehearse several times a year — all companies should have a table-top tested, written incident response plan ("IRP") ready to go in the event of a cyber-attack. Directors and officers should consider the following elements essential to a good IRP:

a) The IRP needs to be in writing, fully documented, and regularly updated so there are no surprises when it is invoked after an incident is detected. The IRP needs to be in place *before* the breach. Putting one in place after you've been hacked is not the best time to try to figure out "on the fly" how to proceed.

b) The IRP should define the professionals (in-house and third-party vendors) that are part of the incident response team ("IRT"). The IRT needs to have clear delegation of authority (who does what), and clear lines of communication (who reports to whom). The team should have a legal component (whether in-house personnel, an outside firm, or most likely both) that is skilled in forensic investigations, disclosure obligations, and the preservation of evidence since law enforcement may ultimately be involved, depending upon the severity of the breach. Also, companies should consider having both a human resources person and a finance department designee on the IRT, since issues well beyond "just the hack" may suddenly surface (like the theft or loss of employee data). The IRP should have full sign-off by senior management so, again, there are no surprises and no excuses.

c) The IRT and IRP should be "owned" by one person in the organization ("the head" of the IRT). This no time for having too many cooks in the kitchen. It is the time for action, and ultimately to get the organization back online. The head of the IRT should have a deputy who is completely skilled on his or her own with strong incident response skills and experience, and who can, as an alternate, also serve as the owner of the incident response plan. Underneath the owner and the deputy are normally skilled incident response handlers who, on their own, have strong technical intrusion detection and forensic skills. The size and shape of internal IRTs vary from company to company, and are obviously budgetary dependent, as 24/7 ready IRTs have a price.

It goes without saying that if the organization is solely U.S.-based, it is possible to have only one owner of the IRP and one head of the IRT. In a global organization, the "one owner" policy may not be possible or even practical. Global organizations need to "globalize" their IRPs so that a local "owner" is in place — a person who is closer to the action and closer to his or her designated third party vendors. A local owner will also likely be more familiar with local laws relating to cyber- and privacy-related disclosures that may be implicated when a cybersecurity breach is investigated.

d) Many companies rely, in part, upon cyber breach lawyers and third-party vendors to work with and guide them through a data breach.[11] The lawyers and vendors should be pre-selected in advance, and be on a retainer in the event of a breach. The lawyers and vendors need to be available 24/7. There are no vacations in cybersecurity land. Firm evidence of a breach discovered by the IRT and its vendors may ultimately be developed, which will require a great deal of attention thereafter by all involved in the company, so outside counsel should be involved in retaining the vendors to preserve any applicable privileges.

e) The IRT should contain some element of "pre-planned" internal and external crisis communications because, depending upon the severity of the breach and the potential for severe reputational damage, there will likely be disclosure obligations (both formal and informal) following the breach. Notification of a "material" breach to investors may be necessary under U.S. SEC guidance, or may otherwise be necessary in order to reassure both customers and investors that the company is on top of the cyber breach and doing everything possible to protect investors and consumers. Given that today's news cycle is 24/7, the company needs to be ready to act on a moment's notice if it discovers (or is notified by a third party like the FBI or Secret Service) that it has been breached. Finally, some sort of formal notification may be required in various jurisdictions, or by regulatory authorities depending upon privacy concerns.[12] Because of potential formal notification requirements, it is important to have inside or external lawyers involved with and overseeing breach notifications.[13]

Thus a good crisis management/investor relations firm with experience in major corporate catastrophic events should be on retainer as well. Perhaps the only thing worse than a major hack and the associated costs involved is losing the faith and trust of customers, clients, or patients. These circumstances could cause a "death spiral" that may be impossible to recover from.

f) Organizations should engage law enforcement before a breach occurs. As we noted previously in the federal regulation chapter, the April 29, 2015 DOJ Incident Response memo makes it very clear that DOJ recommends/suggests that a company get to know its local federal law enforcement agents (the local field office of the FBI and U.S. Secret Service) before a breach occurs. We considered this good advice even before the DOJ IR memo, and now we strongly recommend this to all our clients. It makes complete sense to build a one-on-one relationship with these offices in order to facilitate a working and cordial relationship, just in case something happens and the company needs immediate help. Having such a relationship is a great way to understand (well in advance) how your cyber-attack case will be handled by law enforcement, what information the FBI or Secret Service will need to help them to their job and help you, and who they will want to talk to. The FBI or Secret Service can be a "friend in need" if the company later discovers it has been breached.[14]

g) Practice, Practice, Practice.

"Practice does not make perfect. Only perfect practice makes perfect."

-Vince Lombardi -

"Incident response plans are, in many ways, like family relics. These written instructions, which detail how firms should adequately detect, respond, and limit the effects of an information security incident, are highly valued by some, and yet all too often left gathering dust in the cupboard."[15] IRPs and IRTs are no good if they are dusty and unpracticed. Drills need to be conducted on a regular basis (we recommend at least quarterly) so that all members of the IRT and third party vendors (and the company's lawyers and PR team) know exactly what they are supposed to do and say in the event of a major cybersecurity incident. All stakeholders need to be involved, and "because responsibility for having an incident response plan is likely to fall to the information security manager, they have to understand a good one involves a lot of other people and areas outside of IT and security."[16] Rather than repeat the same "exercise" over and over, practice sessions should be pre-planned to simulate a wide variety of situations, from DDoS attacks to situations involving the destruction of data. In one quarter, try a ransomware exercise. In another quarter try a DDoS attack. By keeping it fresh and keeping it real, you are keeping your IRTs well-trained to act when needed. Boring is bad and creates apathy, and apathy costs money.

A good IRT is like a college rowing team rowing a scull down the Charles River: everyone needs to row in cadence and in the same direction to immediately respond to a cyber attack given both customer information and corporate reputations are at the heart of any breach. As noted in one recent report:

> Failure to act decisively when customer, investor, and staff interests are at the heart of the matter, can cost a business a fortune, and, for senior executives, their jobs. Companies under stress from a cyber incident are like families under stress: the strong ones come together, and those that aren't can fall to pieces under the pressure."[17]

2. Detection and Analysis of Threat Vectors, or, "Houston, We have a Problem"

No incident response plan will be effective without the ability to accurately detect and assess possible incidents. How exactly this is done today is a moving target of both software and hardware necessary to detect incidents from a variety of threat vectors. The technical side of this equation is too complicated for laymen to understand, but, in sum, organizations need to be able, through "continuous monitoring,"[18] to identify "indicators" or "evidence" of an attack through network monitoring systems such as "event-based alert monitoring" and "header and full packet logging."

AI and machine learning hardware should make this even easier, and may head off an attack in its entirety. As noted in one recent article, "You have to monitor and detect for anomalies," and part of monitoring and detecting demands collecting intelligence. By collecting intelligence, security teams will better know precisely how to build an effective IRP specific to their business. Intelligence begins with looking at transactions."[19] In sum, non-signature based IDS are designed to collect data transferred but are also systems to help the IRT detect malicious digital signatures, generate network system activity logs, or identify data that might show evidence of compromise when looked at in the whole. Today, AI and machine learning hardware will help narrow down where to look, or indeed point to the exact place to start the investigation. Here a few of the potential indicators of compromise that may show up:

- A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server.
- Antivirus software alerts when it detects that a host is infected with malware.
- A system administrator sees a filename with unusual characters.
- An application logs multiple failed login attempts from an unfamiliar remote system.
- An email administrator sees a large number of bounced emails with suspicious content.
- A network administrator notices an unusual deviation from typical network traffic flows.[20]

But today, since many cyber attacks are found to flow from one-time only use of malware (thus have no recognized "signature" to identify it as a threat), many companies are now transitioning to a signature-less intrusion detection system. One long-term industry expert noted in a recent interview, "We don't know what to look for when nobody else has seen it. The [signature] model breaks down…. How you protect yourself from a shotgun blast is very different than how you protect yourself from a sniper's bullet. Traditional protection mechanisms are geared toward those noisy mass attacks."[21] To combat this cyber-attack technique, "Rather than relying on detecting known signatures, [many] companies marry big-data techniques, such as machine learning, with deep cybersecurity expertise to profile and understand user and machine behavior patterns, enabling them to detect this new breed of attacks. And to avoid flooding security professionals in a sea of useless alerts, these companies try to minimize the number of alerts and provide rich user interfaces that enable interactive exploration and investigation."[22]

Whatever the monitoring system in place (which includes antivirus software alerts), incident response information may contain evidence of either network traffic anomalies, or evidence of actual data theft, which could lead to the conclusion that there has been a data breach. Today, many monitoring systems are automated (and even outsourced) because, quite simply, large organizations may have tens of thousands of incidents daily that need to be analyzed, correlated, and investigated. Logs should be kept and retained for some defined period (e.g. 90 days) as a matter of good practice, as they may be needed for a breach investigation.

3. Containment

Containment means, "How do we stop the bleeding so that no further damage can be done?" Again, this topic is complicated, so both in-house and outside legal experts and third party vendors are needed. In sum, a containment program should generally involve:

1. Isolating a network segment of infected workstations and taking down production servers that were hacked;[23]
2. A plan to isolate infected systems, forensically copy them, and transfer them to another off-grid environment for further analysis by either your forensic team or law enforcement;
3. Triaging and analyzing the infection or malware so that an eradication plan can be formulated; and
4. Notifying law enforcement immediately if the company suspects that the incident stemmed from criminal behavior. Note here that the April 29, 2015 DOJ IR memo states that any subsequent law enforcement investigation will be done with as little disruption as possible,

and with as much discretion as possible.[24] Indeed, as we now know, law enforcement has information that companies may not be privy to, like digital signatures from breaches of other companies. They may have other indicators that could help the company identify the nature of the threat vector involved or determine where to look on the server to find the evidence of compromise, as well as other helpful information.

Finally, assuming the company has concluded that a breach has occurred, and personally identifiable information has been compromised, it is important to have the IR/PR/legal team available to advise the IRT on potential disclosure obligations under federal law (like HIPAA), state law, or under the law of a foreign government (EU/UK GDPR directives) that may be applicable.

If the company's incident response plan was prepared well in advance, these disclosures should be something close to "ready to go," but for filling in the facts as the company then understands them to be at the moment the press release is issued. Though it is critical for a company to not be too quick to issue a press release if it does not understand all the facts at that time, it can be equally critical to show the public (consumers and investors) that the company took decisive action when it first discovered the breach. Here again, experienced counsel and an experienced cyber IR/PR advisor can help the company find a happy medium for both public and required disclosures to regulators. Though there is no right or wrong answer as to when to issue a breach press release, and how much to say in the release, clearly the trend is towards more and quicker disclosure rather than less when a company is breached. Keeping customer confidence is critical if a company wants to get right back on its feet after a cybersecurity breach. In fact, as one customer study noted, "Thirty-five percent of respondents said they would stop shopping at a company altogether if it lost their personal data, while an additional 23% said they would be 'much less likely' to shop there. With figures like this, it's clear that breaches do drive customers away. And while large firms with deep pockets may be better able than smaller ones to ride out the storm and wait for customers' memories of the breach to fade, many millions of dollars will be lost in the interim." [25]

Lastly, disclosure will be necessary to the company's cyber insurance provider. Many cyber insurance policies provide coverage (under their terms and conditions, which should be reviewed well in advance of any breach) so as to allow the company to take advantage of forensic and remediation services and coverage, as well as a "breach coach" and suggested third party vendors if the company does not have such vendors on retainer.

4. Remediation and Eradication

Remediation and eradication means "fixing the problem" as rapidly as possible after the threat vector is fully identified so that the attacker doesn't have time to change his or her method or mode of attack. Eradication efforts could involve:

- Blocking malicious IP addresses identified during the investigation.
- Changing all passwords.
- Patching holes in the network architecture that are identified during the investigation.
- Fixing all vulnerabilities identified during the investigation.

5. "Lessons Learned" Post-Mortem

Cyber post mortems are like many post-event discussions: lessons can always be learned as to what went right with your IRP (where did you excel), what went wrong (what didn't work so well), and what areas can be improved upon by the entire IRT so that it can perform better during the next incident investigation.

6. Making the Most of Pen Tests and Red-Teaming Exercises

Is it really a good idea to wait until there's a breach to evaluate whether one's incident response plan is sound? If "practice makes perfect," are there opportunities for a company to learn its lessons in the safety of a "practice" scenario instead of taking a beating with live ammunition? Absolutely.

Here is how NIST defines pen-testing activities:

> Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies."[26]

Yet, there's another form of testing that is even more efficient at evaluating the effectiveness of the company's detection systems (by which we mean hardware, software, and personnel) and their incident response capability — how well the incident response team and processes operate under stress, in realistic conditions. That cyber-stress test, called a Red Teaming Exercise, is defined by NIST as:

> Red team exercises extend the objectives of penetration testing by examining the security posture of organizations and their ability to implement effective cyber defenses. As such, red team exercises reflect simulated adversarial attempts to compromise organizational mission/business functions and provide a comprehensive assessment of the security state of information systems and organizations. Simulated adversarial attempts to compromise organizational missions/business functions and the information systems that support those missions/functions may include technology-focused attacks (e.g., interactions with hardware, software, or firmware components and/or mission/business processes) and social engineering-based attacks (e.g., interactions via email, telephone, shoulder surfing, or personal conversations)."[27]

How are pen tests and red-team exercises different? Red-team exercises are a simulated adversarial attempt at breaking in, in some cases literally, as some RTEs include physical break-ins as part of their scope. As you can imagine, if an attacker is able to walk out of your company with a server under their arm, you definitely suffered a breach.

NIST provides additional clarification, indicating, "While penetration testing may be largely laboratory-based testing, organizations use red-team exercises to provide more comprehensive assessments that reflect real-world conditions. Red-team exercises can be used to improve security awareness and training and to assess levels of security control effectiveness."[28]

WHY IS AN EFFECTIVE INCIDENT RESPONSE PLAN SO IMPORTANT TO ANY ORGANIZATION?

> "We are in a world now where, despite your best efforts, you must prepare and assume that you will be penetrated. It is not about if you will be penetrated, but when…." -Admiral Mike Rogers, head of the NSA and U.S. Cyber Command[29]

We placed this section here at the end of the chapter because, frankly, we didn't want to give away the punchline too early. But we kind of did already with Admiral Roger's quote above. An effective IRP is absolutely vital to your organization because: (1) it may have already been hacked (and possibly doesn't know it yet), and thus (2) your organization needs to be able to take a "cyber punch" and get off the canvas to fight another day. An effective, table-top practiced incident response plan is essential for a variety of other reasons:

1. If you are in a specific industry sector, most especially the regulated financial services sectors, your regulators will specifically ask whether your organization has an incident response plan. If your answer is, "No," that answer might not be well received;
2. A battle-tested incident response plan may be evidence of cybersecurity best practices if the company is later the subject of a lawsuit or regulatory proceeding resulting from disclosure of the breach; and
3. A battle-tested incident response plan will hopefully prevent an organization from having a cyber incident develop into a catastrophic event, either financial, reputational, or both, which could cause the company's decline or death in some cases if there is a "crisis in confidence" among customers or investors, or a "run on the bank" following disclosure of the cyber breach.

ENDNOTES:

[1] Found at http://www.marketwatch.com/story/one-year-after-targets-breach-what-have-we-learned-2014-10-31.

[2] Found at: http://threatpost.com/nsa-director-rogers-urges-cyber-resiliency/108292#sthash.V4bkayBQ.dpuf.

[3] The author thanks Austin Berglas, a Senior Managing Director at K2 Intelligence, for his criti-cal review and comments to this section.

[4] See "Sony Films Are Pirated, and Hackers Leak Studio Salaries," found at http://www.nytimes.com/2014/12/03/business/media/sony-is-again-target-of-hackers.html?_r=0; "Hackers Using Lingo of Wall St. Breach Health Care Companies' Email," found at http://www.nytimes.com/2014/12/02/technology/hackers-target-biotech-companies.html; "Hack-ing the Street," a Fire Eye/Mandiant Special Report, found at https://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf.

[5] See "Intrusion Detection FAQ: Can you explain traffic analysis and anomaly detection?" found at http://www.sans.org/security-resources/idfaq/anomaly_detection.php.

[6] See "New Ponemon Institute Study Reveals That Improving Cyber Resilience is Critical for Prevailing Against Rising Cyber Threats," available at http://www.freshnews.com/news/1129839/new-ponemon-institute-study-reveals-that-improving-cyber-resilience-critical-prevailin.

[7] See "4 steps to a strong incident response plan," available at http://www.csoonline.com/article/3104203/techology-business/4-steps-to-a-strong-incident-response-plan.html.

[8] See NIST "Computer Security Incident Handling Guide," (hereinafter, the "NIST Incident Handling Guide," found at http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.

[9] Id.

[10] Next generation intrusion prevention systems and next generation firewalls will generally have some element of "machine learning" about what network behavior is "normal" versus what can be considered "abnormal." See e.g. "Creating cybersecurity that thinks," available at http://www.computerworld.com/article/2881551/creating-cyber-security-that-thinks.html (dis-cuss the transition from signature-based to non-signature based intrusion detection technology).

[11] Three of the larger companies that we and our multi-national clients regularly deal with from an incident response perspective are Fire Eye/Mandiant, Verizon, and IBM. See https://www.fireeye.com/, http://www.verizonenterprise.com/products/security/, and http://www-935.ibm.com/services/us/en/it-services/security-services/emergency-response-services/?S_TACT=R02102GW&S_PKG=-&cmp=R0210&ct=R02102GW&cr=google&cm=k&csr=IT+Emergency+Response+Services_UN&ccy=us&ck=security%20services&cs=b&mkwid=sk3dL6Acl-dc_49046510203_4326fb30773. There are certainly other companies in the incident response space that have the ability to fully respond to domestic breaches, see e.g. https://www.k2intelligence.com/.

[12] See "The Role of Cybersecurity Incident Response," available at http://www.cioreview.com/news/the-role-of-cyber-security-incident-response-nid-18068-cid-21.html.

[13] In some cases, and for some larger companies, it may even be important for companies to con-sider "off the grid" communications systems, like temporary cellphones and satellite phones so that key IRT members can communicate with each other in the event that the breach also affects a Company's corporate phone lines. See "Spike in Cyber Attacks Requires Specific Business Continuity Efforts," found at http://www.emergency-response-planning.com/blog/topic/cyber-security.

[14] Just a note here. Under the White House's recent announced Cyber Action Plan, if a breach reaches a certain level of severity (Level 3, which means it is like to result in a "likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties or public confidence, . . . The law enforcement investigation, attribution and pursuit of the threat actor of a cyber incident will be the responsibility of the Department of Justice, acting through the FBI and the National Cyber Investigative Joint Task Force." See "White House unveils federal cybersecurity plan and attack rating system," available at http://searchsecurity.techtarget.com/news/450301495/White-House-unveils-federal-cybersecurity-plan-and-attack-rating-system.

[15] See "How to improve your incident response plan," available at http://www.csoonline.com/article/3095810/data-protection/how-to-improve-your-incident-response-plan.html.

[16] Id.

[17] See KPMG "Global CEO Outlook 2015," http://www.kpmginfo.com/ceo-outlook2015/documents/CEOSurvey_2015-US-Revise-07-22-FINAL-R.pdf.

[18] "Continuous Monitoring" is the hallmark of a Implementation Tier 4 organization in the NIST cybersecurity framework. See NIST Cyber Security Framework, found at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[19] See "Detection and Response, Where to Begin," available at http://www.csoonline.com/article/3114805/techology-business/detection-and-response-where-to-begin.html.

[20] See "Cybersecurity and Privacy Diligence in a Post-Breach World," available at http://corpgov.law.harvard.edu/2015/02/15/cybersecurity-and-privacy-diligence-in-a-post-breach-world/.

[21] See "On prevention vs. detection, Gartner says to rebalance purchasing," available at http://searchsecurity.techtarget.com/news/2240223269/On-prevention-vs-detection-Gartner-says-to-rebalance-purchasing.

[22] See "Why Breach Detection Is Your New Must-Have, Cyber Security Tool," available at http://techcrunch.com/2014/09/06/why-breach-detection-ss-your-new-must-have-cyber-security-tool/. A very good description of how big-data cyber analytical tools work is available in the fol-lowing article, "Connecting the Cyber-Threat Dots Through Big Data," available at http://www.smartdatacollective.com/juliehunt/332900/connecting-cyber-threat-dots-through-big-data.

[23] For a very good summary of basic incident response plans and techniques, see Incident Han-dler's Handbook," SANS Institute: InfoSec Reading Room, available at http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901.

[24] Cooperation with law enforcement may also garner a company "more favorable" treatment by the Federal Trade Commission in any subsequent breach investigation by that agency. See "If the FTC comes to call," available at https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call?utm_source=govdelivery ("We'll also consider the steps the company took to help affected consumers, and whether it cooperated with criminal and other law enforcement agencies in their efforts to apprehend the people responsible for the intrusion. In our eyes, a company that has reported a breach to the appropriate law enforcers and cooperated with them has taken an important step to reduce the harm from the breach. Therefore, in the course of conducting an investigation, it's likely we'd view that company more favorably than a company that hasn't cooperated."),

[25] See "Survey: Consumer Confidence in the Security-Breach Era," available at http://intelligent-defense.softwareadvice.com/consumer-confidence-security-breach-era-0614/.

[26] Controls page section of the NIST Special Publication 800-53, rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations." https://web.nvd.nist.gov/view/800-53/Rev4/control?controlName=CA-8

[27] Id

[28] Id

[29] For the article containing the quote, see "NSA Chief Expects More Cyberattacks Like OPM Hack: Mike Rogers says, 'I don't expect this to be a one-off'" available at http://www.wsj.com/articles/nsa-chief-expects-more-cyberattacks-like-opm-hack-1436985600

CHAPTER 6:

USING CYBER INTELLIGENT SOLUTIONS TO DEFEAT HACKERS (OR AT LEAST LEVEL THE PLAYING FIELD)!

> "[It is] my firm conviction that machine learning and artificial intelligence are the keys to just about every aspect of life in the very near future: every sector; every business. If you run a business, its future depends on your ability to generate data about its activities, data that can then be fed into algorithms. Today's big companies have been storing data away about our activities, will continue to do so through new methods and interfaces, and the reason is not to spy on us, but to feed their algorithms; to create the products and services of the future.[1]
>
> Leaders of every industry and institution are sprinting to become digital, adopting digital products, operations, and business models. But once everything becomes digital, who will win?
>
> The answer is clear: it will be the companies and the products that make the best use of data. Data is the great new natural resource of our time, and cognitive systems are the only way to get value from all its volume, variety, and velocity. Having ingested a fair amount of data myself, I offer this rule of thumb: if it's digital today, it will be cognitive tomorrow."[2]

Yep, this is the chapter you have been waiting for. The big one! This is the chapter where we talk about artificial intelligence, machine learning, robots, Westworld, and other cool, cutting-edge stuff. Well, not really, but sort of. This chapter is about the future of cybersecurity. If you haven't noticed from the trade journals and blogs, the future of cybersecurity is about several important buzzwords you will hear this year and next, and thereafter:

Big Data analytics

Artificial intelligence

Machine/deep learning (supervised and unsupervised)

Cognitive computing

In truth, the above concepts are similar in some ways, but meaningless *without* the context provided by the nearly 2.5 quintillion gigabytes of data which are created daily in our businesses.[4] How we use this data, in ways we can both imagine today (and engineer for) and in ways we can only dream about, will be the undeniable future, and the driver of the next 10 years of international business and trade. And it will affect nearly all forms of industry. Indeed, how we use the raw data we accumulate from our network sensors, endpoints, firewalls and firewall logs, intrusion detection and prevention devices, and other security hardware (including the plethora of written documents on malware and vulnerabilities), *along* with professional journals, blogs and threat intelligence feeds will not only define the future of cybersecurity, but may also will define the future of our country and the world in general, as we try to protect ourselves from not only widespread data and IP theft, but from cyber terrorism and abject cyber criminality.[5]

Apart from humongous amounts data to analyze, the cyber skills shortage presents another challenge. "According to a recent Peninsula Press analysis of data from the Bureau of Labor Statistics, more than 350,000 cybersecurity jobs are currently open in the United States, and job postings are up over 74% over the past five years."[6] We simply cannot graduate enough individuals with computers or cybersecurity degrees to even make a dent in these numbers. Absent enough trained individuals, how can corporations help themselves? AI, machine learning, and cognitive computing. But before we delve into the cool stuff, let's first discuss the more general concept of Big Data analytics.

WHAT IS BIG DATA ANALYTICS?

"You can't manage, what you can't measure."

There's much wisdom in that saying, which has been attributed to both W. Edwards Deming and Peter Drucker, and it explains why the recent explosion of digital data is so important. Simply put, because of Big Data, managers can measure, and hence know, radically more about their businesses, and directly translate that knowledge into improved decision making and performance.[7]

Several studies have noted that at least 80% of the 2.5 quintillion gigabytes of data created every day comes in unstructured form. Structured data is pretty simple to explain: it is data that is readily identifiable. "[S]tructured data refers to information with a high degree of organization, such that inclusion in a relational database is seamless and readily searchable by simple, straightforward search engine algorithms."[8] "By comparison, unstructured data has no identifiable structure. Unstructured data typically includes bitmap images/objects, text and other data types that are not part of a database. Most enterprise data today can actually be considered unstructured. An email is considered unstructured data. Even though the email messages themselves are organized in a database, such as Microsoft Exchange or Lotus Notes, the body of the message is really freeform text without any structure at all — the data is considered raw."[9]

And this is the amount of data we create today. Imagine if the pundits are right and we have 50 billion endpoints by the year 2020. The creation of the large amounts of data generated today has created the field of "Big Data analytics," which is the general field of creating "structure" from unstructured data so that it can be used by businesses, manufacturers, electric grids, and other data "creators" to accurately and efficiently serve their customers, suppliers, and stakeholder constituents.[10] When you think about the potential sources of data, whether from the field of genomics, disease, cancer, diabetes, electric supply and consumption, airline flight and travel, and even statistics regarding the best golf swing, the field of Big Data analytics is immense. And because of the inherent value of data, it was recently said in a panel on artificial intelligence, "Data is the new oil…."[11]

Without getting hyper-technical, the good folks at IBM typically define "Big Data" by its characteristics: "Volume, variety, velocity, and veracity."[12] Volume means the amount of data being analyzed. Variety what sort of data is (i.e., freeform text, images) being collected during the average business day and where the data comes from. Velocity means how quickly the data arrives on your doorstep and is processed by you. Finally, "[v]eracity is a term that's being used more and more to describe Big Data; it refers to the quality or trustworthiness of the data. Tools that help handle Big Data's veracity transform the data into trustworthy insights and discard noise."[13] For any business depending upon Big Data, and most certainly for cybersecurity, the Big Data analytics engine you

choose must separate the "noise" (data that is essentially "meaningless" when stored and digested) that is present from any data set from real actionable data that can be depended upon or acted upon by the company.

> Typical deep learning applications [a form of machine learning] cover image recognition (tracking a person in a crowd, for example), as well as speech recognition and understanding, including understanding in a first-time exposure to a voice (the system has not been trained to understanding only one person's speech pattern), a Holy Grail in AI. Current best accuracy is the 95% region using deep learning.[14]

WHAT IS ARTIFICIAL INTELLIGENCE?

> "We are entering an extremely critical time in history where society will change dramatically — how we work, live, and play. Science fiction is morphing into reality. Flying cars exist, cars that drive themselves are on the road, and artificial intelligence that automates our lives is here."[15]

This whole area of research starts with the term "artificial intelligence," (hereinafter referred to as "AI") the idea of which has been around since the time of Frankenstein. The classic Wikipedia definition notes that AI is "intelligence exhibited by machines. In computer science, an ideal 'intelligent' machine is a flexible rational agent that perceives its environment and takes actions that maximize its chance of success at some goal."[16] Said differently, "Artificial intelligence encompasses the techniques used to teach computers how to learn, reason, perceive, infer, communicate, and make decisions like humans do."[17] One expert notes, "Artificial intelligence refers to 'a broad set of methods, algorithms, and technologies that make software 'smart' in a way that may seem human-like to an outside observer."[18]

For those who are curious about the technology and science, in English, AI has been more recently developed based upon the formation of artificial neural networks ("ANN"), which are modeled on the architecture of the human brain.[19] "Artificial neural networks are a class of models that is frequently used in machine learning, both in the supervised and the unsupervised setting, because of their ability to handle large amounts of training data. Neural networks consist of a number of layers, each of which contain[s] a number of parameters whose values are unknown a priori and need to be trained (i.e. 'tuned' on training data). Each layer in an artificial neural network contains artificial neurons. Each neuron receives, as input, the outputs of neurons in a previous layer. The inputs are then summed together (and passed through a non-linear 'activation' function). This behavior is reminiscent of biological neurons, which is where the name 'neural' network came from."[20] A simple ANN might have 5-10 layers of artificial neurons. Networks with hidden layers (called "deep layers," which hence generated the term "deep learning") were created to attempt to draw more representations from the data before its results are communicated to the output layer.

Said a little more simply, "Nodes are generally arranged in layers. But historically it was feasible to train networks with only one hidden layer of neurons in addition to the input and output layers. Deep learning takes these methods to the next level by filtering the data through multiple [hidden] layers of neurons…. At each layer, the network can learn successively more abstract representations of relationships between data points. With enough layers, nodes, and data, deep neural networks can perform a host of functions with accuracy rates far surpassing all other machine learning techniques."[21] "Training the many layers of virtual neurons in the experiment took 16,000 computer processors — the kind of computing infrastructure that Google has developed for its search engine and other services."[22]

With this in mind, let's now discuss the various families of AI, which many laypeople use in the same breath: machine learning, deep learning, and cognitive computing.

MACHINE LEARNING:

Early AI suffered from a lack of success for two reasons: lack of computing horsepower and lack of a large quantity of documents and images to train the networks. Both are no longer problems. A tremendous increase in computing power, starting in or around 2009, coupled with companies that create millions of terabytes of information and text documents each year, has spawned the AI subfield of "machine learning." Under this concept, computers learn from the data they process. The "computers discover patterns within data and then use those patterns to make useful, and ideally correct, predictions…."[23] Said differently, "all of machine learning is about recognizing trends from data or recognizing the categories that the data fit in so that when the software is presented with new data, it can make proper predictions…."[24]

There are two forms of machine learning[25]:

1. **UNSUPERVISED LEARNING** — In "unsupervised learning," machines learn from the millions of documents and pieces of data created every day. They do not create additional rules of the road in terms of how they should respond and interact with humans; they provide a response to humans in accordance with pre-set underlying algorithms running within the previously-mentioned clusters of computer-generated neural networks. The easiest way to explain unsupervised learning is that it looks at all behavior and documents and tries to determine what is "normal" behavior at any given point in time, and what looks like abnormal behavior (or behavior that appears to be an "outlier"). Abnormal data is then dealt with according to pre-set rules. In short, unsupervised learning looks for previously hidden patterns or previously hidden "structure" in the data. It could be a "good" structure or an "indifferent" or "bad" structure that bears more examination.[26] That is for the analyst to later decide.[27]

   As demonstrated by a company called Deep Instinct, at BlackHat 2016, on the topic of Deep Learning:

   > Deep learning has shown groundbreaking results, even compared to classical machine learning, in detecting first-seen malware, superseding any solution currently available on the market. In deep learning, it takes just a few milliseconds to feed the technology with raw data and pass it through the deep neural network to obtain the prediction. This enables not only detection, but also prevention in all cases (the moment a malicious file is detected, it is already removed as well). Our brain works in a similar way as well. It takes us a long time to learn something, but once we learn it, we can use it very quickly in prediction mode.
   >
   > Furthermore, when applying deep learning, as opposed to machine learning, there is no need to conduct manual feature engineering. Instead, datasets of many millions of malicious and legitimate raw files are fed into the infrastructure, enabling deep learning to learn on its own the useful high-level, non-linear features necessary for accurate classification.[28]

2. **SUPERVISED LEARNING** — With supervised learning, analysts help the machines generate the correct rules to interpret the data. The network is first run with a "training" set of data against a set algorithm with a desired outcome in mind, and then, based upon the output, the algorithm is tweaked in order to achieve the desired output. After a certain period of time and with a large amount of data, the algorithm should eventually produce a "near" correct output.

Here is an example of supervised learning: say I want to train a machine to determine if a photo is a car or a truck. To train the machine, I provide it with 100 photos of cars and 100 photos of trucks or buses. Once the machine is trained, I can give it a picture and it can tell me if the photo is a car or a truck.

Not all machine learning solutions are created equal. One measure to determine the effectiveness of a machine learning model would be its accuracy in future predictions. For example, I ask the cars and trucks model to tell me if a photo is a car or a truck. Let's say I provide it with 10 photos of cars, and of that 10 it says eight are cars and two trucks. We can then say the model is 80% accurate. While this is reasonably accurate, one can easily improve upon this model. One way to improve a machine learning system is to provide more data — essentially provide broader experiences to improve its capabilities. For example, instead of 100 photos, one might provide 10,000 or 100,000 photos to train the machine. This increase in volume provides huge improvements in the accuracy of such models. Imagine then providing the model with a million pictures, or 10 million pictures. Then imagine the computing horsepower required to process 10 million pictures. Today we have this computing horsepower, which accounts for the rapid growth of AI solutions.

COGNITIVE COMPUTING:

Cognitive Computing is proving successful at helping humans process and understand the vast world of unstructured data. Cognitive computing involves self-learning systems that use data mining, pattern recognition, and natural language processing to mimic the way the human brain works.[29] "The goal of cognitive computing is to simulate human thought processes in a computerized model. Using self-learning algorithms that use data mining, pattern recognition, and natural language processing, the computer can mimic the way the human brain works."[30]

In sum, under cognitive computing dogma, Watson is exposed to structured data that might normally be found in any network, along with unstructured data fed into the system by the analyst (say, e.g., a cybersecurity report and newspaper articles on a particular strain of malware). In this way, Watson becomes smarter about the task he is given.[31] "The more data the system is exposed to, the more it learns, and the more accurate it becomes over time. The neural network is a complex "tree" of decisions the computer can make to arrive at an answer."[32]

IBM's cognitive platform, Watson,[33] made its debut much earlier than other forms of AI. Its claim to fame came when Watson "defeated Brad Rutter and Ken Jennings in the Jeopardy Challenge of February 2011."[34] "In healthcare, IBM Watson for Oncology, trained by Memorial Sloan Kettering ("MSK"), helps oncologists treat cancer patients with individualized evidence-based treatment options by analyzing patient data against thousands of historical cases trained through more than 5,000 MSK MD and analyst hours. Watson can help doctors narrow down the options and pick the best treatments for their patients. The doctor still does most of the thinking. Watson is there to make sense of the data and help make the process faster and more accurate."[35]

We have only begun to see the vast applications of artificial intelligence, machine learning and cognitive computing. As noted by one prize-winning scientist, Raymond Kurzweil, "My mandate is to give computers enough understanding of natural language to do useful things — do a better job of search; do a better job of answering questions." Essentially, he hopes to create a more flexible version of IBM's Watson, which he admires for its ability to understand Jeopardy! queries as quirky as, "A long, tiresome speech delivered by a frothy pie topping." (Watson's correct answer: "What is a meringue harangue?").[36]

APPLYING AI AND MACHINE LEARNING PRINCIPLES TO CYBERSECURITY

> "It's not about replacing humans, but about making them superhumans." -Caleb Barlow, IBM Security[37]

We need to get that statement out of the way early before any reader starts sharpening his or her spear to throw at us. At this moment in time, there is no way possible that AI has the ability to totally replace humans in making decisions about their computer networks. And there may be no way five years from now to replace humans. We are not there. We may never be there, and that is not the point of introducing AI to cybersecurity.

The point is that with the plethora of sensors, laptops, smartphones, and network hardware and software devices creating terabytes of information every day, there is simply no way for humans to keep up. And, most certainly, with the ever-present Internet of Everything, the growth in data in the future will continue to be exponential, creating even more work to do.[38] So AI and machine learning do serve a useful purpose in cybersecurity — to crunch A LOT of network data coming from on premises, the cloud, ICS sensors, and a whole lot of other places.

APPLICATIONS OF AI AND MACHINE LEARNING TO CYBERSECURITY

Darktrace, a leading UK cybersecurity company founded by former MI5 and GCHQ intelligence staff, developed the first product that applies unsupervised machine learning to cybersecurity. With probabilistic mathematics initially developed at the University of Cambridge, Darktrace's Enterprise Immune System self-learns what is normal for users, devices, and networks and can detect anomalies as they arise without relying on knowledge of past attacks. Darktrace's additional product, Antigena, automates the fight against those threats, essentially allowing a network to self-defend against threats in real time, giving the human supervisor time to catch up. Antigena "'replicates the function of antibodies in the human immune system' by inoculating threats as they appear. Depending on the intrusion, Antigena will respond by either stopping or slowing down activity related to a specific threat; quarantining users, systems, or devices as required; or marking specific pieces of content for further investigation."[39]

"As such, Darktrace Antigena is a unique product, complementing Darktrace's core detection capability. It allows critical, mitigating action to be taken, without human intervention — and faster than any security team can respond. Depending on the severity of the anomalous activity detected by Darktrace, these responses could involve:

- Stopping or slowing down activity related to a specific threat.
- Quarantining people, systems, or devices.
- Marking specific pieces of content for further investigation or tracking.[40]

Says Dave Palmer from Darktrace, "In this new era of automated attacks, no security analyst can keep up. The machine must fight back. The future is self-defending networks which autonomously respond to threats — wherever they may lie."

While Darktrace trains on the evolving behaviors of people and devices on an organization's network to recognize inexplicable changes in behavior caused by both outside attacks and insider threats, systems like Microsoft's advanced threat analytics platform rely on knowledge of historical attacks in order to recognize future ones. Microsoft uses machine learning capabilities that help analyze malicious or suspicious network traffic. "Its Advanced Threat Analytics platform ("ATA") uses a combination of log file analysis, deep packet inspection, and data from Active Directory to detect inappropriate access to corporate networks. Log files can reveal, for example, users logging on at unusual times, from unusual machines, or from unexpected locations. Deep Packet inspection (DPI) can show more obviously malicious behavior, such as attempts to use Pass-the-Hash or other credential-reuse attacks. Anomalous logins and resource accesses are detected with machine learning-based heuristics, with the DPI used to detect the signatures of attacks."[41]

Microsoft is also able to leverage information that it has access to through its market leading position in the cloud. "'We're pretty excited about this volume because it's the first one we've ever released with data from our cloud services and there are a lot of customers, including CISOs and CIOs, that are interested in the data we have from our cloud,' Tim Rains, chief security advisor at Microsoft, told *Infosecurity*, a leading information technology publication. By implementing their machine learning system capable of processing 10 terabytes of data every day, the firm has been able to leverage its widespread cloud data to create an extensive, intelligent security graph to help protect its customers. 'The intelligent security graph is our attempt to collect trillions of signals from billions of data sources so that we can triangulate what the bad guys are doing and where they're at. The graph allows us to us to put a great deal of data together, analyze it and make changes to our security posture.'"[42]

FireEye also has advanced machine learning hardware to help its clients see potentially malicious traffic before it can do harm to its network. As noted by one FireEye executive, "When you're able to take our intelligence and drive that into their detection platforms, you're going to be able to protect against things you would have not otherwise seen."[43] "The FireEye Threat Management Platform combines advanced detection, investigation and response technologies, real-time threat intelligence, and leading security expertise in products and services to reduce the business risks of cyber attacks on the network, at the endpoint and in the cloud. Threat intelligence derived from machine learning, incident response and a global network of researchers is orchestrated across the Threat Management Platform to detect new attacks quickly and reduce response times across multiple attack vectors.[44] Advanced analytics and forensics capabilities, backed up by human expertise, complement virtual machine-based detection in an adaptive framework that lowers complexity of security operations and total cost of ownership while enabling customers to manage risks more effectively."[45]

FireEye's security automation and orchestration product (which it obtained when it acquired Invotas in 2016) removes manual intervention from the conventional event and threat response capabilities, replacing it with machine speed decision making and response. The ability to automate the response using high-fidelity detection backed by the richest intelligence allows security analysts to scale and increase their efficiency and effectiveness in responding to emerging and voluminous threat volumes. Says Paul Nguyen at FireEye, "Given the current shortfall in the workforce to meet the current and future demands, automation and orchestration becomes a necessity to bridge that

gap to more effectively address the threat landscape. We have to offload the human dependency and move to intelligence-led automation and orchestration to scale our defensive capabilities which include people, technology, and data."

Cyber 20/20, Inc. has developed a highly accurate automated malware analysis platform that uses Deep Neural Networks ("DNNs") to analyze and identify current unknown malware, zero-day exploits, and advanced persistent threats. Malware is a central and industry-wide challenge to Internet security, and currently the state-of-the-art malware detection engines are constructed with manual intensive, inefficient, and slow processes. Cyber 20/20 offers a revolutionary new automated design approach to malware analysis and detection by removing the human in the loop risk and time factors.

Their platform leverages accelerated high-performance machine learning algorithms to be able to process and continually learn from very large malware repositories, yielding an extremely high detection rate of 99.5% and low false positive rates of less than 0.1%. They have developed a malware analysis and detection engine for the financial industry using a curated Big Data set of millions of financial malware variants from over 70 distinct malware families, and are currently working to develop purpose-built models for other sectors.

Cyber 20/20 uses a variety of different static and dynamic analyses because of the inherent disadvantages of using either static analysis or dynamic analysis on their own. Static techniques can fail when the malware has been packed or encrypted, and it may not bring into focus parts of the program important during the application's execution. Dynamic analysis has problems because malware hides its behavior when it detects it is running in a sandboxed environment. The data from static and dynamic analyses is transformed into several characterization representations, e.g., flat vectors and graph-based features. Cyber 20/20 trains several DNNs combined in an ensemble fashion to build highly accurate malware detection and analysis. Removing humans from the loop allows their solution to quickly close windows of exposure left open by other products that have out-of-date malware detection engines.[46]

Finally, MIT has designed its own security intelligence and response platform based upon machine learning. MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) and the machine learning startup PatternEx has developed a supervised learning platform that, upon initial testing, "can detect 85% of attacks, which is roughly three times better than previous benchmarks, while also reducing the number of false positives by a factor of five. The system was tested on 3.6 billion pieces of data known as 'log lines,' which were generated by millions of users over a period of three months."[47]

After the data is first clustered through an unsupervised learning algorithm, a human analyst provides feedback on whether or not the alleged events are actual attacks. That feedback is then incorporated into the program for future attacks. CSAIL can be scaled up to incorporate more data, and holds a lot of promise for its ability to reduce the number of actionable security events that analysts must investigate. PatternEx, then, trains on what human analysts think attacks look like in order to recognize them if they happen again in the future.

WHERE DO WE GO FROM HERE?

Given the ongoing shortage of skilled human IT resources, the Internet of Things, the resulting increase in endpoints, and the high skill-sets of attackers, there appears to be little doubt that AI

and machine learning will continue to dominate cybersecurity discussions, with the result being the continued introduction of automated cybersecurity products. Despite the likely reluctance of some parties to attend the cybersecurity dance, AI, machine learning, and deep learning can be broadly applied to on-premises, cloud, and critical-infrastructure environments without great difficulty. The object here obviously is to lessen dwell time, i.e., the time before which an attacker has had a chance to wreak havoc with your network. In fact, a very recent study states:

> Big Data analytics strengthens cybersecurity posture. Seventy-two percent of respondents say the use of Big Data analytics to detect advanced cyber threats is very important. In fact, 71% of heavy users are more likely to believe in the importance of Big Data analytics. Seventy-six percent of high users believe Big Data analytics is very important, as opposed to 67% of light user respondents.[48]

A November 2016 report by IBM's Institute for Business Value (IBV) titled "Cybersecurity in the Cognitive Era: Priming Your Digital Immune System,"[49] provides a similar indication of the value that security leaders are placing in this technology: 57% of security leaders indicated that cognitive security, IBM's term for the application of cognitive computing to cybersecurity, can significantly slow the efforts of cybercriminals.

The same IBM report also mentions that the most-cited benefits (by security leaders) of cognitive security will be the impact on the speed gap (improving response times), the intelligence gap (improving decision-making capabilities when it comes to incident detection and response), and the accuracy gap (improving the ability to determine incidents from mere events).

When it used Watson, its own AI data analytics platform, to analyze patterns in the survey responses provided by security leaders, IBM found that organization could be categorized in one of three maturity levels:

1. The Pressured (52%), characterized by funding and staffing challenges, and appearing to know relatively little about the benefits of cognitive security.
2. The Prudent (27%), a middle-of-the-road group, not yet ready to implement the technology, but more aware that the former group.
3. The Primed (22%), characterized by their familiarity with the technology, having a higher confidence in its value. This group also reported having the highest slice of funding for security relative to the IT budget (over 10% of the IT budget, as reported by 92% of those in this group).

When organizations leverage cognitive computing to improve their ability to lower dwell time (or even stop an attacker dead in his or her tracks), such improvements make it much harder for attackers to cause a great deal of damage, or steal a lot of critical IP. Artificial intelligence and machine learning are the key buzzwords of this year, and for good reason — this is where companies need to be to meet the cybersecurity threats of tomorrow.

"But delaying the implementation of artificial intelligence is not an option. We pay a significant price every day for not knowing what can be known..." —Guru Banavar, Chief Science Officer of Cognitive Computing at IBM

What are you waiting for?

ENDNOTES:

[1] See Enrique Dans, "Right Now, Artificial Intelligence Is The Only Thing That Matters: Look Around You," available at http://www.forbes.com/sites/enriquedans/2016/07/13/right-now-artificial-intelligence-is-the-only-thing-that-matters-look-around-you/#2046ba0b2480.

[2] See "The Natural Side of A.I.," available at http://www.wsj.com/articles/the-natural-side-of-a-i-1476799723 (quote from Ginni Rommety, CEO of IBM).

[3] See "Every Day Big Data Statistics – 2.5 Quintillion Bytes of Data Created Daily," available at http://www.vcloudnews.com/every-day-big-data-statistics-2-5-quintillion-bytes-of-data-created-daily/. As noted in this article, this amount of data will fill the equivalent of 10 million blue ray discs, which when stacked, would equal the height of 4 Eiffel Towers, stacked one on top of each other. "90% of the data in the world today has been created in the last two years alone." See "What is big data?" available at https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html. Frankly, this is not big data, it is humungous data.

[4] See "Big Data: The Management Revolution," available at https://hbr.org/2012/10/big-data-the-management-revolution/ar. ("[It] is estimated that Walmart collects more than 2.5 petabytes of data every hour from its customer transactions. A petabyte is one quadrillion bytes, or the equiv-alent of about 20 million filing cabinets' worth of text. An exabyte is 1,000 times that amount, or one billion gigabytes.").

[5] See "IBM's Watson Has a New Project: Fighting Cybercrime," available at https://www.wired.com/2016/05/ibm-watson-cyber-crime/ ("First, there's simply too much of it; according to a recent IBM report, the average organization sees over 200,000 pieces of security event data every single day. There's simply no way to keep up with it all.").

[6] See "AI can address cybersecurity personnel shortage," available at https://gcn.com/articles/2016/08/08/ai-cyber-staff-shortage.aspx.

[7] Id.

[8] See "Structured v. Unstructured Data," available at https://brightplanet.com/2012/06/structured-vs-unstructured-data/

[9] See "What is unstructured data," available at http://searchstorage.techtarget.com/feature/What-is-unstructured-data-and-how-is-it-different-from-structured-data-in-the-enterprise

[10] The field of big data analytics has created its own cottage industry and share of pundits as well. See e.g. "Unstructured Data: The Other Side of Analytics," available at http://www.forbes.com/sites/steveandriole/2015/03/05/the-other-side-of-analytics/#6fa4f5c99a86 ("I just Googled "big data analytics" and got 107,000,000 results in 0.29 seconds.")

[11] See "Why Data Is The New Oil," available at http://fortune.com/2016/07/11/data-oil-brainstorm-tech/?iid=rightrail-more.

[12] See "Harness the Power of Big Data: The IBM Big Data Platform," available at www.ibmbigdatahub.com/whitepaper/book-harness-power-big-data [hereinafter "the IBM Big Data Book")

[13] Id.

[14] See "Machine Learning in Business Use Cases," available at https://www.nvidia.com/object/ovum-machine-learning.html?gclid=CIW3lb_Uwc4CFYokhgodYa0DoQ#utm_source=PPC-US&utm_medium=PPC&utm_content=PPC&utm_campaign=Campaign-DGX-1-Ovum-Q2-PPC

[15] See "What Leading AI, Machine Learning And Robotics Scientists Say About The Future," available at http://www.forbes.com/sites/jlim/2016/10/12/what-leading-ai-machine-learning-and-robotics-scientists-say-about-the-future/#7cdcebd46b37.

[16] See https://en.wikipedia.org/wiki/Artificial_intelligence

[17] See "CIO Explainer: What is Artificial Intelligence?" available at http://blogs.wsj.com/cio/2016/07/18/cio-explainer-what-is-artificial-intelligence/. For those who are curious, in English, AI is based upon the formation of artificial neural networks which are modeled on the brain.

[18] See "5 things you need to know about A.I.: Cognitive, neural and deep, oh my!," available at http://www.computerworld.com/article/3040563/enterprise-applications/5-things-you-need-to-know-about-ai-cognitive-neural-and-deep-oh-my.html .

[19] See "Google DeepMind's AlphaGo: How it works," available at https://www.tastehit.com/blog/google-deepmind-alphago-how-it-works/.

[20] See "Google DeepMind's AlphaGo: How it works," available at https://www.tastehit.com/blog/google-deepmind-alphago-how-it-works/

[21] See "Now You Too Can Buy Cloud-Based Deep Learning," available at http://spectrum.ieee.org/computing/software/now-you-too-can-buy-cloudbased-deep-learning.

[22] See Deep Learning, available at https://www.technologyreview.com/s/513696/deep-learning/

[23] See "Report: Machine Learning Driving AI," available at http://www.datanami.com/2016/07/11/report-machine-learning-driving-ai/.

[24] See "5 things you need to know about A.I.: Cognitive, neural and deep, oh my!" available at http://www.computerworld.com/article/3040563/enterprise-applications/5-things-you-need-to-know-about-ai-cognitive-neural-and-deep-oh-my.html

[25] There actually is a third form that Google uses called "reinforcement learning." "This para-digm of learning by trial-and-error, solely from rewards or punishments, is known as reinforce-ment learning (RL). Also like a human, our agents construct and learn their own knowledge di-rectly from raw inputs, such as vision, without any hand-engineered features or domain heuris-tics. This is achieved by deep learning of neural networks." See "Deep Reinforcement Learn-ing," available at https://deepmind.com/blog.

[26] A very good discussion of unsupervised machine learning can be found here: http://www.aihorizon.com/essays/generalai/supervised_unsupervised_machine_learning.htm

[27] Google's "Deep Mind" computing division is a function of unsupervised machine or in this case "deep learning" using deep-layer automated neurons and a massive amount of computing horse power provided by GPU processing chips. See "NVIDIA GPUs - The Engine of Deep Learning," available at https://developer.nvidia.com/deep-learning; See Machine Learning in Business Use Cases, available athttps://www.nvidia.com/object/ovum-machine-learning.html?gclid=CIW3lb_Uwc4CFYokhgodYa0DoQ#utm_source=PPC-US&utm_medium=PPC&utm_content=PPC&utm_campaign=Campaign-DGX-1-Ovum-Q2-PPC . It was recently announced that Google would be partnering with the UK national healthcare system to create a supervised learning solution to diagnose sight threatening eye con-ditions. See "Google DeepMind pairs with NHS to use machine learning to fight blindness," available at https://www.theguardian.com/technology/2016/jul/05/google-deepmind-nhs-machine-learning-blindness ("At the heart of the research is the sharing of a million anonymous eye scans, which the DeepMind researchers will use to train an algo-rithm to better spot the early signs of eye conditions such as wet age-related macular degeneration and diabetic retinopathy.").

[28] See "Deep Learning: An Artificial Brain that Protects Against Cyber-Attacks," available at http://blog.deepinstinct.com/2016/05/31/deep-learning-an-artificial-brain-that-protects-against-cyber-attacks/.

[29] See "What is Cognitive Computing," available at http://whatis.techtarget.com/definition/cognitive-computing

[30] See "What Everyone Should Know About Cognitive Computing," available at http://www.forbes.com/sites/bernard-marr/2016/03/23/what-everyone-should-know-about-cognitive-computing/#9fdda15d6e72

[31] See "IBM Watson takes on cybercrime with new cloud-based cybersecurity technology," available at http://www.techrepublic.com/article/ibm-watson-takes-on-cybercrime-with-new-cloud-based-cybersecurity-technology/.

[32] Id.

[33] Watson is obviously a trademarked name of IBM.

[34] See "Why Cognitive Systems," available at http://www.research.ibm.com/cognitive-computing/why-cognitive-systems.shtml#fbid=qFtOtKE6CLW.

[35] Id.

[36] See Deep Learning, available at https://www.technologyreview.com/s/513696/deep-learning/

[37] IBM also stated it was focused recently on "augmented intelligence, systems that enhance hu-man capabilities, rather than replace it." See "IBM: AI should stand for Augmented Intelli-gence," available at http://www.informationweek.com/government/leadership/ibm-ai-should-stand-for-augmented-intelligence/d/d-id/1326496.

[38] One report on Microsoft's machine learning systems notes that this volume could amount to approximately "tens of terabytes a day and 13 billion login transactions." See "How much secu-rity can you turn over to AI?" available at http://www.csoonline.com/article/3040147/security/how-much-security-can-you-turn-over-to-ai.html.

[39] See "Darktrace's 'digital antibodies' fight unknown cybersecurity threats with machine learn-ing," available at http://www.zdnet.com/article/darktraces-digital-antibodies-fight-unknown-cybersecurity-threats-with-machine-learning/.

[40] See Darktrace Antigena, available at https://darktrace.com/products/; see also the company mentioned above, Deep Instinct, which is based upon a similar unsupervised machine learning premise, http://www.deepinstinct.com/.

[41] See "Microsoft bangs the cybersecurity drum with Advanced Threat Analytics," available at http://arstechnica.com/information-technology/2015/05/microsoft-bangs-the-cybersecurity-drum-with-advanced-threat-analytics/

[42] See "Microsoft Using Machine Learning to Strengthen Security," available at http://www.infosecurity-magazine.com/news-features/microsofts-machine-learning/

[43] See "FireEye to grow intelligence capabilities with iSight Partners deal," available at http://www.csoonline.com/article/3025273/security/fireeye-to-grow-intelligence-capabilities-with-isight-partners-deal.html.

[44] A description of FireEye's security orchestration product can be found here: http://swimlane.com/use-cases/security-orchestration-for-automated-defense/

[45] See "FireEye Reports Strong First Quarter Results as Growth of Platform Billings Acceler-ates," available at http://www.marketwired.com/press-release/fireeye-reports-strong-first-quarter-results-as-growth-platform-billings-accelerates-nasdaq-feye-2122095.htm

[46] See Cyber 20/20 Inc., available at http://www.cyber2020.com/

[47] See "System predicts 85 percent of cyber-attacks using input from human experts," available at http://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418

[48] See "Big Data Cybersecurity Analytics Research Report," available at http://go.cloudera.com/ponemon_ty

[49] See IBM: Welcome to the new era of cognitive security at http://www-03.ibm.com/security/cognitive/

CHAPTER 7:
CYBERSECURITY FIDUCIARY DUTIES OF DIRECTORS AND OFFICERS

PURPOSE OF THIS CHAPTER:

1. To identify the board of directors' role in cybersecurity oversight.
2. To identify relevant standards of liability in Delaware for breach of fiduciary duty.
3. To set forth cyber governance related questions boards should be asking their executives (and themselves) on a regular basis regarding the cybersecurity posture of their company.

"While Caremark many not have had the wide-ranging impact envisioned by some, and may actually have been overtaken by rules and regulations imposed by Congress, the SEC, and self-regulatory organizations, it still has served as a wake-up call to corporate America… emphasizing the need for increased monitoring of corporate affairs before they get out of hand."[1]

"For those worried that what happened to Sony could happen to you, I have two pieces of advice. The first is for organizations: take this stuff seriously. Security is a combination of protection, detection and response. You need prevention to defend against low-focus attacks and to make targeted attacks harder. You need detection to spot the attackers who inevitably get through. And you need response to minimize the damage, restore security and manage the fallout."[2]

"Cybersecurity threats know no boundaries. That's why assessing the readiness of market participants and providing investors with information on how to better protect their online investment accounts from cyber threats has been and will continue to be an important focus of the SEC. Through our engagement with other government agencies as well as with the industry and educating the investing public, we can all work together to reduce the risk of cyber attacks."[3]

Picture courtesy of www.csrandthelaw.com

Among the most notable cyber breaches in the public company sector in 2013 was the one that hit Target Corporation (40 million estimated credit and debit cards allegedly stolen, 70 million or more pieces of personal data also stolen, and a total estimated cost of the attack to date of approximately $300 million).[4] It was remarkable on several levels; not just because of the enormity of the breach and its aftermath, but also because it focused attention on public company directors with respect to their duties to oversee the enterprise risk management of their organization. Justified or not, ISS issued a voting recommendation against the election of all members of Target's audit and corporate responsibility committees — seven of its 10 directors — at the up-coming

annual meeting. ISS' reasoning was that, in light of the importance to Target of customer credit cards and online retailing:

> "[the] failure of the committees to ensure appropriate management of these [cyber] risks set the stage for the data breach, which has resulted in significant losses to the company and its shareholders.[5] Though the ISS bid was unsuccessful, the ISS report "puts corporate board members on notice to treat the risks associated with cyber attacks more seriously, particularly directors at retailers which store vast amounts of data like credit card numbers and personal information that cyber criminals seek. Other retailers like Michaels Stores Inc. and Neiman Marcus Group have fallen victim to cyber attacks where credit-card information was compromised. The ISS move is raising a red flag about risk oversight that is a growing issue for boards…."[6]

If the reputational black eye suffered by Target and its fellow retailers was not enough of a "red flag" to the U.S. corporate community, then maybe the cyber breach lawsuits filed in 2014 were. Calendar year 2014 progressed with breach after breach, and lawsuits piled up against companies that suffered cyber attacks. At least 140 customer lawsuits were brought against Target alone, which have recently been allowed to proceed past the motion to dismiss phase (these do not include suits brought by banking partners against Target relating to the breach, which have also been allowed to proceed).[7] At least 50 class actions have been filed against Anthem Healthcare relating to its data breach in 2015. At least 31 actions have been filed against Home Depot arising out of its breach.[8] And then there was Sony Pictures, where at least six lawsuits have been filed by ex-employees relating to the late November 2014 breach.

Clearly over the last year, the risk calculus for cybersecurity breaches has changed in many different ways:

1. Prior to 2014 the risk of customer class actions was thought to be negligible. Not today. The Adobe, Target, and Neiman Marcus lawsuits have all survived motions to dismiss their consolidated complaints;
2. The average cost of responding to a cyber attack for U.S. companies has been increasing steadily;
3. The number of cyber attacks has increased significantly year over year to the point where one cannot say these are random events; and
4. The destructiveness of the cyber attacks and rampant theft of customer, employee, and patient data has now been evidenced with 18 months of hard data.

This leads us to the board of directors. Charged with generally overseeing the affairs of the company, a board must now factor into its analysis not only the hazard risk that its company may face (i.e. property damage, flood damage or natural catastrophes, like hurricanes, and earthquakes), but also the cyber risk its company may face. Unlike many other aspects of directing the affairs of a public company, like overseeing its financial reporting function and obligations, "cyber" is new for many directors, and certainly far from intuitive. For this reason, this chapter will focus specifically on the responsibilities of public company directors to oversee their company's cybersecurity program (within the framework of the company's enterprise risk management structure), the basic questions directors should be asking about a company's cybersecurity program, incident response and crisis management programs, and the potential value of a standalone cyber insurance policy to transfer some of the risk of a cyber attack to a reputable insurance carrier.

Directors' Duty of Oversight With Respect to Cybersecurity/Other Duties and Regulations Lurking About for Directors

> [T]he board cannot and should not be involved in actual day-to-day risk *management*. Directors should instead, through their risk *oversight* role, satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are consistent with the company's strategy and risk appetite, that these policies and procedures are functioning as directed, and that necessary steps are taken to foster a culture of risk-aware and risk-adjusted decision making throughout the organization. The board should establish that the CEO and the senior executives are fully engaged in risk management and should also be aware of the type and magnitude of the company's principal risks that underlie its risk oversight. Through its oversight role, the board can send a message to management and employees that comprehensive risk management is neither an impediment to the conduct of business nor a mere supplement to a firm's overall compliance program, but is instead an integral component of strategy, culture and business operations.[9]

Thus, as a general rule, "the business and affairs of every corporation…shall be managed by or under the direction of a board of directors…." *See D.G.C.L. Section 141(a)*. A public company director's "duty of oversight" or "fiduciary duty to monitor" generally stems from the concept of good faith. As noted in the seminal Delaware Chancery Court case, *In re Caremark Int'l, Inc. Derivative Litigation, 698 A.2d 959 (Del.Ch. 1996)*, as a general matter "a director's obligation includes a duty to attempt in good faith and loyalty to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that the failure to do so in some circumstances, may, in theory, at least render a director liable for losses caused by non-compliance with applicable legal standards."

This simple statement, however, does not come without a high hurdle to meet. To find liability under Chancellor William Allen's duty of oversight, a plaintiff must either show that:

1. The board must have failed to provide reasonable oversight in a "sustained or systemic" fashion; and
2. The information reporting system on which the board must have relied must have been an "utter failure."[10]

Importantly, under *Caremark*, that actual failure to prevent wrongdoing does not in and of itself mean the information reporting system "is an utter failure." A court must also consider the design of the system, how it was tested and maintained by management, and how employees were trained under the provisions set forth in the system. Caremark thus sets forth a holistic approach to determining the level of board oversight. In sum, trying to set up a system of oversight and control over cybersecurity with appropriate supervision and control is much better than not trying at all and sticking one's head in the sand.[11]

In a later Delaware Supreme Court case, *Stone v. Ritte*r, the court refined the *Caremark* standard as a two part test, where liability stems from either:

1. Utterly failing to implement any reporting or information system or controls; or
2. Having implemented such system or controls, *consciously failing* to monitor or oversee its operations.[12]

Placing the liability for failure to monitor in terms of a "conscious failure," the Delaware Supreme Court placed an inherent *scienter* requirement for plaintiff's attempt to surmount. But the hope obviously is that such a suit never comes to fruition based upon a board's conscious attempt to stay informed about the enterprise risk management of its company. Indeed, the business judgment rule generally protects a director's "informed" and "good faith" decisions unless the decision cannot be attributed to any rational business purpose, or the directors breached their duty of loyalty in making such decision.[13]

In today's world it would be hard to question that cybersecurity should not be part of any organization's enterprise risk management function, and thus, by inference, part of any director's duty of oversight. Indeed, the plaintiffs' securities class action bar has filed two shareholder derivative actions against the boards of directors of both Target and Wyndham Worldwide Hotels as a result of their publicly reported cyber breaches. In these complaints, the plaintiffs alleged that the boards "failed to take reasonable steps to maintain its customers' personal and financial information," and, specifically with respect to the possibility of a data breach, that the defendants failed "to implement any internal controls at Target designed to detect and prevent such a data breach."[14] Indeed, SEC Commissioner Luis Aguilar confirmed this exact cyber governance point in his June 10, 2014 speech, titled, "Cyber Risks in the Boardroom." He said:

> [E]nsuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities. In addition to the threat of significant business disruptions, substantial response costs, negative publicity, and [the] lasting reputational harm [that could result from a cyber attack], there is also the threat of litigation and potential liability for failing to implement adequate steps to protect the company from cyber threats.[15]

As was made clear by the panelists' questioning in an SEC Cyber Roundtable on March 26, 2014, *see Webcast of SEC Cyber Roundtable, dated March 26, 2014*,[16] there are other reasons for directors to be intimately involved with decisions concerning a company's cybersecurity, i.e., "the regulators." Over the last several months, not only has the SEC been more involved generally with cyber "thinking" and security issues, but also the Office of Compliance, Inspections and Examinations of the SEC (governing investment advisors and asset managers) and FINRA are in the game.[17] So is the FTC, FDIC, FFIEC, OCC[18] and FCC,[19] as well as state regulators such as the New York State Department of Financial Services. Each of these organizations has its own exhaustive list of factors or areas of examination/consideration. They are long and extensive. And we have yet to see whether the SEC will issue additional guidance to public companies concerning what information is required to be disclosed to investors regarding cybersecurity incidents.[20]

The failure to adhere to regulations or guidance on cybersecurity can be troublesome because of the concept of "red flags," i.e., danger signs that something is wrong within the organization. There are all sorts of red flags, and many do not rise to the level of trouble. For instance, the fact that a company has thousands of potential cyber incident intrusion alerts every day might be viewed by an SEC OCIE examiner as a normal occurrence within any major financial organization. The fact that none of the potential intrusions (or alerts) were elevated for further review, or otherwise followed up upon, or that the company has no written cyber incident response plan might be viewed as a huge "red flag" that could lead to an unfavorable report or even a fine or penalty by the regulatory organization. If that red flag is not followed up upon by a board of directors or senior management and something worse happens (i.e. a major breach), the red flag could serve as a very convenient base on with to build a civil litigation case. "Red flags are…useful when they are either

waived in one's face or displayed so that they are visible to the careful observer."[21] Given that many of the major cyber breaches are relatively new, we have yet to see how regulators will respond to any particular fact pattern.

DECISION IN THE TARGET DERIVATIVE ACTION

"On July 7, 2016, District of Minnesota Judge Paul Magnuson, in reliance on the report of the special litigation committee appointed to investigate the claims, and in the absence of opposition from the plaintiff, granted the motions of the special litigation committee and of the defendants and dismissed the consolidated cybersecurity-related derivative litigation that had been filed against Target Corporation's board."[22] One commentator noted several takeaways from the Target derivative action decision:

"Directors and officers can look to the Target SLC report as a guidepost for the types of measures that should be a part of a robust information security program to help establish that they have discharged their fiduciary duties. Factors that the SLC reviewed, considered, and relied upon included:

- "The existence of network-security insurance that mitigated the cost of the breach.
- "Pre-breach policies and procedures that incorporated technical, administrative, and physical controls for data security.
- "Pre-breach vendor security procedures.
- "Employee training related to data security requirements."[23]

DECISION IN THE WYNDHAM CYBER DERIVATIVE ACTION

Though there have been several cases in the Financial Crisis context that have been decided based upon a *Caremark/Stone v. Ritter* analysis, there have been no decisions in the cybersecurity context decided "on the merits" other than the recent one by Judge Stanley Chesler in the Wyndham derivative action. Though the facts around the commencement of the Wyndham derivative action were different than other actions brought following the announcement of a breach (the Wyndham derivative action was filed 3 1/2 years after the original data breach, while a derivative action against Target, for example, was filed one month after Target's breach[24]), the Wyndham derivative action was dismissed by Judge Chesler on a factual record that the board of directors had not only met many times before the breach to discuss and implement cybersecurity procedures and implement them, but it also held 14 quarterly meetings after the attack to discuss the company's cybersecurity procedures and proposed enhancements. Furthermore, the audit committee (which investigated the facts of the attacks) met at least 16 times to review cybersecurity. This record gave the court ample opportunity to conclude that the board's decision to refuse the shareholder's demand that the company investigate the breaches and sue the company's personnel that were involved was protected by the business judgment rule. (Note: At the time of publication, the Court in the Home Depot data breach derivative litigation also dismissed the derivative litigation on demand futility grounds.)

Judge Chesler's decision obviously raises more questions than it answers. What would have happened if there was not an extensive factual record of board involvement in the company's cybersecurity affairs, and the company had not taken both pre- and post-corrective action? Or worse, if there was a very sketchy record of board involvement showing that the board was uninterested in the firm's cybersecurity procedures and did not receive regular reports on cyber-

security prevention and detection measures. On that note, the 2015 U.S. State of Cybercrime Survey issued by PwC reveals the startling fact that despite 18 months of intense PR pressure around cybersecurity:

> "Our research shows that one in four (26%) respondents said their chief information security officer (CISO) or chief security officer (CSO) makes a security presentation to the board only once a year, while 30% of respondents said their senior security executive makes quarterly security presentations. But 28% of respondents said their security leaders make no presentations at all.[25]

Not every company will have 3 1/2 years to fill a factual record prior to the commencement of litigation. And, as clearly noted by the PwC report, not every company spends a lot of time discussing cybersecurity issues. What history is teaching us is cybersecurity breaches have the potential to not only create regulatory risk, but also risk to the directors and officers of the company for breach of fiduciary duty for failure to oversee the company's cyber risks. In addition to questions regarding cyber insurance, questions regarding the company's directors and officers insurance for cyber related actions may also arise.

CYBER GOVERNANCE SCORECARD FOR DIRECTORS TO CONSIDER

One of the key takeaways of the decision in the Wyndham derivative action is that board conduct matters, and will be reviewed, not only by the court of public opinion, but also potentially by Delaware Chancery Court or other courts around the country. Wyndham teaches that having a factual record and documentation of board action and involvement is key to getting share-holder derivative actions either dismissed or settled on a reasonable basis.

Here are some basic questions public company directors should be considering when reviewing their company's cybersecurity framework:

1. What part of the board should handle examination of cybersecurity risks? Should it be the whole board? Should this responsibility be assigned to the audit committee? The risk committee (if there is one)? Should the board create a "cyber committee" to exclusively deal with these issues? Should additional board members be recruited who have specific cybersecurity experience?

2. How often should the board (or committee) be receiving cybersecurity briefings from management? In this world, which moves at the speed of light and in which cyber breaches are reported daily, are quarterly briefings enough? Should the board be receiving monthly briefings? More frequent (given the company's industry, e.g., tech/IP company)?[26] Another recent study notes:

   > "At the other end of the spectrum, only 25% of respondents said their full board is involved in cyber risks."[27]

   Is this very low number because the full board of directors designated the oversight of cyber risk to another board committee, like the audit or risk committee, or is it because companies are still not appreciating the cyber risks their companies face? You decide. The same PwC report also notes, "It's also essential that boards treat cybersecurity as an overarching corporate risk issue rather than simply an IT risk. Many have yet to adopt this approach, however. Almost half (49%) of boards view cybersecurity as an IT risk, while

42% see cybersecurity through the lens of corporate governance."[28] Whatever the answer, cybersecurity is very much like my seven-year-old twins — it needs the attention of its parents, the board of directors.

3. Given the sheer complexity and magnitude of many cybersecurity issues, should the board hire its own "cyber advisers" to consult on cybersecurity issues and be available to ask questions of the company's senior management, CISO and CIO?

4. What are the company's highest value cyber assets (e.g. credit card information, healthcare records), and where are they located (e.g. company servers, the cloud, a third party vendor)? And what is currently being done to protect those assets? If those highest value assets are not IP assets, but rather infrastructure assets, what is being done to protect those assets from a cyber attack?[29]

5. What are the greatest threats and risks to the company's highest value cyber assets, and who are the potential threat actors (nation-states, cyber criminals)? Does the company's human resources and financial capital line up with protecting those high value assets?

6. What is the company's volume of cyber incidents on a weekly or monthly basis? What is the magnitude/severity of those incidents? What is the time taken and cost to respond to those incidents?

7. What would the "worst case" cyber incident cost the company in terms of both lost business (because of downtime to systems that were attacked and need to be brought back), and in terms of lost business because of the harm to the company's reputation as a result of the attack?

8. What is the company's specific cyber incident plan, and how will it respond to customers, clients, vendors, the media, regulators, law enforcement, and shareholders? Does the company have a crisis management plan to respond to all these various constituencies, as well as the media (both print and electronic/high activity bloggers)? Finally, has the cyber incident plan been tested (or "war-gamed") so that it is ready to be put into place on a moment's notice?

9. What cybersecurity training does the company give its employees on social media, spear-phishing scams, and email hijacking?

10. What sort of program does the company have in place to monitor the level and robustness of the "administrative privileges" that it gives to its employees and executives?

11. What sort of cyber due diligence does the company perform with respect to its third-party service providers and vendors?[30]

12. In a mergers and acquisitions context, what is the level of "cyber due diligence" that is done as part of the consideration of any acquisition?

13. Has the company performed an analysis of the "cyber-robustness" of its products and services to analyze potential vulnerabilities that could be exploited by hackers?

14. Should the company consider adopting, in whole or in part, the NIST Cybersecurity Framework as a way or method of showing affirmative action and due care to protect the company's IP assets?[32]

15. Finally, does the company purchase cyber insurance? If not, why, given the risks involved and the tremendous costs associated with remediating a sophisticated cyber breach?

This list could go on for pages, but it won't, since we believe it's served its purpose, i.e., there are plenty of tough questions that directors need to ask senior management and senior IT staff; not just once a quarter, but as needed in order to meet the ever-changing threat and risk environment. Directors may also need their own advisors and professionals to help them fulfill their oversight duties in assessing risks and asking the tough questions of management. As the Sony cyber attack proved, cyber is not just an IT department's problem; it is everyone's problem — especially the board of directors. Full engagement is critical and may be essential for the survival and growth prospects of the company. We submit that the day where 15 minutes of board attention for cybersecurity was acceptable is a thing of the past. Cybersecurity is the issue of the day. It must be treated as the issue of the day.

ENDNOTES:

[1] See "Revisiting Caremark and a Director's Duty to Monitor: The Chancery Court's wake-up Call to Directors," found at http://www.conference-board.org/retrievefile.cfm?filename=DN-004-10.pdf&type=subsite.

[2] See "Sony Made It Easy, but Any of Us Could Get Hacked," available at http://www.wsj.com/articles/sony-made-it-easy-but-any-of-us-could-get-hacked-1419002701.

[3] Statement by SEC Mary Jo White, which is available at https://www.sec.gov/spotlight/cybersecurity.shtml

[4] See "The Target Breach: By the Numbers" at http://krebsonsecurity.com.

[5] See "ISS's View on Target Directors Is a Signal on Cybersecurity," available at http://online.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278?mod=_newsreel_4; Following Target's announcement that affected 40 million cus-tomers and 46 percent profit loss, CIO Beth Jacob, who oversaw Target's web site and internal computer systems since 2008 resigned in March 2014. Shortly thereafter, the board decided it was time for new leadership and CEO Gregg Steinhafel resigned in early May 2014. See "9 data breaches that cost someone their job," available at http://www.csoonline.com/article/2859485/data-breach/9-data-breaches-that-cost-someone-their-job.html#slide2.

[6] Id.

[7] Note also that Target board of directors was sued in a shareholder derivative class action, and Target was itself was named in securities class action arising out of the breach.

[8] We note that there is also current pending a Delaware Section 220 "books and records" demand made against Home Depot arising out of the cybersecurity breach. See "Next Up: A Home Depot Data Breach-Related D&O Lawsuit?" available at http://www.dandodiary.com/2015/06/articles/cyber-liability/next-up-a-home-depot-data-breach-related-do-lawsuit/.

[9] See "Risk Management and the Board of Directors – An Update for 2012," available at http://blogs.law.harvard.edu/corpgov/2012/01/03/risk-management-and-the-board-of-directors-an-update-for-2012/.

[10] *Caremark*, 698 A.2d at 970-971.

[11] See "Cybersecurity and the board of directors: avoiding personal liability," found at http://blogs.reuters.com/financial-regulatory-forum/2013/07/25/cybersecurity-and-the-board-of-directors-avoiding-personal-liability-part-i-of-iii/

[12] See *Stone v. Ritter*, 911 A.2d at 362, 370 (2006) (emphasis added).

[13] See generally Holland, "Delaware Director's Fiduciary Duties: The Focus on Loyalty," available at http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1334&context=jbl.

[14] See "Wyndham Worldwide Board Hit with Cyber Breach-Related Derivative Lawsuit," at http://www.dandodiary.com/2014/05/articles/cyber-liability/wyndham-worldwide-board-hit-with-cyber-breach-related-derivative-lawsuit/ ("the Wyndham Derivative Action"); see "Target Corporation Cybersecurity-Related Derivative Litigation Dismissed," available at http://www.dandodiary.com/2016/07/articles/cyber-liability/target-corporation-cybersecurity-related-derivative-litigation-dismissed/ (hereinafter, the "Target Dismissal Article").

[15] See Commissioner Aguilar's speech at http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

[16] This webcast is available at http://www.sec.gov/news/otherwebcasts/2014/cybersecurity-roundtable-032614.shtml

[17] See "Cybersecurity and Financial Firms: Bracing for the Regulatory Onslaught," at http://www.strozfriedberg.com/wp-content/uploads/2014/04/Cybersecurity-and-Financial-Firms-Bracing-for-the-Regulatory-Onslaught_BloombergBNA_Stark_April2014.pdf

[18] See, e.g., "Cybersecurity Assessment General Observations and Statement," available at http://www.occ.gov/news-issuances/bulletins/2014/bulletin-2014-53.html.

[19] See. e.g. "Cybersecurity and Communications Reliability Division, Public Safety and

Homeland Security Bureau," available at http://www.fcc.gov/encyclopedia/cybersecurity-and-communications-reliability-division-public-safety-and-homeland-securi.

[20] Its original guidance was issued in 2011, well before events of the recent past. See "CF Disclo-sure Guidance, Topic No. 2," at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[21] See *In re Citigroup Shareholder's Litigation*, 2003 WL 21384599 (Del.Ch.June 5, 2003).

[22] See The Target Dismissal Article

[23] See "Target's Directors and Officers Dismissed from Data Breach Lawsuit," available at http://www.ulmer.com/news/targets-directors-officers-dismissed-data-breach-lawsuit/.

[24] See "Target Directors and Officers Hit with Derivative Suits Based on Data Breach," found at http://www.dandodiary.com/2014/02/articles/cyber-liability/target-directors-and-officers-hit-with-derivative-suits-based-on-data-breach/

[25] See "PwC 2015 US State of Cybercrime Survey," available at http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf.

[26] See "4 Ways to Engage Executives in Cyber Risk," available at http://deloitte.wsj.com/cio/2015/07/20/4-ways-to-engage-executives-in-cyber-risk/ (noting, in a survey of retail executives in 2014 that "just 37 percent of survey respondents [retail CIO's] say their organizations report to the board on a quarterly basis regarding their cyber risk posture, while 44 percent say their organizations never report on cyber risk to any business stakehold-ers.").

[27] See "US cybersecurity: Progress stalled: Key findings from the 2015 US State of Cybercrime Survey," available at http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf.

[28] Id.

[29] See "NSA Director Warns of 'Dramatic' Cyberattack in Next Decade," available http://www.wsj.com/articles/nsa-director-warns-of-dramatic-cyberattack-in-next-decade-1416506197.

[30] See "Trustwave 2013 Global Security Report," noting that 63% of all investigations showed that a cyber breach emanated from a third-party vendor or IT administrator, found at http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf.

[31] See "Why You Should Adopt the NIST Cybersecurity Framework," available at http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf ("If, for instance, the security practices of a critical infrastructure company are questions in a le-gal proceeding, the Court could identify the Framework as a baseline for "reasonable" cyberse-curity standards"); See also, "Understanding and Implementing the NIST Cybersecurity Framework," available at http://corpgov.law.harvard.edu/2014/08/25/understanding-and-implementing-the-nist-cybersecurity-framework/ ("By choosing to implement the Framework (or some part of it) sooner rather than later, organizations can potentially avoid the inevitable con-clusion (or parallel accusation by a plaintiff's attorney) that they were "negligent" or "inatten-tive" to cybersecurity best practices following disclosure of a cyber breach. Organizations using the Framework should be more easily able to demonstrate their due care in the event of a cyber attack by providing key stakeholders with information regarding their cybersecurity program via their Framework profile.").

CHAPTER 8:

INSURANCE FOR CYBER EXPOSURES; CRITICAL CONSIDERATIONS FOR EFFECTIVE INSURANCE PURCHASING[1]

PURPOSE OF THIS CHAPTER:

1. Help risk managers boards of directors understand that insuring cyber exposures involves more than purchasing a single type of policy.
2. Stress that cyber should be viewed as a peril that can (or soon will) impact most, if not all, of the policies. within a commercial insurance portfolio.
3. Provide detailed insight and specific considerations for structuring an appropriate "cyber event-ready" insurance structure.

BTC PIPELINE EXPLOSION – INSURANCE GAME CHANGER?

In "Navigating the Cybersecurity Storm", we included a chapter that highlighted available standalone cybersecurity insurance for data breach claims. At the time, standalone cybersecurity insurance was making its breakthrough in the insurance markets (post-Target, post-Home Depot, post-Sony) as a method to transfer some of the risk of a cybersecurity breach to an insurance company for a fair premium. These policies provided for recoveries of (among other things) breach notification and PR costs, forensic and remediation costs, and the costs of third party litigation brought by consumers and patients.

What we did not cover in Book One was the availability of coverage for property damage and third party personal injury claims suffered as a result of a cybersecurity breach. We did not because such coverage was, at best, circumspect, difficult to procure, and confusing to navigate. Since we wanted to keep book one in plain English, and since reading insurance policies is sometimes likened to reading hieroglyphics, we thought, "Lets save this topic for another day."

Well, it's another day, and over the last 12 months the markets have responded to the need for cybersecurity insurance for critical infrastructure claims with some better (and simpler) insurance products, providing insureds with more fulsome coverage for this critical risk. Here is some background.

On August 7, 2008, a segment of the Baku-Tbilisi-Ceyhan (BTC) pipeline, largely located in Turkey, exploded. The impact was meaningful: 30,000 barrels of crude oil spilled, pipeline operations were disrupted for three weeks, Azerbaijan faced approximately $1B in revenue losses/ delays, and BP lost $10 million in tariff revenue. Viewed in a vacuum, nothing about this event would be viewed as extraordinary — the pipeline is located in a region of political instability and critical infrastructure assets are frequent targets, and from time to welds, valves, or other pipeline components can fail.

In 2009 speculation began to surface that this event might actually be extraordinary after all; precipitated by cyber means, and specifically by hackers employed by the Agency of Russian Special Services. By December 2014 reports were concluding that the event was in fact caused via cyber means — hackers accessed the pipeline's control systems, duped the operators by disabling the surveillance equipment, and intentionally caused the over-pressurization. On December 10, 2014, *Bloomberg Technology* featured an article titled, "Mysterious '08 Turkey Blast Opened New Cyberwar," calling the blast a watershed event and indicating that "the main weapon was a keyboard."[2]

On June 19, 2015, the SANS Industrial Control System Blog published a post titled, "Closing the Case on the Reported 2008 Russian Attack on the BTC Pipeline," and deemed the event not to be cyber predicated. The SANS report relied on additional investigations, including one published by *Sueddeuntsche* (a German national newspaper) refuting some of the key conclusions in the *Bloomberg* article and others. In particular, the German article contained insight from an internal audit that explosives had been found at the scene of the event and that there was no wireless network installed for the valve stations.

Big deal, right? What's wrong with a thought provoking and lessons-learned-producing debate about whether an explosion was cyber predicated or not? The timing of how it played out doesn't raise any suspicions, after all — prior to the revelation of Stuxnet in 2010, very few individuals would have immediately jumped to a cyber-centric conclusion, or even thought of that possibility. Additionally, root cause analysis on burning-hole-in-the-ground events like these can be extremely challenging due to a dearth of details and evidence. That holds true even with technology in the mix, as some critical infrastructure assets are entirely "air gapped," meaning no outside connectivity, so post-event there is not much difference between the computer system that may have caused the event or the faulty weld that may have caused the event: both are largely destroyed.

Except perhaps when insurance implications are considered. Put yourself in the shoes of the property insurer of this asset (note: the authors of this chapter have no knowledge of any insurance implications of this event; this paragraph is written entirely on general insurance industry insight). Sometime in 2009, you tender a substantial payment to the owner of the pipeline despite the chatter about the event being caused by cyber means and despite the fact that the property policy that you issued contains a CL-380 exclusion (see below). Come 2014 and the event is concluded by reputable sources to have been cyber predicated. Do you ask for a return of the policy proceeds? Can you? One year later, the situation reverts back to the event having not been cyber predicated. Oh-boy. Return the funds to the policyholder with an apology note and box of chocolates? Or perhaps you might have been better served not paying policy proceeds and instead litigating over the nature of the event, which probably would have taken you past 2014 anyways.

Welcome to the new reality of risk in a post-Stuxnet world. Cyber exposure is no longer limited to credit card breaches, losses of Social Security Numbers, and system shutdowns; it's everything: potential pipeline explosions, hacking of medical devices, automobile navigation systems failures, waterway manipulations, the non-tangible destruction of technology assets, and much more. For insurers, the implications are many, as evidenced by the theoretical implications on the insurance portfolio of the BTC pipeline's owner:

1. **PROPERTY DAMAGE TO THE ASSET** — Likely covered by an all-risk property insurance policy, barring any cyber or electronic data exclusions.
2. **PROPERTY DAMAGE TO THE ASSET IF THE EVENT IS DEEMED TO BE AN "ACT OF TERRORISM"** —Covered by the terrorism insurance policy, barring any cyber exclusions.
3. **LOSS OF REVENUE DAMAGES TO THE ASSET OWNER** — Likely covered by the property insurance policy, assuming that business interruption is elected and barring any cyber exclusions.
4. **THIRD PARTY BODILY INJURY AND PROPERTY DAMAGE** — Likely covered by the general liability and excess liability policy, barring any cyber exclusions (and barring any terrorism exclusions if the event is deemed such).
5. **ENVIRONMENTAL DAMAGE** — Likely covered by the environment liability policy, barring a any cyber exclusions (and barring any terrorism exclusions if the event is deemed such).
6. **BODILY INJURY TO EMPLOYEES** — Likely covered by worker's compensation insurance, barring any cyber exclusions, or covered by applicable governmental programs, depending on jurisdiction.
7. **RESULTING DIRECTORS AND OFFICERS LITIGATION** — Likely covered by the D&O policy, barring any cyber exclusions.
8. **CRISIS MANAGEMENT AND PUBLIC RELATIONS EXPENSES** — Should be covered by a cyber insurance policy, except that most off-the-shelf cyber policies contain very property damage and bodily injury exclusions, which may dramatically limit the policy's response.

As the hypothetical insurance implications of the BTC pipeline attack evidence, there are numerous considerations and potential pitfalls, of which risk managers, senior executives, and boards of directors need to be cognizant.

THE CURRENT AND EVOLVING INSURANCE INDUSTRY LANDSCAPE

The wide availability of cyber insurance as of this publication should surprise very few, if anyone, in the risk management community. It's arguable that no emerging insurance product has received as much attention as cyber insurance over the past few decades, save potentially directors and officers insurance in the 1980s. Cyber insurance gets brought up by brokers at every opportunity, insurers are continually attempting to out-duel each other with respect to coverage extensions and pricing considerations, and every cybersecurity technology company is attempting to assist in the space. In short, every cybersecurity vendor is "all in" on cybersecurity insurance, much akin to hungry bluefish circling moss bunker in the Long Island Sound. The trajectory and perceived importance of the product has even led some to suggest that failing to purchase cyber insurance should be considered a breach of fiduciary duty by directors and officers.

What's largely been overlooked in the product hoopla and in a post-Stuxnet risk climate is the big picture on cyber risk and cyber insurance: cyber should be considered a peril, or a loss causing event, and one that can impact the entire financial-to-tangible-risk spectrum. This reality opens the door to the possibility that a cyber event can impact various types of commercial insurance products, and is not limited to the boundaries of what most in the insurance industry have traditionally sold under the cyber insurance masthead.

Those types of "traditional" cyber insurance policies are largely centered on breaches of personally identifiable information, business interruption losses from malicious systems interruptions, and certain other slices of resultant financial expenses such as cyber extortion payments or the cost to replace destroyed data or code. Subsequent policy evolutions included coverage for civil penalties relating to breaches, certain regulatory penalties such as HIPAA fines and PCI-DSS penalties, and non-malicious systems interruptions. Overall these policies provide a healthy scope of coverage but should not be considered a one-stop shop to insure the entirety of cyber risk.

A meaningful limitation of traditional cyber policies lies is that most, if not all, do not cover losses relating to bodily injury and property damage, usually in the form of exclusion language that reads:

This policy does not cover costs or losses arising out of, attributable to, or based upon Bodily Injury or Property Damage.

In response to that coverage limitation and the new reality that cyber events can cause physical damage, the insurance industry has released a new wave of products designed to cover cyber physical damage and other emerging exposure categories. Some policies take the form of Difference-in-Conditions policies that fill holes caused by certain coverage limitations that will be subsequently discussed, some are intended to act as primary insurance and respond first to the loss, and others harmonize coverage segments that are better together than apart — such as cyber and physical damage predicated business interruption coverage. For instance, one major insurer now offers coverage specifically for cyber predicated property damage, third party bodily injury or property damage, product liability, as well as combined physical and non-physical business interruption. These developments prove the insurance industry is embracing the evolving world of cyber risk, and is aware of important considerations for critical infrastructure industries like the energy sector, whose primary cyber risk likely concerns the manipulation or failure of industrial control systems or operational technology.

Despite the positive new coverage developments, a debate over how to appropriately treat the peril of cyber has been ignited. Is the appropriate treatment the exclusion of cyber in its entirety from every type of traditional insurance coverage and the continued development of cyber-specific coverage structures? Or is the appropriate treatment the inclusion of cyber into existing coverage lines, underwritten alongside the basket of existing perils? There are plusses and minuses to both approaches, and with the resolution of that debate years away, the only short term certainty is the availability of a variety of options to insure cyber risk, with no single policy providing a comprehensive solution.

PRACTICAL ADVICE TO MAXIMIZE CYBER RISK TRANSFER EFFECTIVENESS

Certainly there is a lot to consider to get things right, or at least not wrong, but we believe that cyber risk transfer effectiveness can be achieved by following a few critical steps:

1. UNDERSTAND YOUR CYBER EXPOSURE

This step is an absolute must unless your insurance strategy relies on blind faith. We recommend utilizing a loss scenario based approach — start by generating a set of realistic loss scenarios based on the firm's utilization of computer technology and digital communications across the enterprise. A few starter scenarios could include:

- Breach of personally identifiable information (customer and employee information), protected health information, or other confidential data (such as corporate financials).
- Network business interruption (non-physical damages business interruption, such as that which could be caused by a distributed denial of service attack (DDoS) or a widespread outage of the firm's network).
- Firmware corruption of the firm's technology infrastructure.
- Attack on, or failure of, the firm's industrial control/SCADA systems and resulting tangible damage.
- Product liability (for example a software defect in a medical device or automobile that enables cyber attackers to cause bodily injury).
- Product recall (due to discovered vulnerabilities in the software that could be leveraged to cause tangible damage).
- Social engineering leading to fraudulent electronic funds transfer.
- Theft of key intellectual property and/or trade secrets.

It's important to capture as wide of a set of scenarios as possible, especially for firms that depend on operational technology or industrial control systems.

Second, select the subset of scenarios that would result in the most organizational heartburn. Which of those scenarios, if they actually occurred, would produce a very bad day. Or, said another way, which scenarios look and feel like they would exceed the organization's normal risk tolerance?

Finally, role play each scenario and use the organization's inherent knowledge of how it operates. Use related information from other risk management exercises or losses that have previously occurred, and, where available, information from outside reports like the Verizon Data Breach Incident Response report, in order to generate a realistic estimate of what each scenario would cost if it did occur. In most instances we find that the information necessary to construct and estimate a realistic cyber scenario is readily available, but never before analyzed under a cyber lens.

2. UNDERSTAND YOUR CURRENT INSURANCE PORTFOLIO

Purchasing a new insurance policy is not a foregone conclusion of our suggested process. Viewing cyber as a peril in conjunction with your existing insurance portfolio most often produces a conclusion that certain cyber exposures are already, in fact, covered. For instance, a crime policy with a coverage grant for electronic funds transfer fraud or a social engineering extension provides affirmative coverage for cyber-predicated funds theft. Many kidnap and ransom policies contain coverage grants for cyber extortion or ransomware payments. Definitely consider property, as some property insurers include coverage extensions for non-physical damage to data, programs, and software. The following are a few key considerations for conducting an effective analysis:

a. Understand the policy triggers — What type of perils give rise to coverage under the policy? Is your property policy "all-risk" or "named perils"? The latter might allow the insurer a means out, based on the argument that an electronic event is not listed along with fire, explosion, machine malfunction, and others. Does your crime policy contain an insuring agreement for Electronic or Computer Funds Transfer Fraud? It's

also important to analyze any actual cyber insurance policies you purchase — don't automatically assume that it triggers in all instances. Consider, for instance:

> The insurer shall pay all Loss, in excess of the applicable Retention, that an Insured incurs solely as a result of an alleged Security Failure or Privacy Event that has actually occurred or is reasonably believed by such Insured and the Insurer to have occurred.

The presence of both "Privacy Event" and "Security Failure" is good, and allows the policy to respond for events beyond breaches of credit cards, Social Security Numbers, and other personally identifiable information. Unfortunately, we often see firms whose cyber risk is everything but privacy-related, and while they tout their cyber insurance policy as the answer to all of their cyber concerns, they later discover that the policy only triggers from a "Privacy Event."

Another important consideration from a trigger perspective is that, in the true sense of the risk, a cyber event does not have to be malicious in nature, and therefore may escape a policy trigger that requires malicious intent. Employee mistakes, for instance, might not technically be considered "security failures," but could lead to very similar damages. Or, similar to the tangible world, sometimes things simply don't work or fail — the failure or malfunction of computer or networking equipment can cause considerable damages similar to a cyber attack, but such damage may not trigger cyber coverages. There are numerous examples in recent news reports about multinational companies experiencing considerable operational disruptions caused by computer networking equipment malfunction.

b. Understand the policy exclusions — What exclusionary language in present in current policies, whether explicit or meaningfully related to how a cyber event could occur? This step is crucial and always requires a careful consideration of exclusions that speak to intentional acts, the reliance on third party infrastructure, and terrorism or actions of hostile actors backed by nation states.

In certain instances, such as the energy or maritime industries or for certain coverage facilities like the Lloyds of London terrorism offering, there are easily identifiable exclusions that will render the policy completely null from a cyber perspective. Consider the Institute Cyber Attack Exclusion Clause CL-380:

- "(1.1) Subject only to clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

- "(1.2) Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing of any weapon or missile."

Less cut and dried are a variety of "Electronic Data" exclusions that are commonly found in property, general liability, and excess liability policies. Most of these exclusions were designed to negate the potential for coverage for liability suits resulting from breaches of confidential or personally identifiable information, but they often have much broader implications. If, for example, you are a critical infrastructure operator and concerned about the possibility of third party bodily injury resulting from a cyber event, the following exclusion in your liability policy may result in a serious coverage limitation:

- This policy does not apply to any liability based on, attributable to, arising out of or in any way related, either directly or indirectly, to: a) erasure, destruction, corruption, misappropriation, misinterpretation of "data" including any loss or use arising therefrom; b) erroneously creating, amending, entering, deleting or using "data" including any loss or use arising therefrom, or c) the distribution or display of "data" by means of a website, the internet, an intranet, extranet, or similar device or system designed or intended for electronic communication of "data."

Don't forget terrorism — especially given recent world events and increasing concerns that terrorist groups are trying to develop cyber capabilities. As a starting point, policies generally default to excluding terrorism by using that word explicitly, or other qualifiers like "hostile actors." The good news is that coverage does exist, whether via the Terrorism Risk Insurance Program Reauthorization Act (TRIPRA) or other commercial market solutions. The big problem, however, is the uncertainty about how an act would be adjudicated (or not) as that of terrorism. For example, the attack on the Metcalf substation in California did not meet the FBI's definition of terrorism, but that wasn't without debate.[4] And an FBI determination technically doesn't matter with respect to the activation of TRIPRA — that's up to the Secretary of the Treasury. Ultimately this is a very tricky issue as there does not exist a consensus or preferred approach for coverage, or even a consensus on how terrorism would be treated by the insurance industry. At a minimum, it's advisable to at least understand all of the alternatives.

c. Understand legal fundamentals — It's also important to take stock of the legal jurisdiction of each policy, as that could be a key factor in determining the out-come of a coverage dispute based on uncertainty. In the United States, uncertainty, including policy silence with respect to cyber perils, usually inures to the benefit of the policyholder, so, for example, an all-risk property policy without any cyber exclusions should almost certainly pay for cyber predicated property damage. In other legal jurisdictions, the same type of policy uncertainty might not produce the same out-come because uncertainty often inures to the benefit of the insurer, especially when the insurer can show that cyber was not contemplated during the underwriting process, regardless of the lack of any exclusionary language in the contract.

3. STRESS TEST YOUR INSURANCE PORTFOLIO

With the exposure and insurability analyses complete, you are now well positioned to stress test your existing insurance portfolio. The concept is simple: presume that any or all of the final scenarios occur, put on your coverage advocacy hat, and determine how the scenarios would be treated by existing coverages. The process, however, might be more complex:

- Property/Terrorism Catch 22 — You might find that a cyber predicated property damage event should be covered by your property policy, but not if that act is deemed to be terrorism, in which case you'd normally look to the terrorism policy, but you may then find that your terrorism policy contains a CL-380 exclusion.

- "Bricking" Limitation — You might find that the replacement of IT infrastructure impacted by a firmware-level attack likely won't be covered by your traditional cyber insurance policy due to a broadly written bodily injury and property damage exclusion. Recovery for this damage may also have limited coverage under the property policy because the nature of the loss is such that no tangible damage actually occurred.

- Business Interruption Alignment — You might find that a network business interruption loss could hit both your property policy that contains a non-physical damage business interruption extension, and your cyber insurance policy that features full policy limits for network business interruption coverage, assuming that both cover malicious and non-malicious causes of loss.

Undertaking this process provides a snapshot of how much of your cyber exposure should be recoverable by existing coverage, and how much of your cyber exposure is anticipated to hit the balance sheet — critical insight towards making an informed determination on what, if any, additional coverage or limits to purchase.

OUTLOOK ON INSURANCE FOR CYBER RISK

As of this writing, the insurability potential for cyber exposure is strong and continually improving. A large majority of the financial to tangible cyber risk spectrum is insurable, with the main two exceptions being a) first party financial losses attributable to the theft of intellectual property or trade secrets, and b) criminal fines or penalties. Additionally, it's important to recognize that the vast majority of cyber claims have, in fact, been paid. We advise digging deeper when seeing a report about a cyber claim denial — those instances usually relate to privacy breach suits being claimed against legacy general liability policies, or earlier generation cyber policies that contained stipulations about maintaining certain levels of security controls. Thankfully the current-generation policies have eliminated those dubious thresholds.

It's also important to heed our advice about taking a holistic approach to understanding exposure and a portfolio approach to insurability — the cyber peril cannot be entirely insured with a single policy; it requires a consideration and tuning of the entire commercial property and casualty portfolio. Also recognize that the insurance market is continually evolving as it understands and adapts to the dynamic cyber risk climate, and strives to seek consistency on coverage concerns such as terrorism, which is anything but consistent across policy forms and insurers. That all said, an informed and educated approach provides you with the strongest potential to achieve appropriate insurance recovery for an unfortunate and all too often inevitable event.

ENDNOTES:

[1] We thank By: Scott Kannry and David White of Axio Global for their substantial contribution to this chapter.

[2] http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

[4] http://www.sfgate.com/business/article/FBI-Attack-on-PG-amp-E-substation-in-13-wasn-t-5746785.php

CHAPTER 9:
CYBER RISK REPORTING & GOVERNANCE

"Every board now knows its company will fall victim to a cyberattack, and even worse, that the board will need to clean up the mess and superintend the fallout.[1]

When you look at the bottom line, the monetary costs from the highly publicized Target breach are staggering: $150 million in initial response costs, $400 million in replacement credit cards, and an estimated $1 billion of ultimate costs.[2]

PURPOSE OF THIS CHAPTER:

1. **Identify the important role of the board of directors in proper cybersecurity governance.**
2. **Highlight key elements of sound governance models.**
3. **Highlight key elements of sound cybersecurity risk reports.**

Cyber Risks — A Risk Directors Cannot Run Away From

One thing is clear for 2016 and beyond: the impact of a cybersecurity breach is deep, going well beyond a mere public relations issue and potentially impacting shareholder value, customer confidence, employee retention, and possibly exposing the company to regulatory risks. Following a cyber breach, there is a very real risk that directors and officers may be sued for breach of fiduciary duty for their alleged failure to properly oversee the company's cyber risks.

Nowhere is this trend more evident than in the ever-shrinking length of time between the moment a breach is announced and a class-action lawsuit filing, an interval which is now measured in mere days. From nine days in the case of the 2011 Sony breach,[3] to a next-day lawsuit for the University of Central Florida (with a second class action suit filed within three weeks) in early 2016,[4] down to a same-day filing of a class action suit against Scottrade[5] later in the year.

A recent Robinson+Cole news article comments that "toward the end of the year [2015], class action cases were filed the same day as the notification" and cautions that "companies can also assume that a shareholder's derivative suit is in the mix as well."[6]

Given the increased propensity for post-breach lawsuits, how are directors and officers to minimize the likelihood and impact of such legal imbroglio? The article[7] points out that in the case of Wyndham, "the directors discussed cybersecurity during board meetings and did not disregard the risk, because the minutes of the meetings reflected the discussion of the risk."

With the increased scrutiny, it is clear that "Cybersecurity is a risk that boards would do well to pay attention to and document that the board is questioning whether the organization is taking appropriate measures to protect its data in order to combat shareholders' derivative suits."[8]

Despite the enormous publicity given to cybersecurity risks over the past 12 months, you might find it funny that directors still claim to be generally ill-informed about them. We find it sad. The question at the end of the day is time and resources. Cybersecurity is not just an IT problem. It is everyone's problem. If a company does not put in the time and effort to assess cybersecurity risks, then it should not be surprised if it suffers a breach, and if the consequences of the breach are more severe than they would otherwise be if the company had been more proactive. Below we identify the pertinent points of what cyber risk really means and how to assess it.

Cyber Risks — FTC & SEC Flexing Their Muscles

It would be hard for board directors and top leadership to claim that they were not aware of the need for proper governance and management of cybersecurity risks. For its part, the FTC has, for the past several years, been sending clear, unmistakable signals about the important role of directors and management:

> In a January 2016 speech, Julie Brill, Former FTC Commissioner, remarked:[9]
>
> "Eighty years ago, Congress gave the FTC authority to protect consumers from a broad range of 'unfair or deceptive acts or practices.' Under this authority, the FTC has brought nearly 100 privacy and data security enforcement actions.
>
> "The flexibility and breadth of our authority to obtain remedies that protect consumers has allowed us to keep up with rapid changes in technology. For example, we have brought actions against companies for allegedly collecting information inappropriately from consumers' mobile devices, making unwarranted intrusions into private spaces, exposing health and other sensitive information, exposing previously confidential information about individuals' networks of friends and acquaintances, and providing sensitive information to third parties who in turn victimize consumers."

And while the FTC's authority in this domain has been challenged, it scored an important victory against Wyndham in August 2015. FTC Chairwoman Edith Ramirez released an official communication,[10] stating: "Today's Third Circuit Court of Appeals decision reaffirms the FTC's authority to hold companies accountable for failing to safeguard consumer data." She added, "It is not only appropriate, but critical that the FTC has the ability to take action on behalf of consumers when companies fail to take reasonable steps to secure sensitive consumer information."

For its part, the SEC has been equally clear in holding directors and officers to their responsibilities:

> "Effective board oversight of management's efforts to address these issues is critical to preventing and effectively responding to successful cyber-attacks and, ultimately, to protecting companies and their consumers, as well as protecting investors and the integrity of the capital markets."[11] — SEC Commissioner Luis A. Aguilar, June 10, 2014.
>
> "In addition to proactive boards, a company must also have the appropriate personnel to carry out effective cyber-risk management and to provide regular reports to the board."[12] — SEC Commissioner Luis A. Aguilar, June 10, 2014

"…board oversight of cyber-risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper prepara-tion, deliberation, and engagement on cybersecurity issues."[13] — SEC Commissioner Luis A. Aguilar, June 10, 2014

"…boards also need to be aware of the increased regulatory focus on a company's cybersecurity oversight."[14] — SEC Commissioner Aguilar, October 14, 2015

While the initial focus of federal regulators has been fairly narrow in scope — primarily aimed at the banking and finance sectors — recent enforcement actions point to a clear pattern that all businesses, no matter their size, are in regulators' crosshairs.

Cyber & The Board — A Bleak Current Reality

One of the first issues for boards to address is their own ability to devote enough time and attention to the cyber issue, and ultimately to exercise proper oversight of cyber risks. A 2014 report by EY[15] highlights many of the reasons why boards have been reluctant to tackle cybersecurity:

- A crowded agenda.
- The IT silo.
- "Not our problem."
- Difficult to gauge.
- Invisible pay-off In the face of competing demands for scarce resources.
- Wrong priorities.

However, the past five years have shown a definite trend towards improvement. As Deloitte recently summarized: "Increasingly, cybersecurity is becoming a top-of-mind issue for most CEOs and boards, and they are becoming more preemptive in evaluating cybersecurity risk exposure as an enterprise-wide risk management issue, not limiting it to an IT concern."[16]

A Cybersecurity Governance Primer

Board directors understand they must do "something" about the cybersecurity risks faced by their organizations. But what?

When it comes to board governance of cyber risks, Deloitte writes that boards need to "verify that management has a clear perspective of how the business could be seriously impacted, and that management has the appropriate skills, resources, and approach in place to minimize the likelihood of a cyber incident — and the ability to mitigate any potential damages."[17]

SEC Commissioner Aguilar's words bring clarity to this issue: "…boards are responsible for overseeing that the corporation has established appropriate risk management programs and for overseeing how management implements those programs."[18] He added that "board oversight of cyber risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper preparation, deliberation, and engagement on cybersecurity issues."[19]

Essentially, a well-functioning board would pay frequent and special attention to the issue of cybersecurity risks, the way these risks are evaluated and communicated, would participate actively in providing clear direction to management on the acceptability of those risks, and would monitor management's effectiveness in its ability to implement proper security controls to bring the risks in alignment with organizational parameters (i.e. risk appetite).

One of the organizations leading the charge on improving the governance of IT and cybersecurity is ISACA, which was once focused on auditing IT systems but has, for the past decade, broadened its scope to include governance and risk management issues. An ISACA publication, "Information Security Governance: Guidance for Boards of Directors and Executive Management," states that, when it comes to cybersecurity governance, boards should:[20]

- Ensure that they are informed on relevant developments in cybersecurity.
- Define a global risk profile, used as part of an enterprise-wide risk management program.
- Be a strong supporter of change, especially when it comes to risk awareness and the impact of cultural values.
- Support information security activities with appropriate resources.
- Ensure that responsibilities for cybersecurity are clearly assigned, to competent personnel, and that management is aware of its own responsibilities to keep the organization safe.
- Establish priorities — at an appropriate level for the board, of course.
- Direct management to undertake information security activities in a coordinated, planned manner, and ensure that key performance indicators are recorded and reported.
- Leverage reports from internal and external auditors to gain a level of assurance of the effectiveness of the information security activities undertaken by management.

Another key organization in cybersecurity governance, the Institute of Internal Auditors ("IIA"), released a practice guide in 2010 titled, "Information Security Governance,"[21] which cautions that effective cybersecurity governance requires quantifiable yet meaningful deliverables, and must reflect the business priorities, the organization's risks appetite, and account for changes in risk levels due to internal or external factors. To that end, the IIA sees the board's role as:[22]

- Providing oversight.
- Communicating business imperative.
- Establishing and overseeing security policy.
- Defining corporate security culture.

As can be expected, the IIA sees a big role for the chief audit executive, at the very least to provide the board with assurances about the representations brought forward by management.

Cybersecurity Governance as a Cycle

Another approach to the governance of cybersecurity risks is to follow a three-step cyclical approach advocated by many of the leading cybersecurity and auditing organizations, including ISACA (with CoBIT 5) and the IIA: boards should evaluate, direct, and monitor on issues related to cyber. Before we explore this triad further, let's take a moment to focus on the meaning of governance (a board-level activity) versus management (an executive/officer level activity).

ISACA defines governance thusly:[23] "Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions, and options; setting direction through prioritization and decision-making; and monitoring performance, compliance, and progress against agreed direction and objectives."

In this case, governance — by the board of directors — is contrasted to management's role, which is defined as:[24] "Management plans, builds, runs, and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives."

When it comes to the role of the board, to govern over matters of IT and security, directors should:[25]

a) Evaluate the current and future use of IT.

b) Direct preparation and implementation of plans and policies to ensure that use of IT meets business objectives.

c) Monitor conformance to policies, and performance against the plans.

We'll explore each in more detail.

CYBER RISK EVALUATING

Board of directors should — on a near-continuous basis or after an incident — review and determine the applicability and effectiveness of the information security efforts undertaken by management. In doing so, boards should consider both internal and external pressures and factors that can impact the organization with respect to cybersecurity, including the current compliance and regulatory landscape.

CYBER RISK DIRECTING

Boards should ensure that someone in management, positioned at an appropriate level (e.g., CISO reporting to the CEO), is tasked with implementing and managing the organization's cybersecurity efforts and policies.

CYBER RISK MONITORING

Boards should monitor the effectiveness of cybersecurity efforts. The goal of such monitoring is for the board to reassure itself that the organization's cyber risks are within the tolerance levels set by management, in accord with the board's direction.

Those three phases are part of the governance cycle. Yet this cycle isn't just a once-a-quarter type activity. An organization's cybersecurity risk profile can change in a matter of days, or possibly hours. As Norman Marks writes, "Risk management must operate at the speed of the business and its environment."[26] In the cyber environment, things can change in an instant. Put another way, "When risk management is seen as 'something we do once a quarter,' it is seen as an exercise separate from how the organization is managed every minute of every day."[27]

Putting a Price on the Impact of Cyber Risks

But how are board directors supposed to govern in matters of cybersecurity risks when the reports and presentations they are provided with don't translate how cybersecurity risks can impact the

business? A report by BayDynamics found[28] that "only two in five IT and security executives agree or strongly agree that the information they provide to the board contains actionable information. As a result, only 29% of respondents believe they get the support they need from their boards."

How can boards get more actionable information and ensure that the organization is making the best decisions when it comes to its handling of cyber risks? By relying on cyber risk data that's been evaluated in financial terms. "Value at Risk" ("VaR") is proving to be an effective way to measure cyber risks.

According to Deloitte, "…cyber value-at-risk ultimately seeks to help them [corporate leaders] make more informed, confident decisions about their organizations' risk tolerances and thresholds, cybersecurity investments, and other risk mitigation and transfer strategies."[29]

The World Economic Forum ("WEF"), in a special report on Cyber Resilience, describes that cyber value-at-risk models are "characterized by generic applicability across industries, scalability, ease of interpretation, and ability to support executives' investment and risk management decisions. Building the complete cyber value-at-risk model and having a comprehensive outlook on the organization's assets under threat, organizations can also make decisions with regard to the appropriate amounts of investments in security systems."[30]

To get the most out of a cyber value-at-risk model, boards should seek a solution that not only quantifies cyber risks in financial terms, but also supports visualizing the impact of various cybersecurity efforts (i.e. "quick wins" and "best bang for the buck" type scenarios) and comparing the organization's posture (risk exposure, controls, effectiveness) across time.[31]

The ability to quantify cyber risks as part of a larger risk management system is key to allowing the organization to develop and execute on strategy. As Norman Marks puts it, "the effective consideration and management of uncertainty can lead to better decisions, improved outcomes, and enhanced long-term value to stakeholders."[32] An organization that has found a way to consider, communicate, and manage cyber uncertainties will inevitably be in a better position than its competitors lost in a world of arbitrary decisions about cyber.

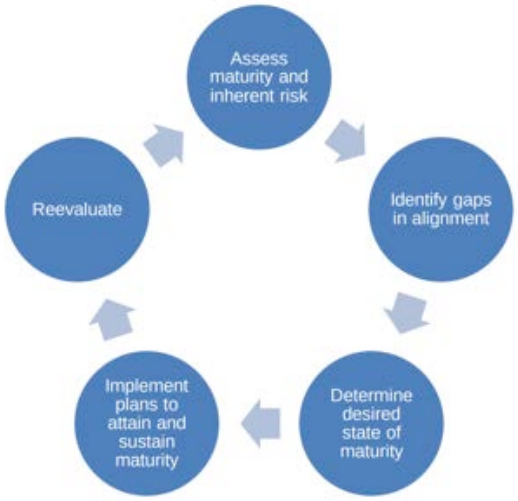
Nick Sanna, CEO of RiskLens, a company that provides a cyber risk quantification platform, sees a similar trend: "Board of directors and business executives are asking cyber risk professionals to add an economical dimension to their reporting of cyber risks. What they are seeking is the possible return on security investments, where the cost of cybersecurity initiatives can be compared to related risk reductions, in quantifiable terms: dollars and cents."[33]

Being able to express cyber risks in financial terms will truly enable directors and officers to be better decision-makers when it comes to cyber risks. Yet, there's another important aspect for directors to consider in governing over cybersecurity: how is the maturity of the organization's security efforts improving — or hopefully improving — over time?

Maturity's Role in Governance

In 2015, the FFIEC released a Cybersecurity Assessment Tool. Primarily aimed at financial institutions — as these organizations are experiencing a very large volume of cyber-attacks — the tool aims to help directors and officers guide their organizations towards more effective cybersecurity controls. Yet, instead of focusing on the controls themselves, the tool takes a maturity-

based approach to enhancing the organization's cyber resilience, as the figure below illustrates.[34]



The FFIEC states the following benefits to using its maturity-based approach to assess cybersecurity:[35]

- Identifying factors contributing to and determining the institution's overall cyber risk.
- Assessing the institution's cybersecurity preparedness.
- Evaluating whether the institution's cybersecurity preparedness is aligned with its risks.
- Determining risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired state.
- Informing risk management strategies.

Armed with their organization's maturity rating (maturity of the security program, and even maturity of the security governance process itself) and a way to translate cyber risks into quantified financial impacts, directors are able to take an engaged approach to the governance of cyber risks. Yet, we need one more piece to complete this picture: effective reporting.

Elements of a Good Cybersecurity Report

A 2016 report by Deloitte, titled "10 Questions You Should Be Asking to Embrace Risk and Lead Confidently in a Volatile World,"[36] presents a key question concerning the cyber realm: "Is my risk team giving me the confidence I need to make high-stakes decisions?" The answer for now is likely that we have a ways to go before we get to that point.

As reported in the 2014-2015 NACD Public Company Governance Survey, boards are not fond of getting techno-babble updates when it comes to cybersecurity risks. Boards are not happy with the nature and quality of the information reported to them: "Of the respondents, more than one-third (36%) claimed they were not satisfied with the quality of information from management, while more than half (52%) reported the quantity of information was insufficient."[37]

More troubling, "The indicated lack of information regarding cyber risk may pose a problem even for directors knowledgeable about cyber issues. Although most respondents indicated that they had at least some knowledge regarding cybersecurity risks, many felt they could still improve their understanding."[38]

The results for the latest edition (2015-2016) of the same report (NACD Public Company Governance Survey) shows that the situation has not improved much: "Directors' comprehension of cyber risk is low. Only 14% of survey respondents believe their boards have a high level of understanding of the risks associated with inadequate cybersecurity, and 31% of responding directors are either 'dissatisfied' or 'very dissatisfied' with the quality of information they receive from management on this topic."[39]

In our view, a good cybersecurity report from management to the board should:

1. Paint a clear picture of the organization's current cybersecurity posture. However, that should be contrasted with the various postures achieved over time (previous quarter, previous year) to ensure a forward progression and to draw out engaging debate about the organization's ability to handle current and future cyber risks. Here, numbers are good. How many events during the quarter? How many incidents? Was any data lost or stolen? If so, what was the cause of the breach or data theft? How long were the attackers on the network before we found them? These basic questions, if answered, can reveal a lot about the company's current cybersecurity posture. A lot that is good, and a lot that might not be so good.

2. Put cyber risks into perspective. Heat maps are surely colorful, but not necessarily effective at helping the board and management discern the extent to which the risks and controls are in balance, and most importantly, the likelihood and impact associated with a given threat. After all, the news from the past decade is full of examples of companies that thought they had things under control, or that issues were no big deal, only to find themselves on the front page, followed in a few weeks by mountains of lawsuits and regulators breathing down their necks. Reports should be engaging on the topic of cyber risk; even provocative. Boards need to be fully engaged on cyber risk. And its management's job to provide enough details for a reasonable board member to make an informed decision. Just saying you are "fine" won't cut it any more.

3. Put budgetary reasons or constraints in perspective. One good question to IT and senior executives is: "Do we have the people and resources necessary to protect our network? If not, then why not?" Given the cyber skills gap, being fully staffed is a real problem today. Similarly, if the answer is that your network "is as old as your youngest child in college," then perhaps the company does not have the appropriate people or hardware resources to protect its network. If it does not, then propose solutions. Don't just say you are "fine" when there is smoke seeping out from the door in the server room. Fire may be close by.

4. Provide clear reasoning as to management's approach to dealing with risks, and the extent to which it has been determined that the approach is effective. Simply stating "we have adopted a security framework and have nearly completed our implementation of it" in no way provides any level of guarantee that the organization is doing its due diligence in protecting the information of its customers and its own employees. One simple question: "When was the last time we did spear-phishing training for our employees?" If the answer is "last year" then that is not good. Training must be done at least twice a year. Even better, once a quarter. Employee training and awareness can reduce the chance of a successful spear-phishing attacking dramatically if done over consecutive quarters.

   Without properly testing and challenging what has been done, the organization would simply try various things and hope some of them work, or worse, assume those things are working. Said differently, do not assume your email filter will catch all attempts at spear phishing your employees, because none are 100% effective. Train your employees before they click on the link.

5. Provide a clear vision forward in terms of a roadmap or framework. In exercising oversight of the cyber issue, the board must be satisfied that management has developed a clear and effective roadmap of cyber-related projects across high level domains, has adequately allocated funding for such endeavors, and that staff resources will be available to ensure a successful implementation of the roadmap.

6. Integrate cybersecurity risks into the larger picture of the Enterprise Risk Management framework. The reason being that cyber risks are just one of many risks the board has to oversee, and ultimately the board may find it acceptable to expose the organization to a certain level of cyber risk, as the cost of remediation could end up being orders of magnitude more expensive.

After years of making cybersecurity presentations to boards, we follow two "old school" rules: (1) it's the board's business judgment to make with respect to cybersecurity risk. Give them actionable information so the board can make that judgment; and (2) as they say on NYC transit and subways, "If you see something, say something." Don't sit on the sidelines with information the board needs to hear firsthand (e.g., the increasing severity of DDoS attacks in the financial institutions space). If a cloud-based, anti-DDoS remediation service costs $150,000, but will potentially save the company $8,000 *per minute*, tell the board your rationale for needing one. The board will likely say "yes" and move on to the next agenda item. If you don't tell them, and Anonymous hammers your organization with a 300 Gbs attack that might have been prevented or remediated without much damage, then, well, we don't want to be you.

ENDNOTES:

[1] See "Ten Cybersecurity Concerns for Every Board of Directors" http://www.cybersecuritydocket.com/2015/04/30/ten-cybersecurity-concerns-for-every-board-of-directors/

[2] See "Directors Should Look Beyond Cyber Insurance: Law enforcement officials seek accountability in data breaches and cyber loss" http://www.metrocorpcounsel.com/articles/34142/directors-should-look-beyond-cyber-insurance-law-enforcement-officials-seek-accountab

[3] See "Nine Days from Sony Security Breach to Class Action Lawsuit" https://www.rsaconference.com/blogs/nine-days-from-sony-security-breach-to-class-action-lawsuit

[4] See "2nd class-action lawsuit filed versus UCF for data hack" http://www.centralfloridafuture.com/story/news/2016/02/26/2nd-class-action-lawsuit-filed-versus-ucf-data-hack/80999066/

[5] See "Scottrade announces data breach affecting 4.6M customers"

https://www.dataprivacyandsecurityinsider.com/2015/10/scottrade-announces-data-breach-affecting-4-6m-customers/

[6] See "Look for additional data breach class action cases, standing decisions and shareholders' derivative suits in 2016" https://www.dataprivacyandsecurityinsider.com/2016/01/look-for-additional-data-breach-class-action-cases-standing-decisions-and-shareholders-derivative-suits-in-2016/

[7] Id

[8] Id

[9] See "Privacy and Data Security in the Age of Big Data and the Internet of Things"

https://www.ftc.gov/public-statements/2016/01/privacy-data-security-age-big-data-internet-things

[10] See "Statement from FTC Chairwoman Edith Ramirez on Appellate Ruling in the Wyndham Hotels and Re-sorts Matter" https://www.ftc.gov/news-events/press-releases/2015/08/statement-ftc-chairwoman-edith-ramirez-appellate-ruling-wyndham

[11] See "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus" https://www.sec.gov/News/Speech/Detail/Speech/1370542057946

[12] Id

[13] Id

[14] See "The Important Work of Boards of Directors" https://www.sec.gov/news/speech/important-work-of-boards-of-directors.html

[15] See EY — "Cyber Program Management" https://webforms.ey.com/GL/en/Services/Advisory/EY-cybersecurity-cyber-program-management

[16] See "Cybersecurity: The changing role of audit committee and internal audit" http://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-security-changing-role-in-audit-noexp.pdf

[17] See "Cyber security: The changing role of the Board and the Audit Committee" https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-cyber-security-noexp.pdf

[18] See "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus" https://www.sec.gov/News/Speech/Detail/Speech/1370542057946

[19] Id

[20] See "Information Security Governance: Guidance for Boards of Directors and Executive Management" http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Information-Security-Governance-Guidance-for-Boards-of-Directors-and-Executive-Management-2nd-Edition.aspx

[21] See "Information Security Governance" https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG15.aspx

[22] Id

[23] See CoBIT 5 and GRC https://www.isaca.org/COBIT/Documents/COBIT5-and-GRC.ppt

[24] Id

[25] Id

[26] Marks, Norman (2015). World-Class Risk Management. https://normanmarks.wordpress.com/normans-books/

[27] Id.

[28] See "Telling the Board What They Want to Hear Instead of What They Need to Hear" https://baydynamics.com/blog/telling-the-board-what-they-want-to-hear-instead-of-what-they-need-to-hear/

[29] See "The Benefits, Limits of Cyber Value-at-Risk" http://mobile.deloitte.wsj.com/cio/2015/05/04/the-benefits-limits-of-cyber-value-at-risk/

[30] See "Partnering for Cyber Resilience — Towards the Quantification of Cyber Threats" http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf

[31] See "What CISOs Need to Tell The Board About Cyber Risk" http://www.darkreading.com/operations/what-cisos-need-to-tell-the-board-about-cyber-risk/a/d-id/1325923

[32] Marks, Norman (2015). World-Class Risk Management. https://normanmarks.wordpress.com/normans-books/

[33] Personal correspondence with Nick Sanna, CEO of RiskLens

[34] See "FFIEC Cybersecurity Assessment Tool — Overview for Chief Executive Officers and Boards of Directors" https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf

[35] Id

[36] See "10 questions you should be asking to embrace risk and lead confidently in a volatile world"

http://www2.deloitte.com/us/en/pages/risk/articles/ten-questions-you-should-be-asking.html

[37] See "Survey Indicates Directors Concerned with Lack of Proper Cyber and IT Risk Information" http://www.tripwire.com/state-of-security/latest-security-news/survey-indicates-directors-concerned-with-lack-of-proper-cyber-and-it-risk-information/

[38] See "NACD Survey: Directors Want Changes to Risk Oversight Process" http://www.bna.com/nacd-survey-directors-n17179918037/

[39] See 2015–2016 NACD Public Company Governance Survey Executive Summary https://www.nacdonline.org/files/2015-2016%20NACD%20Public%20Company%20Governance%20Survey%20Executive%20Summary.pdf

CHAPTER 10:
TRUST BUT VERIFY – ASKING THE TOUGH QUESTIONS

"There is no substitution for proper preparation, deliberation, and engagement on cybersecurity issues."[1]

— SEC Commissioner Luis A. Aguilar, June 10, 2014

"Boards must be ever aware of their need to overcome the information imbalance and get what they need in order to provide effective oversight and advice. They need to improve the quality and usefulness of the information they receive about the business and also about the industry."[2]

— Nancy Falls, author of Corporate Concinnity in the Boardroom: 10 Imperatives to Drive High Performing Companies

PURPOSE OF THIS CHAPTER:

1. **Provide a list of issues directors should address at the board level.**
2. **Provide a list of tough questions boards should address with management.**
3. **Provide a list of tough questions boards should ask of the CISO/CRO.**
4. **Cover other important cyber-related issues that should be addressed at the board level, such as security leadership and the nature of communications within the C-Suite.**

As boards begin to take stock of their cybersecurity responsibilities and the growing range of cyber issues, some key points are becoming clear:

- Boards are actively seeking to better understand the nature of cyber risks that impact their organization.
- Boards are now asking for more frequent updates about cyber risks, and requesting that these updates are provided by people in the know, not just briefings from the CEO or CIO.
- Boards are increasingly likely to question and challenge the organization's management of cybersecurity issues, which is absolutely a step in the right direction. Relegating cyber to the techies is not a valid option, unless one wants to draw the ire of regulators, customers, and shareholders.

However, the quality of the discussions and engagements at the executive level and board level has only slightly improved. A 2012 article reported that "thirty-three percent of GCs [General Counsels] 'believe their board is not effective at managing cyber risk.'"[3] Things have improved a little. More recently, only "fifty-six percent of directors and 57 GCs surveyed still named IT and cybersecurity as a reason they lose sleep,"[4] ahead of business innovation and shareholder activism.[5]

How are directors to exercise proper oversight of the organization's risk management program to ensure that cybersecurity risks are properly accounted for, reported, and addressed at the very highest levels of the organization? How can directors ensure that their organization is prepared for the inevitable data breach?

By asking the tough questions. It is only by asking the tough questions that boards can hope to overcome "information asymmetry," a state in which management, by its position and day-to-day activities, knows more about the organization than what the directors know. Boards should not just be "content" to get input from the CEO, but should seek out input and comments from the right people, be they people from within the organization or outsiders with knowledge and expertise of the domain at hand, such as cybersecurity and effective governance in this area.[6]

"So it is critical that the board not only ask the hard questions, but ask them of the right people."[7] — Nancy Falls, author of Corporate Concinnity in the Boardroom: 10 Imperatives to Drive High Performing Companies

Questions Directors Should Address at the Board Level

The National Association of Corporate Directors (NACD) provides valuable guidance for what directors should address at the board level, with three key questions[8]:

1. Do we understand the nature of the cyber threats as they apply to our company?
2. Do our board processes and structure support high quality dialogue on cyber matters?
3. What are we doing to stay current as the cyber threat landscape continues to evolve?

Let's address each in more detail.

1. DO WE UNDERSTAND THE NATURE OF THE CYBER THREAT AS IT APPLIES TO OUR COMPANY?

This by no means implies that board directors should be swamped by technobabble presented by the CIO or the CISO. Directors should provide ample guidance to those tasked with presenting to the board to ensure that information is presented in a clear, understandable manner devoid of obscure technical jargon. The non-technical question they should be prepared to answer (or answer on their own) is: Do any of the cybersecurity threats out there in today's cybersecurity ecosystem have the ability to (1) shut us down, (2) hurt us badly, (3) steal our most critical IP, or (4) hurt our corporate reputations, stakeholders and stock-holders?

Presenters should be able to explain the threats using analogies and show how those threats can impact the organization. Using public examples of significant breaches (like Target, OPM, Hollywood Presbyterian, or the HSBC or Dyn DDoS attack) helps ground executives by relating to what they already know or understand to have been a big problem for other companies or institutions. The goal of having directors understand threats is not to turn them into techies, but to ensure that directors possess, at a high-level, the ability to critically analyze the rest of the security information presented to them to ensure that risks are properly addressed.

2. DO OUR BOARD PROCESSES AND STRUCTURE SUPPORT HIGH-QUALITY DIALOGUE ON CYBER MATTERS?

This is, in our opinion, one of the most important aspects of board oversight of cybersecurity today. When it comes to the board, it is relatively easy for directors to determine whether the board's own processes and structure foster honest, possibly heated, debate concerning the organization's handling of cyber risks. One key question is whether the board is making enough time in its schedule to have heavy-duty cybersecurity discussions. In today's environment, 15 minutes per board meeting (later lowered to 10 minutes when another topic runs overtime) might not be enough time to have an active, informed discussion.

However, how can boards assess the quality of the dialogue that may or may not happen below them, for example, between the CISO and the CIO they report to, between the CISO and CEO they may hardly get a chance to talk to, or between the CISO and CFO, CMO, or CHRO who might hardly pay attention to any security matters? Boards may have to commission an expert to do just that: observe the quality of the interactions between the CISO and the rest of the C-Suite. We agree with the expert studies here: quality of information is a huge problem. If board's don't know there is a potential cyber problem brewing, then how will they ever be able to opine on a solution.

3. WHAT ARE WE DOING TO STAY CURRENT AS THE CYBER THREAT LANDSCAPE CONTINUES TO EVOLVE?

Boards have the ultimately responsibility for ensuring that the organization is moving forward in its ability to not only handle the cyber threats of today, but also those on the horizon that will be knocking at the institution's door in a matter of months.

So how can boards ensure the organization will be able to handle coming threats without being months or years behind? One way is to track the organization's maturity when it comes to its cybersecurity efforts. Is the organization highly immature, constantly fighting fires, and failing to learn from its mistakes? Or is the organization constantly improving its ability to strategically invest in security related projects, and improving with every cycle? An example of the latter would be an organization for which the next case of ransomware infection is not only detected more rapidly, but remediated in a tenth of the time it took to contain and eradicate the first instance. Another example would be the organization's incident response team kicking attackers off the network before they do harm or damage or steal stuff (which would also indicate very mature detection capabilities).

Here we again recommend "new math" as the best offense and defense for board members. Data around cybersecurity is "the new oil." They should insist on mathematical quantifications of events, incidents, and breaches. They should look at dwell time (the length of time the attackers were on the network before they were found). They should look at real-time breaches and their causes. They should study budgets put forth by their management and CISO (i.e., is the budget sufficient from both a people and a hardware perspective to deal with the threats that the company knows of, and the threats of the future?). Some may say these are pretty simple questions. We would say that sometimes the simple questions are the best ones to draw out answers that might not be acceptable when viewed in the totality of a company's cyber ecosystem.

QUESTIONS BOARDS SHOULD ADDRESS WITH MANAGEMENT

How can board directors address management's handling of cybersecurity risks? A 2015 Spencer Stuart article, titled *Cybersecurity: The Board's Role*,[9] provides some key questions:

1. Does management have "a clear and consistent understanding of cybersecurity relative to the business?" Management may want to collect huge amounts of information in order to crunch it to understand their customer's buying habits. But what does that really mean? What sorts of data? Where are they going to store the data? What privacy obligations exist with respect to the data and where it is being stored? You get the point. As businesses processes changes, so do cybersecurity needs. Cybersecurity is not a snapshot. It is a constant moving target.
2. Does management understand its responsibility for cybersecurity, and the extent to which management has "an adequate system of controls in place?" The classic example here is a regulated institution, like an investment bank or federally regulated bank. What sort of compliance regulations go hand-in-hand with being regulated? How is data being kept safe and secure (like under Regulation S-P)? What other cybersecurity regulations does the bank have that may come up in an annual examination. The concept of "controls" can mean both actual controls of data management (like multi-factor authentication) or compliance-related controls that, if violated, can bring grief upon the institution if there is a subsequently discovered breach.
3. Is the cybersecurity budget appropriately funded as requested? Or is it stagnant or being cut in order to address other business needs? What cybersecurity-related requests are not being funded, and how are those requests reviewed/addressed in terms of their impact on cyber risks?
4. Is there an executive-level position tasked with tracking, reporting, and managing cybersecurity risks? Is this position given the appropriate level of support and visibility? Who does this executive report to? And what is the quality and quantity of the interactions between this person and the rest of the C-Suite?
5. Does the organization carry cybersecurity liability insurance to cover the cleanup and potential litigation consequences of a major breach?

A PwC handout asks a complementary question that boards should address with management: "Does management sufficiently oversee, monitor, and report on cybersecurity governance?"[10]

Another important question that the board should address with management — perhaps through the lens of an auditor or cybersecurity consultant — is, "To what extent are cybersecurity issues taken into account when developing business and IT strategy?" Data touches every part of the business (e.g., an IoT business strategy), thus the security of the data should be a high priority for all areas of the organization, and especially when planning or implementing a new product or service.

QUESTIONS BOARDS SHOULD ASK OF THE CISO/CRO

As mentioned in chapter 9, one of the key questions that boards and directors should be able to answer in a strong affirmative is: "Is my risk team giving me the confidence I need to make high-stakes decisions regarding the cybersecurity posture of the company?"[11]

As we've written about recently, here are some questions to ask of the CISO:[12]

1. What are my cyber threats and vulnerabilities? For starters, there are people, employees, vendors, nation state actors, aging computer hardware and software issues, and hackers for hire.
2. What am I doing about those threats and vulnerabilities? Am I training my employees not to click on the link? Am I patching my software packages in a timely fashion? Am I following a "least privileged user" policy? Is my cybersecurity hardware state-of-the-art, or 20 years old? The older the hardware and software, the more likely it could be that vulnerabilities exist that might have no known patch.
3. How likely is it that I might be attacked via a known threat or vulnerability (and what am I doing about it if that likelihood is high and the potential for damage is also high).
4. How bad will the damage be if I am attacked?
5. When was the last time we did a vulnerability assessment? When was the last time we did a compromise assessment?
6. Do we have an incident response plan in place if we are attacked? When was the last time it was practiced?
7. Do we have an incident response specialist (like FireEye or K2 Intelligence) on 24/7 retainer ready to go? Or is it our intention to hire an incident response consultant on the fly?
8. Do we have a business continuity plan in place, with sufficiently tested and segmented back up media so that if we are breached (or attacked with ransomware), we can reboot the network in an accurate and timely fashion?
9. Do we have a crisis communications plan in place to deal with the potential notification consequences of a potential breach? This is an especially important question for all companies, especially those that are publicly traded.

OTHER IMPORTANT ISSUES FOR BOARDS TO ADDRESS

Relationships in the C-Suite

The board should review the relationships in the C-Suite to ensure that cybersecurity is not just relegated to an IT issue and that there are positive and frequent interactions on the topic of data security with these CXOs:

- Chief Human Resource Officer (CHRO).
- Chief Marketing Officer (CMO).
- Chief Financial Officer (CFO).
- Chief Data Officers (CDO).

And of course, with the

- Chief Executive Officer (CEO).

A 2016 report by IBM's Institute for Business Value recommends that boards and management, "Elevate and regularly discuss cybersecurity at C-suite and board meetings, and engage risk, finance, marketing, human resources and supply chain."[13]

Cybersecurity Leadership

On the topic of personnel, the position of CISO has continued to evolve, to become a critical component of the modern organization's C-Suite. As a recent Cisco report states, "CISOs must be able to frame the discussion in a strategic way that clearly communicates the potential impact of a data breach on stock price, customer loyalty, customer acquisition, and the brand."[14]

The board must ascertain that the positioning of the CISO role is appropriate given the key role it plays. In some organizations, the now CIO reports to the CISO.[15] Whether the CISO-CIO roles are flipped, the goal is to "ensure that privacy and security roles within the organization are separated and that responsibilities are appropriately assigned. The CIO, CISO/CSO, and CPO should report independently to senior management."[16] This is principally so that budgetary requests do not get bogged down in budgetary politics or pressures. Ideally the CIO/CISO/CSO should report to the CEO or to the audit committee of the board of directors.

The board must also determine whether the current CISO has the attributes required to properly lead the organization when it comes to managing cybersecurity risks. "No longer merely a digital sheriff called on to protect the firm's data valuables, the CISO is expected to act as a full strategic partner with the rest of the C-Suite."[17]

Egon Zehnder, the executive search and talent management consultancy, summed up the four key traits of successful leadership: curiosity, insight, engagement, and determination.[18] The board and management should ensure that their current CISO possesses these traits, or can be trained/mentored towards them.

What about a "risk leader?" What traits should an organization look for in a risk leader? According to the Chartered Global Management Accountant (CGMA) association, a successful risk leader should exhibit the following traits: be independent and influential, be a clear and concise communicator, be a standard-bearer for what's right, and be credible.[19]

In summary, the boards should determine that the organization's CISO:20

- Has a sound understanding of the business.
- Be a good communicator (not overtly techy).
- Be receptive to change and self-assessment procedures.
- Provide value and insight.
- Have good emotional IQ.
- Have the courage and strength to fight the good fight.

One Question To Rule Them All

What is our level of certainty that…

Or, put another way,

How do we know that…

Asking that question allows an organization's board and leadership to properly evaluate the range of controls and threats presented to them. As the FFIEC reminds boards, "Controls should be evaluated for effectiveness against identified threats or vulnerabilities."[21]

By asking "how do we know that our antivirus solution is effective at protecting us against ransomware," for example, the organization's board and leadership can determine the level of confidence to attach to the representations from the CISO about how effective the various controls implemented truly are.

FINAL THOUGHTS

As part of their fiduciary duty, board directors should ensure that they exercise effective oversight of cybersecurity; that they engage in healthy, vigorous and regular debate of cyber issues with management; and that they have adequate access to cybersecurity expertise to review, debate, and possibly question the effectiveness of the cybersecurity efforts put forth by the organization. As a 2015 report from the Global Network of Director Institutes states, "Boards should have adequate access to cybersecurity expertise and discussions about cyber risk management should be given regular and adequate time on the board meeting agenda."[22]

Allow us to repeat this last point: it is critical for boards to have access to cybersecurity expertise to assist them in evaluating the effectiveness of their organization's efforts to detect, respond, and recover from a cyber incident. Since there are currently very few cybersecurity experts sitting on boards, directors need to seek external help to validate the assertions of management (reaching the board via the CISO, the CIO, or the CEO). Doing so can make the difference between just believing that their organization is secure and having a clear picture of where the blind spots are and where the organization needs to make improvements.

Cybersecurity is not a destination. It is a journey; one that the modern organization has to fully embark on and navigate for decades to come. As we've said before, "Organizations should assess the extent to which their security capabilities are maturing, evaluate whether cyber risks are integrated within the larger enterprise risk management system, and continually examine [their] ability to be resilient when it comes to the cyber realm."[23]

ENDNOTES:

[1] See "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus" https://www.sec.gov/News/Speech/Detail/Speech/1370542057946

[2] Falls, N. (2015). Corporate Concinnity in the Boardroom: 10 Imperatives to Drive High Performing Companies

[3] See "Growing Concerns Over Cybersecurity" https://www.cooley.com/66877

[4] See "Is cybersecurity becoming less of a concern?" http://www.insidecounsel.com/2016/06/06/is-cybersecurity-becoming-less-of-a-concern

[5] See "LAW IN THE BOARDROOM: WHAT KEEPS YOU UP AT NIGHT?" https://www.nyse.com/publicdocs/Law_in_the_Boardroom.pdf

[6] Id

[7] Falls, N. (2015). Corporate Concinnity in the Boardroom: 10 Imperatives to Drive High Performing Companies

[8] See "Cyber-Risk Oversight: 3 Questions for Directors" http://ethicalboardroom.com/risk/cyber-risk-oversight-3-questions-for-directors/

[9] See "Cybersecurity: The Board's Role" https://www.spencerstuart.com/research-and-insight/cybersecurity

[10] See "PwC's Board Cybersecurity Governance Framework" https://www.pwc.com/ca/en/consulting/publications/20160310-pwc-reinforcing-your-organizations-cybersecurity-governance.pdf

[11] See "10 questions you should be asking to embrace risk and lead confidently in a volatile world"

http://www2.deloitte.com/us/en/pages/risk/articles/ten-questions-you-should-be-asking.html

[12] See "3 Fundamental Takeaways from the DNC Hack" http://levick.com/blog/crisis/3-fundamental-takeaways-dnc-hack/

[13] See IBM Institute for Business Value report "Securing the C-Suite" http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03738USEN&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US

[14] See Cisco Report — "Mitigating the Cybersecurity Skills Shortage"

http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf

[15] See "Is Your CISO Out of Place?" https://securityintelligence.com/is-your-ciso-out-of-place/

[16] See "Governance of Cybersecurity: 2015 Report" https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/tech-briefs/governance-of-cybersecurity.pdf

[17] See "Evaluating and Attracting Your Next CISO: More Sophisticated Approaches for a More Sophisticated Role" http://www.egonzehnder.com/leadership-insights/evaluating-and-attracting-your-next-ciso-more-sophisticated-approaches-for-a-more-sophisticated-role.html

[18] See "Digging for hidden treasure" http://www.egonzehnder.com/the-focus-magazine/topics/the-focus-on-potential/leadership-insights/digging-for-hidden-treasure.html

[19] See "How to pick a successful risk leader" http://www.cgma.org/magazine/news/pages/how-to-hire-a-risk-leader-201512248.aspx

[20] See "Is Your CISO Ready to Be a Risk Leader?" https://securityintelligence.com/is-your-ciso-ready-to-be-a-risk-leader/

[21] See "FFIEC Information Technology Examination Handbook" https://www.ffiec.gov/press/PDF/FFIEC_IT_Examination_Handbook_Management_Booklet_2015Final.pdf

[22] See "Guiding Principles for Cybersecurity Oversight" http://gndi.weebly.com/uploads/1/4/2/1/14216812/gndi_cybersecurity_final.pdf

[23] See "Cyber Risks: Three Areas of Concern for 2016" https://securityintelligence.com/cyber-risks-three-areas-of-concern-for-2016/

CHAPTER 11:
THE GREAT MIRACLES AND CHALLENGES OF CLOUD COMPUTING

PURPOSE OF THIS CHAPTER:

1. What are the various methods and offerings through which companies can transition some or their entire network or data storage needs to the cloud?
2. Why has cloud computing become so popular?
3. What risks can be anticipated when moving to the cloud?
4. What defense measures/steps can be taken to secure data in the cloud?

The last two years have shown tremendous growth in the delivery of cloud computing services to corporations and organizations of all types, sizes, and industry sectors.[1] Given the exponential growth of unstructured data that gets created during every sales day, coupled with the additional growth of real-time data generated by Internet of Things (IoT) devices and sensors (which will account for nearly 1/3 of all network traffic by 2019)[2], the volume of real-time data simply outstrips nearly every company's need to store it on premises and digest it for advanced corporate decision making.

The cloud provides a solution. It is both disruptive and transformative for businesses because of certain well-defined attributes that lack many of the constraints of on-premises network computing (most especially cost-efficiency and agility). In fact, Cisco recently noted, "Within the next three years…more than 4/5 of all data center traffic, 83%, will be based in the cloud."[3]

According to another study, almost 95% of all companies are using cloud computing in some capacity or another — public, private, or hybrid (we will explain these terms in more detail below).[5] Indeed many companies are using one or more clouds to operate their businesses. This growth is dramatic, and the numbers bear this out: "Global spending on public cloud services is expected to grow 16% to $204.2 billion this year, compared with 13.8% growth in 2015 and a 17.7% rise in 2014."[6]

Furthermore, more than 77% of businesses have adopted the private cloud in some capacity. That adoption has driven the growth of hybrid cloud computing, where companies use some combination of both private and public clouds. Remember that with the concept of virtualization (explained below), the real number of companies using one or more "clouds" in their business is even greater.

One might wonder, given companies' broad adoption of the cloud, whether these are just technology-based companies or if the adoption of cloud computing is more broad based across every industry sector. The answer is actually the latter.

One recent article notes that big pharmaceutical company, Johnson & Johnson, is aggressively adopting the cloud, "aiming to have 85% of its applications in cloud systems from

Amazon.com Inc., Microsoft Corp., and NTT Communications Corp. by 2018. The healthcare and medical devices company is also shutting down or consolidating 40% of existing software applications to cut spending on technology maintenance and streamline operations."[7] J&J is not just moving applications to the cloud; it is moving data too: "The company has moved more than 500 terabytes of data to Amazon Web Services, Microsoft's Azure, and NTT's cloud platform, improving how research is conducted…."[8] There are plenty of other large companies following this migration to cloud computing.[9]

Financial services companies are considering large cloud computing moves as well, both to save money on critical IT infrastructure hardware, and to keep data security at similar or even higher levels using features such as end to end encryption. While financial institutions and large banks might naturally proceed with more caution, clearly the cost savings, elasticity, and flexibility of cloud computing are very appealing.[10] In fact, one recent study noted that "sixty-percent of global companies will have stored customer sensitive data in the public cloud, a 40% increase in just two years."[11]

This chapter is devoted to exploring cloud computing. Cloud computing's methods and modes of operation, and its availability to cloud customers of all types, the advantages of cloud computing, and its governance and liability challenges, especially when it comes to securing data in cloud environments, and most especially hybrid environments that involve both the cloud and traditional on-premises networks. It should be no surprise that with the exponential growth of cloud computing, hackers and cyber criminals know exactly where many of the crown jewels lie today, and we are sure they will stop at nothing to get them.

Reasons for the Growth in Cloud Computing

Why is cloud computing growing exponentially? There are many good reasons:

- Immediate provisioning of resources, in a cost efficient manner, rather than waiting for a server and/or other networking equipment to be physically ordered, installed, and tested.
- Immediate collaboration and exchange of data in a seamless, frictionless way across a multitude of devices and platforms between business, employee, and end-user.
- Malleability and agility based upon user-defined needs. For example, the hybrid cloud has transformed the way many companies are doing business because it combines the ease and cost-efficient use of the public cloud with the more complex needs associated with more valuable and mission-critical information and data that companies need to protect through provisioning a private cloud. Hybrid clouds create the agility necessary to deliver business needs at network speed. And if more storage is needed, it is usually available that very day. No waiting game in cloud computing.
- Security. For Fortune 100 organizations with nearly infinite resources, it would be difficult to argue that they might achieve security benefits by moving some or all of their business operations to the cloud. On the other hand, for SMBs that don't have resources, the cloud is the place to be. As noted in one recent article, "Trusting your data to a cloud service provider (CSP) is actually much safer than using an on-premises data storage solution. CSPs simply have more resources to dedicate to security."[12] This is made possible by:
    - 24/7 monitoring;
    - Multi-layered security measures, such as encryption, standards of care, compliance, and identity-based access policies; and

- Proactive management structures that ensure quick reactions to security breaches and continuous security updates.[13]

How does the move to the cloud square with the acute shortage of skilled cybersecurity workers in the U.S.? "More than 209,000 cybersecurity jobs are unfilled in the U.S., and the number of postings has jumped 74% over the past five years, according to Peninsula Press, a project of the Stanford University journalism program. Demand is expected to grow by another 53% through 2018, and as IT evolves, the skill sets must evolve — meaning the shortage is only going to get worse."[14]

Here, the cloud provides a double-edge sword we need to advise on — while the cloud is clearly an attractive alternative for many companies given the difficulty in hiring good skilled staff, moving to the cloud also creates other complexities for IT staff (like understanding visibility, data storage and traffic concerns, and circumstances that might indicate a cloud breach). For the most part, we think the sword comes down on the side of being better for those who do not have adequate resources to handle and secure data on premises.

Types of Cloud Delivery Offerings

Infrastructure as a Service: This is the most basic method of entering the cloud computing environment. It is rather like renting a car, but here your "car" is your storage, hardware, servers, and network components. You can rent a big car or a small car depending upon your business and storage. The CSP owns, houses, and provides the equipment. You provide everything else, including managing applications, data, runtime, middleware, and operating systems.

Platform as a Service: Here, the CSP provides your basic networking "car," but you get to then "hot rod" it with your applications that are built upon the network platform provided by the CSP.

Software as a Service: The fastest growing sector of the cloud computing environment. Applications are accessed through a web browser without any downloads or installations. Examples of SaaS services include Google Apps, Salesforce, Workday, Concur, Citrix GoToMeeting, and Cisco WebEx. There are potentially huge advantages of adopting a SaaS environment. It is a pay as you go model with inherent flexibility and elasticity.

Types of Cloud Deployment Models

Public Cloud: Owned and serviced by a cloud service provider. Its resources are sold to the public. It can be accessed via the Internet through multiple devices. This is the typical "multi-tenant" concept that people describe when people think of the cloud. With a public cloud, the user can scale up or down on an as-needed basis. It sets its own security and access parameters. When you think of the public cloud, think of Amazon Web Services, Microsoft Azure, or Google/Alphabet.

Private Cloud: The opposite of a public cloud is a private cloud, which is owned or rented by the user. This is the "single family" house of the cloud ecosystem. The private cloud may be located on premises, or on the premises of the CSP. The user is responsible for everything: the operating system and the applications needed for its business.

Hybrid Cloud: This is the fun part! A hybrid cloud arguably gives the consumer the best of both worlds: the agility and elastic nature of a public cloud for tons of raw data, and the availability of a private cloud that can be accessed solely by the consumer for more sensitive data. More broadly

defined, a hybrid cloud by nature is a combination of two cloud infrastructures. Note that one of these infrastructures might also be a private, on premises cloud of the consumer as well. And further note that it is very common for companies to have more than one cloud in their overall network toolbox. Hybrid cloud computing also allows for "cloud bursts," when needed. A cloud burst happens when portable applications and workloads can scale up quickly and exchange data by and between legacy systems and the cloud systems.[15]

The trick with the hybrid cloud (as we develop more below) is that as your environment branches out into it, you must pay attention to architecture integration and connectivity, along with keeping visibility on all the moving "data" parts for security reasons. Legacy on premises systems and applications need to "speak with" cloud networks and applications. Further, some data (e.g. personal healthcare data or credit card data) might be subject to federal, state, and/or other regulatory schemes. Therefore, a very complete governance structure (along with potentially a strict compliance regimen) is a necessary requirement when considering a hybrid cloud infrastructure (or in fact any cloud structure that moves data off premises).[16] Of course, we urge you to also consider cybersecurity hardware (e.g., machine learning- or deep learning-based) that can keep an eye on all data movement through sensor technologies.

Community Cloud: The community cloud is an interesting animal. It is by nature a public cloud environment, but it is shared only by a handful of companies handling the same interests, common needs, or perhaps all companies needing access to the same application for their businesses.

IoT Cloud: This is the truly cutting edge cloud. According to Amazon Web Services, the IoT Cloud "is a managed cloud platform that lets connected devices easily and securely interact with cloud applications and other devices. [It] can support billions of devices and trillions of messages, and can process and route those messages to endpoints and to other devices reliably and securely."[17]

Types of Cloud Service Models

The clever one might ask, "What is the difference between a cloud deployment model and a cloud service model?" That actually is a good, common sense question that deserves an answer.

While the deployment model deals with "multi-tenancy," meaning, "Who's got access to my cloud?" (public, private, or somewhere in between with a hybrid model), a cloud service model deals with, "How is my cloud built, what services are being provided to me, and which party (consumer or CSP) is responsible for which pieces of the cloud cybersecurity puzzle?"

To help you understand how cloud services models are constructed or integrated, the following quotation sums it up nicely:

> By itself, infrastructure isn't useful — it just sits there waiting for someone to make it productive in solving a particular problem. Imagine the Interstate transportation system in the U.S. Even with all these roads built, they wouldn't be useful without cars and trucks to transport people and goods. In this analogy, the roads are the infrastructure and the cars and trucks are the platform that sits on top of the infrastructure and transports the people and goods. These goods and people might be considered the software and information in the technical realm.[18]

Using this very nice quote as the infrastructure for our discussion, here are the various cloud service models:

Infrastructure as a Service (IaaS) — IaaS is the straight provisioning of storage, networks, and servers to a consumer for a price. If the consumer needs more storage, he or she can provision it almost instantaneously (without the associated cost of having to buy the hardware). The consumer can then run his or her own applications and operating systems. The consumer, however, does not own the physical servers — the CSP does. With IaaS, the consumer is responsible for the security of the data kept in the cloud as well as for the security of the operating system and applications. An example of an IaaS provider is of course AwS. IaaS is a very good way for young companies to start computing, or older companies to expand their network while limiting capital expenditures.

Platform as a Service (PaaS) — PaaS is a step above the infrastructure (like the cars and trucks in the analogy above). PaaS is the provision of a cloud infrastructure to end users with certain defined applications that are provided. The consumer can then develop his or her own applications building upon the platform that is provided by the CSP. Microsoft Azure and Google App Engine are two good examples of PaaS. Cybersecurity is usually shared in this model between the consumer and CSP through contractual terms.

Software as a Service (SaaS) — SaaS is the use of the CSP's application (and network and servers) by an end-using consumer. The applications are accessed through the Internet (for example through a smartphone or an iPad). SaaS is used where there is a fundamental application that many companies want to run, and which largely doesn't vary (if at all). Two classic examples of SaaS applications are Salesforce and Groupon. The cybersecurity in a SaaS environment rests with the CSP. SaaS provides a very cost-efficient way to run a generic application that you need for your business.

Risks and Governance Measures Associated with Cloud Computing:

- **WHAT STUFF AM I PUTTING IN THE CLOUD?** Very much like the analysis under the NIST Cybersecurity Framework, before thinking about potential cloud environments, it is important to think about the types of data you are storing or wish to store in the Cloud? Is it generic "Big Data" from sales? Is it personally identifiable information? Is it personal healthcare information that might be governed by privacy regulations such as HIPAA (and thus might be subject to compliance concerns)? Will the data be accessible to customers, or just to internal personnel? Or is it very sensitive or confidential business data like mergers and acquisitions information, business modeling information, the plans to the latest fighter jet, or proprietary financial information that is very sensitive and might cause grave danger to the company if breached?

  Simply put, before any attempted cloud migration, a company, its C-suite executives, and its IT staff must sit down and fully assess and inventory its data (including the intended location of the crown jewels) and the risks of loss that might be associated with migration to either a public, private, or hybrid cloud, as well as what controls should be put in place to mitigate those risks. This discussion will help govern which type of cloud and network architecture is best suited for the company, and what controls (including tokenization and encryption) should be applied to such data when it resides in the cloud. One expert recently noted, "Businesses are slowly coming to the realization that hackers increasingly have the ability to breach company perimeters and more advanced security controls need to be implemented. Encryption adds that extra necessary layer by focusing on protecting the most important aspect, which is the data."[19]

- **WHERE IS MY STUFF?** The physical location of your servers ,and thus the physical location of your data, has always been an import part of the risk calculus. It is even more important today after the passage of the GDPR.[20] With public cloud computing, there is normally no guarantee regarding where your data might be stored or located. This makes regulatory issues and data transfers beyond borders potentially problematic.[21] The same problem exists with a hybrid cloud, where data generally flows smoothly from on-premises to cloud environments and back again. Before migrating a specific data set to the cloud, it is necessary to know exactly what laws and regulations apply and the duties the data owner must comply with. This discussion will illuminate the risks if that data set is breached or exfiltrated, and what specific laws will apply to incident response and disclosure.
- **IDENTITY AND ACCESS MANAGEMENT (IAM, OR "AM I REALLY WHO I SAY I AM?")** — This is where the rubber meets the road as far as cybersecurity goes for either on-premises or cloud networks. Customers and employees (and customers and employees only) must be able to safely and securely access the company's network, portals or information so they can buy, sell, do, or transact business, and this access must be monitored to be sure those accessing the information are doing so in an appropriate manner. There is no more important point in this book.

Because of the depository nature of the cloud (and the multi-tenant/very accessible nature of the public cloud in particular), the stakes here are sky high. If an attacker launches a successful spear-phishing attack and is able to steal multiple passwords, escalate his privileges, and find a home on your cloud, he or she can launch holy hell against your network and potentially steal your company's most important assets.

Thus your IAM controls must be first rate, redundant, and holistic. They will never be perfect, but they should come close. Here are some key tips you should consider:

1. Use a professional identity management provider (or IDaaS). One recent article summed up this tip nicely: "Most IDaaS providers use a common method to handle authentication using identities contained in your organization's existing network directory. The most prevalent option is to have a piece of software installed on your local network, known as an agent, which allows the IDaaS provider to communicate with your directory. That way, admins can keep using the same directory tools they always have, yet seamlessly access apps and resources outside the company network."[22] Many of these identify management services can be customized, and can also provide for Single-Sign/Sign Off across a range of applications. "From a user's perspective, the primary purpose of having an IDaaS solution is to make signing into their web apps easier. A user portal that provides quick SSO access to SaaS apps is a feature in the majority of IDaaS options."[23]
2. Use your CSP's Identity Provisioning System. Many public cloud providers have very good identity management tools, including password and multi-factor authentication. See what tools your cloud service provider officers. Indeed some readily available identity provisioning systems available courtesy of your CSP may be more fulsome than those on your current on-premises network.
3. Passwords (Ugh!). Password management is generally the bane of most corporate

CISO's. They are too easy, too short, or lack any creativity (once again the most prevalent passwords in corporate America are "Password," 0123456," and "Querty"). Passwords must be sufficiently difficult to crack (having combinations of letters, numbers, and characters, like "Mic4eyM@uSe)"). The new rule is if they are sufficiently crafty, passwords only need to be changed every 90-120 days (thus lessening the propensity of employees to write their passwords down on a sticky paper and annex them to their workstations).

4. Multi-Factor Authentication (Yay!). Multi-factor authentication (or MFA) generally involves giving employees token or web applications for their smartphones that allow for an identification code to be transmitted to the employee and only to the employee. He or she is then required to use the token to access the network.

5. Watch for biometric authentication to become standard soon. "Biometric solutions measure specific characteristics of a person, including voice, handwriting, fingerprint(s), face, retina or iris of the eye, gait, vein infrared thermogram, hand geometry and palm print, or some combination of all these identifiers, which are collectively termed multimodal-biometrics. Essentially, they are "something about you" that is practically impossible to copy, steal, or reproduce."[24] Indeed some companies are already experimenting with biometric authentication: "MasterCard has been working to announce its "selfie" pay, which allows users to approve online purchases by taking a picture of themselves (facial recognition) for verification. Users can also opt for authenticating their purchase through a fingerprint. The accuracy of facial recognition systems can vary greatly due to factors like lighting, camera angle, sensitivity, and more. Likewise, fingerprint readers are affected by temperature, position, and other factors."[25] Similarly, Barclays is using voice biometrics in an attempt to get away from the password. One expert recently noted, "Biometric authentication is a powerful enabler, allowing businesses smart enough to deploy it to significantly increase rates of registration, gaining data and insight about their customers while also increasing customer security…. This is a win/win scenario which sounds the death-knell for awkward and insecure passwords sooner than we may imagine."[26]

- **VISIBILITY AND MONITORING** — real 24/7 visibility is required across the network in order to understand all user activity — sanctioned and unsanctioned — so that suspicious traffic is blocked, stopped, or detonated before it can invade the core network. We again draw your attention to machine learning and deep learning cybersecurity hardware that can give the sort of visibility you need to monitor traffic both on premises and in the cloud.

  For an on-premises network down the hall, organizations have both the capability and availability to monitor whatever traffic comes down the pike. For a cloud-based environment, customers are giving up a lot of control over the data, and often their ability to monitor network traffic. If there is a rogue insider, or there was a theft of passwords and privileges because of a successful spearphishing attack, your network devices need to pick up on anything that appears "not normal."

- **APPLICATION SAFETY AND SECURITY** — As we have noted above in talking about by the hybrid cloud model and the SaaS deployment mode, companies often will have many applications they rely upon for their daily business needs. There must be processes and procedures around updating applications so they are adding value rather than adding risk.

Applications in a cloud environment can provide challenges based upon cloud deployment models since, many times, responsibility for the application can vary. Here are the general rules of the road:

- IaaS — With Infrastructure as a Service, since the customer is responsibility for every above-the-bare-bones server and network, the customer is of course responsible for the safety and security of the application. The same is true, therefore, for the application security policy, either on-premises or in the cloud.
- Paas — With Platform as a Service, there is shared responsibility for security. The customer has responsibility for application deployment and for securing access to the application. The CSP has responsibility for securing the infrastructure, operating system, and the middleware.
- SaaS — Application security is generally the responsibility of the CSP, subject to the terms of the service level agreement. Thus it is important for the customer to understand the CSP's patching cycle and cybersecurity defenses, including how the data stored in the cloud is protected against administrative access.
- **AUDITING AND COMPLIANCE IN THE CLOUD** — This is a hot topic currently because of the mass migration of many businesses, including healthcare providers and HMOs, to a cloud environment. Based upon your industry sector, you could be subject to a variety of different regulations:

1. The Health Insurance Portability and Accountability Act of 2013 (HIPAA) designates CSPs as business associates of covered entities, which means CSPs must also be HIPAA compliant.
2. SEC OCIE.
3. FFIEC, which generally provides oversight over banking institutions.
4. SEC Reg. SCI, which is a new SEC regulation governing self-regulatory organizations (like the NYSE) and other trading exchange platforms.
5. SEC Reg. SP (Section 504 of Graham Leach Bliley), which generally governs the collection, disclosure, and protection of PII for financial institutions.
6. Payment Card Industry (PCI) Data Security Standards (DSS), which applies to the handling of credit card data anywhere in the world. "The Payment Card Industry Security Standards Council, which essentially governs the entire credit card industry, published a set of cloud security guidelines in 2013 specifically about cloud security. The 50-page document clearly states that 'cloud security is a shared responsibility between the cloud service provider (CSP) and its clients.'"[27]
7. Sarbanes-Oxley Act of 2002 — "The SSAE 16 standard (which replaces the old SAS 70 standard), is a report that states that a company has the proper internal controls and processes for the type of information and transactions it handles, and for the impact (fi-nancial and otherwise) it causes on other organizations. These can range from data center related elements, such as networking and power redundancy, all the way through to data protection policies."[28] If you need a CSP that is SOX compliant, request such documentation from the CSP you intend to use, which is likely already SOX complaint.

Customers also have to be able to assess, through an audit-like process, documents and evidence showing whether or not cloud service providers that advertise themselves as "regulatory compliant" are truly compliant. Customers need access to reports of the CSP's independent auditor, as well as access to the portion of the CSP's logs and reporting information relating to their own data and audit events. Auditors may be employed by the customer or the provider, but at the very least they need to be independent and have access to the policies and procedures that evidence the CSP's security controls.

Cloud Computing Cybersecurity Concerns:

Visibility and Monitoring. Once again, as more data is migrated to the cloud, and more and applications are accessed from a cloud environment, it will be necessary for companies to have excellent visibility when it comes to monitoring and logging data associated with the company's operations. For a private cloud, this is easier, as the data is under the control of the company and the normal rules applicable to its own on-premises network will apply.

For a public cloud, this is much harder as the level of visibility and monitoring will be subject to whatever is offered in the basic cloud offerings of AwS, Microsoft, and Google/Alphabet. This level of visibility is governed by the SLA in place. Very often for SMBs, the low level of visibility is non-negotiable. For SMB's however, they are able to leverage the cybersecurity of the CSP, which should be more formidable. For bigger companies, they may have more success negotiating more visibility.

Network Controls. To protect its data, it is important for any company to understand what network security solutions to apply. This point is equally applicable for cloud computing and CSP's as well. Here are the more common network controls:

1. Firewalls;
2. Anti-DDoS remediation solution;
3. Intrusion detection and prevention devices;
4. Advanced machine learning or deep learning cybersecurity technology that provides very-high accuracy in detecting malware.
5. If the company does not use an advanced machine learning or deep learning solution, how will its endpoints be monitored? And by whom in a cloud-based environment?[29]

Incident Response. Again if you are a private cloud customer, apply the normal rules you would for any on-premises network when considering incident response planning, incident response, and remediation efforts.

For those customers in a public cloud, their ability to both detect and respond to a cyber-security incident will generally be limited to what is in their service level agreement. For SMBs, the chances of participating in an incident response are pretty limited. Bigger clients might have more negotiating leverage. Generally public cloud customers should insist on:

1. Network logging information as it pertains to their data;
2. Reasonable notice of an incident or breach (we would submit that 12-24 hours is reasonable notice; 72 hours would not be); and
3. Historical network security information concerning incidents and breaches (to understand the effectiveness of the CSP's cybersecurity).

Business Continuity/Disaster Recovery Issues. As with on-premises solutions, companies should understand what happens if the worst case scenario happens and they need to restore their network. Who restores the network? How is it restored? How long does it take to restore the network? All of these are good questions for which answers should be obtained.

Human Resource Issues. In a recent survey by Brightscale of over 1000 IT professionals concerning cloud usage and trends, the participants were asked what their biggest concern was in adopting cloud-based environments. The study noted that "Lack of resources/expertise" increased from 27% last year to 32% this year to supplant security as the largest concern. As more organizations are placing more workloads in the cloud, the need for expertise has grown. Additional training of IT and development staff will be critical to helping address this challenge."[30] This finding is not surprising. As companies adopt cloud platforms, especially hybrid cloud platforms, a new kind of multi-skilled professional will be needed who can keep an eye on the varied elements of a hybrid cloud network. We also don't find it surprising that security automation and orchestration is growing as well, as the need for ultimate visibility in the various attack surfaces continues to grow as well.

Key Questions to Ask When Interviewing/Considering Cloud Service Providers

When considering a cloud migration, based upon the above background, here are inquires potential customers should consider making:

- What information security and privacy standards or regulations will apply to the cloud customer's domain? Can and will the CSP comply with these standards?
- How, by whom, and where will the CSP process and store your data?
- Does the cloud service provider have appropriate governance and notification processes for their services, consistent with the customer's requirements?
- Is it clear what legal and regulatory controls apply to the provider's services? Is the cloud service provider certified by FedRamp, HIPAA, or any other regulatory body that the customer must be in compliance with?
- What do the Master Services Agreement and Service Level Agreement say about the split of security responsibilities between provider and customer?
- What are the CSP's backup and business continuity practices?
- What support is provided by the CSP if data tokenization or encryption is desired as an additional protection against data theft (and as a potential shield if that data is later stolen)?

AUDIT RISK AND CLOUD GOVERNANCE ISSUES

- Is a report by an independent audit agency available for covering the provider's cloud services? Does the audit information conform to one of the accepted standards for security audit such as ISO 27001/27002?
- Does the provider have mechanisms to report to the customers both routine and exceptional behavior related to its services? Are all appropriate events and actions that have security implications logged?
- Is there an incident reporting and incident handling process that meets the needs of the customer?

ACCESS AND IDENTIFICATION CONTROLS PROVIDED BY THE CLOUD SERVICE PROVIDER

- Do the provider services offer fine grained access control? "By implementing more granular access controls and assigning permissions on an as-needed basis, it's possible for security professionals to take charge of critical cloud security policies while delegating more repetitive tasks to third party providers."[31]
- Is multi-factor authentication supported for by the cloud service provider?
- Can the provider give reports for monitoring user access?
- Is it possible to integrate or federate customer identity management systems with the identity management facilities of the provider?
- Who is responsible for monitoring endpoint activity?

DATA PROTECTION AND GOVERNANCE INFORMATION

- Is there a catalog of all data assets that will be used or stored in the cloud environment?
- Is there a description of responsible parties and roles?
- For structured data held in databases in a multi-tenant cloud environment, is there proper separation or segmentation of data belonging to different customers?
- Have appropriate confidentiality, integrity, and availability measures been applied to data used or stored in the cloud (e.g. tokenization and encryption)?

ISSUES RELATED TO DATA PRIVACY FOR DATA STORED IN THE CLOUD

- Is PII or personal healthcare information going to be stored/processed by the cloud service provider?
- What data protection laws and regulations apply, given the industry and the locations in which the customer operates and/or the locations where the provider stores the data?
- Do the provider's services have appropriate controls in place for handling PII?
- Are responsibilities for handling PII stated in the cloud service agreement?
- Is the data to be kept in the cloud tokenized or encrypted? If it is not, should it be in order to add an extra layer of control related to the regulated data?

ENDNOTES:

[1] The National Institute of Standards and Technologies has defined cloud computing as "a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or ser-vice provider interaction" See e.g. NIST Special Publication 800-145, available at http://www.nist.gov/itl/csd/cloud-102511.cfm.

[2] See "Public Cloud Computing Growing Almost 50 Percent Annually, Cisco Says," available at http://www.forbes.com/sites/joemckendrick/2016/05/31/public-cloud-computing-growing-almost-50-percent-annually-cisco-says/#772d0d302273. (hereinafter referred to as the "Cisco Traffic Report")/

[3] Id.

[4] Id.

[5] See "Cloud Computing Trends: 2016 State of the Cloud Survey," available at http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2016-state-cloud-survey.

[6] See "Cloud Computing Shift Accelerates, Reversing Recent Dip," available at http://blogs.wsj.com/cio/2016/04/15/cloud-computing-shift-accelerates-reversing-recent-dip/

[7] See "Johnson & Johnson Targets 85% of Apps in Cloud by 2018," available at http://blogs.wsj.com/cio/2016/07/01/johnson-johnson-targets-85-of-apps-in-cloud-by-2018/

[8] Id.

[9] See "Cloud Computing Shift Accelerates, Reversing Recent Dip," available at http://blogs.wsj.com/cio/2016/04/15/cloud-computing-shift-accelerates-reversing-recent-dip/.

[10] See "Big Banks Starting to Embrace Public Cloud, Deutsche Bank Says," available at http://blogs.wsj.com/cio/2016/06/09/big-banks-starting-to-embrace-public-cloud-deutsche-bank-says/

[11] See "How To Protect Your Cloud Accounts From Being Hacked," available at http://www.csoonline.com/article/3088605/security/how-to-protect-your-cloud-accounts-from-being-hacked.html. The Cisco Traffic Report also notes that Cisco expects an increase in the amount of public cloud traffic as people become more comfortable with the Cloud.

[12] See "Enterprise Impressions of Cloud Security in 2016," available at http://www.tripwire.com/state-of-security/security-data-protection/enterprise-impressions-of-cloud-security-in-2016/.

[13] Id.

[14] See

[15] See generally, "7 things to know about hybrid cloud and hybrid IT," available at http://www.thoughtsoncloud.com/2016/05/7-things-know-hybrid-cloud-it/.

[16] See "A CIO's Biggest Security Challenge May Surprise You: Cloud Compliance," available at http://www.cio.com/article/3101776/leadership-management/a-cio-s-biggest-security-challenge-may-surprise-you-cloud-compliance.html.

[17] See The AwS IoT Cloud, available at https://aws.amazon.com/iot/.

[18] See Understanding the Cloud Computing Stack: Saas, PaaS and Iaas, available at https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas/.

[19] See "Data protection vs. authentication: Tackling the cloud security dilemma," available at http://www.cbronline.com/news/cybersecurity/data/data-protection-vs-authentication-tackling-the-cloud-security-dilemma-4984423.

[20] The "where" is my stuff question is the makings of "data sovereignty," which is "the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located." See Data Protection in the Cloud: Not Your Grandfather's Data Protection," available at http://www.csoonline.com/article/3087409/security/data-protection-in-the-cloud-not-your-grandfather-s-data-protection.html.

[21] Attempts should be made in the SLA to direct/mandate that jurisdiction be held in only one "certain" jurisdiction.

[22] See "The Best Identity Management Solutions of 2016," available at http://www.pcmag.com/article2/0,2817,2491437,00.asp.

[23] Id.

[24] See "Biometric Authentication: Making mobile devices and apps safer," available at http://betanews.com/2016/04/04/biometric-authentication-making-mobile-devices-and-apps-safer/.

[25] Id.

[26] See "Barclays Set to Roll-Out Voice Biometrics," available at http://www.infosecurity-magazine.com/news/barclays-set-to-rollout-voice/.

[27] See "Coordinating Compliance in Your Hybrid Cloud," available at http://www.csoonline.com/article/3088527/security/coordinating-compliance-in-your-hybrid-cloud.html

[28] See "What US businesses should know about compliance and regulatory issues before adopt-ing a cloud strategy," available at http://www.zdnet.com/article/what-us-businesses-should-know-about-compliance-and-regulatory-issues-before-adopting-a-cloud-strategy/.

[29] See "What happens when security enters the cloud?" available at what-happens-when-security-enters-the-cloud-4979003.

[30] See "Cloud Computing Trends: 2016 State of the Cloud Survey," available at http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2016-state-cloud-survey.

[31] See "Attitude Adjustment: Cloud Security Risks Losing Steam as Top Worry," available at https://securityintelligence.com/news/attitude-adjustment-cloud-security-risks-losing-steam-as-top-worry/.

CONCLUSION:
DON'T ABANDON SHIP (JUST YET)

Last year, we joked (somewhat) in the conclusion to "Navigating the Cybersecurity Storm" that it was time to consider abandoning ship given the cyber events of 2015. Though the events of 2016 have really not been much better (some might say that, with ransomware, they have been arguably worse), we have seen this year some sparks of life in our Cybersecurity Ecosystem that lead us to believe we are at or nearing an inflection point, where things could go either way based on how proactive the companies and people reading our book are.

Whether you like going to the health club or not, it's an individual choice on how to act or behave. For instance, to go to the gym regularly means generally a better state of health and fitness. It may even mean living a longer life. To not go to the gym, well, anything goes, including a heart attack.

Individuals can choose to believe the status quo is just fine and continue to play whack-a-mole with cyber threats, incursions, and spear phishing attempts. For instance, they can choose to not follow best practices and not back up their network on a regular basis with a segmented backup solution, and then pay the ransom after their files get encrypted following a ransomware-laced spear phishing attack. Or companies can to do something different and more substantial to improve their cybersecurity posture. This is especially true for companies in transition to an IoT business model, or companies otherwise in fast technological change because their customers and clients demand it.

For others less daring, it might just be incremental improvements to the backup and recovery systems so they are not held hostage to a ransomware attack. But of one thing we are very certain: with cybersecurity, the status quo will not do. Today, cyber attackers are more challenging and devious than ever. We must do something different. Former FBI Assistant Director James Trainor, Jr. made the same point at the Fordham Law School ICCS event (summer 2016), stating, "[C]yber challenges basic intuitions about the threat we're facing, and about how we're organized to combat it. . . [W]e are confronting a challenge that should give us pause, and cause us to alter the way we're organized at a fundamental level." [emphasis supplied]

We have always promised to give you actionable, real advice to help you understand and deal with today's cybersecurity threats. We hope we fulfilled this promise in Book Two. For our concluding chapter, here are some thoughts that Chris and I want to leave you with, to chew on (like a fine piece of filet mignon). These steps are things you can do today. Some cost money; some very little. But all of them will take you in steps towards tomorrow:

1. **CONSIDER THE CLOUD AS A POTENTIAL "SAFE HAVEN"** — How much money do you think Amazon, Alphabet, and Microsoft spend on cybersecurity each year? How much money do you spend on cybersecurity each year? If the answer to question one is "a lot" and the answer to question two is "not very much," then consider moving your business IT and data storage needs to a cloud environment. For the most part, unless you are an international investment bank or global company, we feel it's probably true that the big

three cloud providers can do a better job securing your network than you. They have lots of resources, and lots of controls around accessing your data. You can also encrypt or tokenize your data in the cloud.

For small- to mid-sized businesses (the "SMBs") going to the cloud fixes a lot of evils and provides an excellent return on investment. Yes, you are giving up some control (unless you are moving to a private cloud), but in return you are probably more secure. The investment in moving to the cloud might be the best one you make. Likely it will be a better investment than trying to update or patch your existing "gray-haired" network hardware solution. And the reviews and plans you'll develop in your cloud transition will have a fresh and lasting impact on how your business protects its data.

2. **CONSIDER AI, MACHINE LEARNING, DEEP LEARNING AND COGNITIVE COMPUTING YOUR NEW BEST FRIENDS** — You have heard a lot about these technologies in Book Two. We are big believers that they could be game changers to protect your company or business from disaster. Don't be afraid of these technologies. Don't be afraid of the costs because these solutions are not as pricey as you might think. Be afraid of not adopting these technologies. Especially given the skilled cybersecurity worker shortage we described throughout this book. I would not want to be at a board meeting after a hack, when a director says, "Why didn't we know of this problem months ago? Aren't there devices I read about in [every newspaper and journal] that use AI or machine learning to protect networks?" Umm, what would your answer be to this question? Don't be the next _____ [fill in the blank with a bad attack] by taking five months (or more) to find the malware that has been present on your network and was stealing your stuff all this time.

3. **ADOPT THE NIST CYBERSECURITY FRAMEWORK** — We rolled out the NIST Framework in "Navigating the Cybersecurity Storm", and continue to be very bullish on the positive effects that the Framework can bring to your organization. At the very least, it is a discussion point that allows the C-Suite, and IT to have fulsome discussions around cybersecurity and how to best protect the IT and IP "crown jewels" of the company. And at the other end of the spectrum, the NIST Framework is one of the cornerstone documents underlying various regulatory schemes in the U.S.

4. **SPEAR PHISHING TRAINING ANYONE? ANYONE? BUELLER?** — Spear phishing is one of the most deadly accurate threat vectors this year (see, e.g., about 500 hacks this year that we know of). You cannot train enough. But you can automate your training through PhishMe or some other automated provider. The fact is that spear phishing training works and lowers your risk of attack. How often do you train for spear phishing or business email compromise or CEO email fraud? Once a year, you say? Back to the court for layup practice. Because more training is a layup. It won't reduce your risk to zero, but it will help reduce it to a tolerable number. Our advice: don't click on the link or attachment.

5. **EMAIL FILTERS** — Better yet, employ an acceptable email solution from a variety of big name consultants. Better not to have that Spear phish even hit your employee's inbox. The Sultan of Arabia has lot of riches to give away, but don't let your employees know of that possibility at all. Because it doesn't exist.

6. **IDAAS** — Time to handle this perennial problem in the cloud, where you can more easily manage identity management, access, authentication, and logging, especially in larger companies that run multiple applications. Manual identity management is difficult at best. It

needs to be updated constantly. IDaaS can simplify these problems.

7. **EVERYONE DOES NOT NEED ADMINISTRATIVE PRIVILEGES** — This is the principle that says, in sum, that a user should only have access to whatever system or application that he or she needs to do his or her job. Problems occur when this rule is not explained well or not explained at all to non-IT people who feel it is some sort of slight that they cannot access "everything." Least privilege user, in actuality, is helpful to both the employee and organization because employees can be tricked to click on a link or attachment. If they have privileges to the Kingdom, so will the attacker. If you don't have a least privileged access rule, you should think about getting one and explaining its positive benefits to the organization.

8. **UPDATE YOUR INTRUSION DETECTION/PREVENTION HARDWARE** — If you don't adopt AI or one of its related technologies, at the very least invest in behavioral analytical hardware to help you judge normal from abnormal. And for goodness' sake, we need to get in the mindset of 24/7 continuous monitoring of your network. Just keeping an eye on things during business hours doesn't cut it.

9. **INCIDENT RESPONSE PLANNING** — We focused a lot on this topic in Book One; a little less in Book Two. How did your training go this year? How many times did you table top your incident response plan with all hands on deck? Did you update and review your crisis communications plans? If not, why not? How improved is your incident response capability now? How sure are you that it's at the level it should be? Have you tested your IR plan against a red-team exercise?

10. **SECURITY AS A SERVICE** — Yep, we said it again. If you do not have the staff, HR, and budgetary resources — or time — to monitor your network, consider outsourcing your cybersecurity to a third party. We know of many clients employing this service already and they are very happy. It is not as if you are 100% hands off. The SECaaS companies monitor your network and endpoints and tell you if there is a problem. You get to leverage the extent of their own security services and intelligence across their clientele for just a fraction of the cost to build. If you get a call from them, it is likely a big problem. But it won't be a false positive and thus you won't be chasing your tail, expending even more resources you don't have.

11. **CLOUD BASED DDOS REMEDIATION SERVICES** — Many companies think they can handle a large DDoS attack on their own. If you are a big investment bank or Fortune 50 company, you might have the resources in place to do a decent job against an average-sized attack. The problem is that after the October DDoS of Dyn, described above in Chapter One, the "average-sized attack" seems to be growing weekly, especially with the growth of IoT-connected devices. But otherwise, consider a cloud-based DDoS remediation company that can block all known bad addresses and deflect bad traffic away from your network. There are some very good DDoS remediation companies out there and the service costs very little compared to, statistics say the $50-100,000 per hour large companies lose when hit with a large attack.

12. **CLOUD BASED DATA RECOVERY SERVICES (OR "DRAAS")** — This is another huge improvement made possible by the cloud. With a DRaaS service,[1] you can recreate your network infrastructure in a cloud environment. This can make your back up solution easier and allow you to get back into the game quicker if your network goes down because of an attack.

13. **DON'T PAY THE RANSOM!** — Have cloud-based or offline/segmented backup media ready to go. Again, this is a low cost issue for a very big problem that caught hundreds of companies, universities and hospitals off-guard this year. Paying the ransom only rewards cybercrime and makes it more likely that you and/or others might be attacked again. In addition, make sure you test your backup solution frequently so that it's ready to go when you need it. Fumbling over backups (or worse yet, not having them) can be a large waste of time and money, and to regulators and the public, it might show that your cybersecurity game is not up to par.

14. **VULNERABILITY AND COMPROMISE ASSESSMENTS** — We mentioned these assessments last year as a way for corporate directors to understand how their network, and their network security team, is performing. We mention them this year because we feel the same way. As attackers move much faster than we do, we are becoming increasingly vulnerable to attacks, either through known vulnerabilities or unknown vulnerabilities. Or through spear-phishing employees. We tell clients all the time, "Would you rather know first if you've been hacked ?" Because finding out through other means (like a phone call from the FBI) is generally much more distressing. Note also that the regulatory trend today is that assessments are not just a "nice to have," but a "must have." We can tell you for a fact that such assessments generally don't cost a lot. And their results could be invaluable.

15. **DO YOU SHARE CYBER THREAT INTEL?** — Cyber threat intelligence is a great way to correlate cyber threat information with your other indicators of network compromise. For the most part, it is not costly. And given the participants and providers involved, the threat intelligence is usually actionable. Especially since it is quite common for attackers to stay within the same industry vertical after they have achieved some modicum of success (like the attacks last year in the higher education sector). Again, this is a "why not" solution to the broader cyber problem we face in this nation.

16. **LAST BUT NOT LEAST** — Don't discount the value of engaging — even critical — conversations with the board, the C-Suite, and the CISO about how your organization is tracking, reporting, and managing its security activities. Board directors should seek confirmation that the organization's handling of cybersecurity projects and its ability to detect and respond to incidents are continually improving towards an acceptable maturity level.

We hope you enjoyed reading our book. If you have any questions or comments on anything we have written, please don't hesitate to reach out and contact either of us. We did not write this book for money or glory. We wrote it to hopefully help you deal with the cyber threats of tomorrow. We are here to help and serve. We'd rather that you not wait until a data breach before reaching out to us and seeking our advice, but if you need help after the smoke clears and want to avoid a repeat of a bruising experience, contact us. What are you waiting for?

ENDNOTES:

[1] See e.g. "Magic Quadrant for Disaster Recovery as a Service," available at https://www.gartner.com/doc/reprints?id=1-39N94AJ&ct=160620&st=sg

ABOUT ADVISEN

Advisen is leading the way to smarter and more efficient risk and insurance communities. Through its information, analytics, ACORD messaging gateway, news, research, and events, Advisen reaches more than 150,000 commercial insurance and risk professionals at 8,000 organizations worldwide. The company was founded in 2000 and is headquartered in New York City, with offices in the US and the UK.

ABOUT AIG

American International Group, Inc. (AIG) is a leading global insurance organization. Founded in 1919, today we provide a wide range of property casualty insurance, life insurance, retirement products, mortgage insurance and other financial services to customers in more than 100 countries and jurisdictions. Our diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: http://www.linkedin.com/company/aig.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.

Investigations · Compliance Solutions · Cyber Defense

ABOUT K2

K2 Intelligence is an industry-leading investigative, compliance and cyber defense services firm founded in 2009 by Jeremy M. Kroll and Jules B. Kroll, the originator of the modern corporate investigations industry. Over the last 40 years, Jules, Jeremy, and their teams have built a reputation not only for investigative, analytic and advisory excellence but for the independence and insight they bring to investigations. With offices in New York, London, Madrid, Tel Aviv and Geneva, K2 Intelligence advises governments, companies, boards and individuals in business areas including: Complex Investigations & Disputes; Anti Money Laundering and Regulatory Compliance; Integrity Monitoring & Compliance; Data Analytics & Visualization; Board Advisory; and Cybersecurity Investigations & Defense.
For more information, visit www.k2intelligence.com

DIRECTOR AND OFFICER GLOSSARY OF DEFINED CYBERSECURITY TERMS[1]

A

Active Attack

An actual assault perpetrated by an intentional threat source that attempts to alter a system, its resources, its data, or its operations.

Advanced Persistent Threat

An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

Alert

A notification that a specific attack has been detected or directed at an organization's information systems.

Antispyware Software

A program that specializes in detecting and blocking or removing forms of spyware.

Antivirus Software

A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents. Sometimes by removing or neutralizing the malicious code.

Asset

A person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value.

Extended Definition: Anything useful that contributes to the success of something, such as an organizational mission; assets are things of value or properties to which value can be assigned.

Attack Pattern

Similar cyber events or behaviors that may indicate an attack has occurred or is occurring, resulting in a security violation or a potential security violation. Extended Definition: For software, descriptions of common methods for exploiting software systems.

Attack signature

A characteristic or distinctive pattern that can be searched for or that can be used in matching to previously identified attacks.

Authentication

The process of verifying the identity or other attributes of an entity (user, process, or device).

Authenticity

A property achieved through cryptographic methods of being genuine and being able to be verified and trusted, resulting in confidence in the validity of a transmission, information or a message, or sender of information or a message.

Authorization

A process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Extended Definition: The process or act of granting access privileges or the access privileges as granted.

B

Behavior Monitoring

Observing activities of users, information systems, and processes and measuring the activities against organizational policies and rule, baselines of normal activity, thresholds, and trends.

Bot

A computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under remote the command and control of a remote administrator.

Related term: A member of a larger collection of compromised computers known as a botnet.

Bot Master

The controller of a botnet that, from a remote location, provides direction to the compromised computers in the botnet.
Synonym(s): bot herder

Botnet

A collection of computers compromised by malicious code and controlled across a network.

Bug

An unexpected and relatively small defect, fault, flaw, or imperfection in an information system or device.

C

Cloud Computing

A model for enabling on-demand network access to a shared pool of configurable computing capabilities or resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Critical Infrastructure

The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.

Cryptographic Algorithm

A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output.

Cryptography

The use of mathematical techniques to provide security services, such as confidentiality, data integrity, entity authentication, and data origin authentication.

Cryptology

The mathematical science that deals with cryptanalysis and cryptography.

Cyber Exercise

A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption.

Cyber Infrastructure

The information and communications systems and services composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements:

- Processing includes the creation, access, modification, and destruction of information.
- Storage includes paper, magnetic, electronic, and all other media types.
- Communications include sharing and distribution of information.

Cybersecurity

The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Cyberspace

The interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

D

Data Breach
The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

Data Integrity
The property that data is complete, intact, and trusted and has not been modified or destroyed in an unauthorized or accidental manner.

Data Loss
The result of unintentionally or accidentally deleting data, forgetting where it is stored, or exposure to an unauthorized party.

Digital Forensics
The processes and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes.

Digital Rights Management
A form of access control technology to protect and manage use of digital content or devices in accordance with the content or device provider's intentions.

Digital Signature
A value computed with a cryptographic process using a private key and then appended to a data object, thereby digitally signing the data.

Disruption
An event which causes unplanned interruption in operations or functions for an unacceptable length of time.

Distributed Denial Of Service
A denial of service technique that uses numerous systems to perform the attack simultaneously.

Dynamic Attack Surface
The automated, on-the-fly changes of an information system's characteristics to thwart actions of an adversary.

E

Encryption
The process of transforming plaintext into ciphertext.

Enterprise Risk Management
A comprehensive approach to risk management that engages people, processes, and systems across an organization to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives.

Event
An observable occurrence in an information system or network.

Extended Definition: Sometimes provides an indication that an incident is occurring or at least raise the suspicion that an incident may be occurring.

Exfiltration
The unauthorized transfer of information from an information system.

Exploit
A technique to breach the security of a network or information system in violation of security policy.

Exploitation Analysis

In the NICE Workforce Framework, cybersecurity work where a person: Analyzes collected information to identify vulnerabilities and potential for exploitation.

Exposure

The condition of being unprotected, thereby allowing access to information or access to capabilities that an attacker can use to enter a system or network.

F

Failure

The inability of a system or component to perform its required functions within specified performance requirements.

Firewall

A capability to limit network traffic between networks and/or information systems.

Extended Definition: A hardware/software device or a software program that limits network traffic according to a set of rules of what access is and is not allowed or authorized.

H

Hacker

An unauthorized user who attempts to or gains access to an information system.

I

Incident

An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

Extended Definition: An occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Incident Management

The management and coordination of activities associated with an actual or potential occurrence of an event that may result in adverse consequences to information or information systems.

Incident Response

Cybersecurity work where a person responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats; uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

Incident Response Plan

A set of predetermined and documented procedures to detect and respond to a cyber incident.

Indicator

An occurrence or sign that an incident may have occurred or may be in progress.

Information System Resilience

The ability of an information system to: (1) continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (2) recover effectively in a timely manner.

Inside (R) Threat

A person or group of persons within an organization who pose a potential risk through violating security policies.

Extended Definition: One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.

Intrusion Detection

The process and methods for analyzing information from networks and information systems to determine if a security breach or security violation has occurred.

Investigation

A systematic and formal inquiry into a qualified threat or incident using digital forensics and perhaps other traditional criminal inquiry techniques to determine the events that transpired and to collect evidence.

M

Macro Virus

A type of malicious code that attaches itself to documents and uses the macro programming capabilities of the document's application to execute, replicate, and spread or propagate itself.

Malicious Applet

A small application program that is automatically downloaded and executed and that performs an unauthorized function on an information system.

Malicious Code

Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Malicious Logic

Hardware, firmware, or software that is intentionally included or inserted in a system to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Malware

Software that compromises the operation of a system by performing an unauthorized function or process.

Mitigation

The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences.

Extended Definition: Implementing appropriate risk-reduction controls based on risk management priorities and analysis of alternatives.

Moving Target Defense

The presentation of a dynamic attack surface, increasing an adversary's work factor necessary to probe, attack, or maintain presence in a cyber target.

N

Network Resilience

The ability of a network to:

(1) provide continuous operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged);

(2) recover effectively if failure does occur; and

(3) scale to meet rapid or unpredictable demands.

P

Passive Attack

An actual assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations.

Penetration Testing

An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Phishing

A digital form of social engineering to deceive individuals into providing sensitive information.

Privacy

The assurance that the confidentiality of, and access to, certain information about an entity is protected.

R

Recovery

The activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.

Resilience

The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

S

Secret Key

A cryptographic key that is used for both encryption and decryption, enabling the operation of a symmetric key cryptography scheme.

Spam

The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Spear Phishing

An e-mail spoofing fraud attempt that targets a specific organization, or a specific individual with an organization or organization department, seeking unauthorized access to confidential data.

Spoofing

Faking the sending address of a transmission to gain illegal (unauthorized) entry into a secure system.

Spyware

Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

T

Tabletop Exercise

A discussion-based exercise where personnel meet in a classroom setting or breakout groups and are presented with a scenario to validate the content of plans, procedures, policies, cooperative agreements or other information for managing an incident.

Trojan Horse

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

U

Unauthorized Access

Any access that violates the stated security policy.

V

Virus

A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

Vulnerability

A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

W

Worm

A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

ENDNOTES:

This Glossary was adapted from (but simplified by me) for business executives, directors and officers from the National Institute of Standards and Technology "Glossary of Key Information Security Terms," which is available at http://www.nist.gov/manuscript-publication-search.cfm?pub_id=913810.

ADVISEN'S CYBER DATASET

Advisen's Cyber Database is a proprietary relational database of information about various "Cyber risk"-related events which have or could have resulted in significant financial judgments or financial loss to corporate entities.

"Cyber risk" means any risk of financial or physical loss, disruption of services, privacy violation, or damage to the assets or reputation of an organization through either a failure of its information or technology systems, or a malicious act affecting their information or technology systems. While system "hacks" and data breaches get the lion's share of publicity, Advisen's Cyber Dataset also includes such risks as:

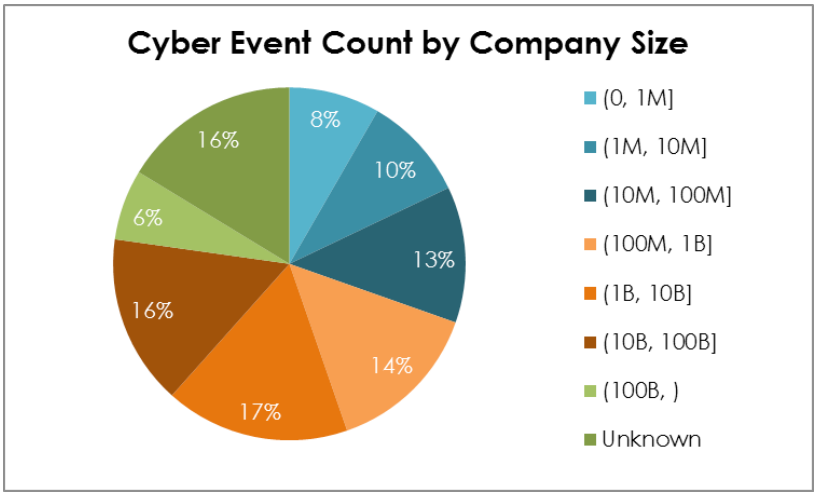
- Cyber Extortion
- Data – Unintentional Disclosure
- Data – Physically Lost or Stolen
- Data – Malicious Breach
- Privacy – Unauthorized Data Collection
- Privacy – Unauthorized Contact or Disclosure
- Identity – Fraudulent Use/Account Access
- Industrial Controls & Operations
- Network/Website Disruption
- Phishing, Spoofing, Social Engineering
- Skimming, Physical Tampering
- IT – Configuration/Implementation Errors
- IT – Processing Errors

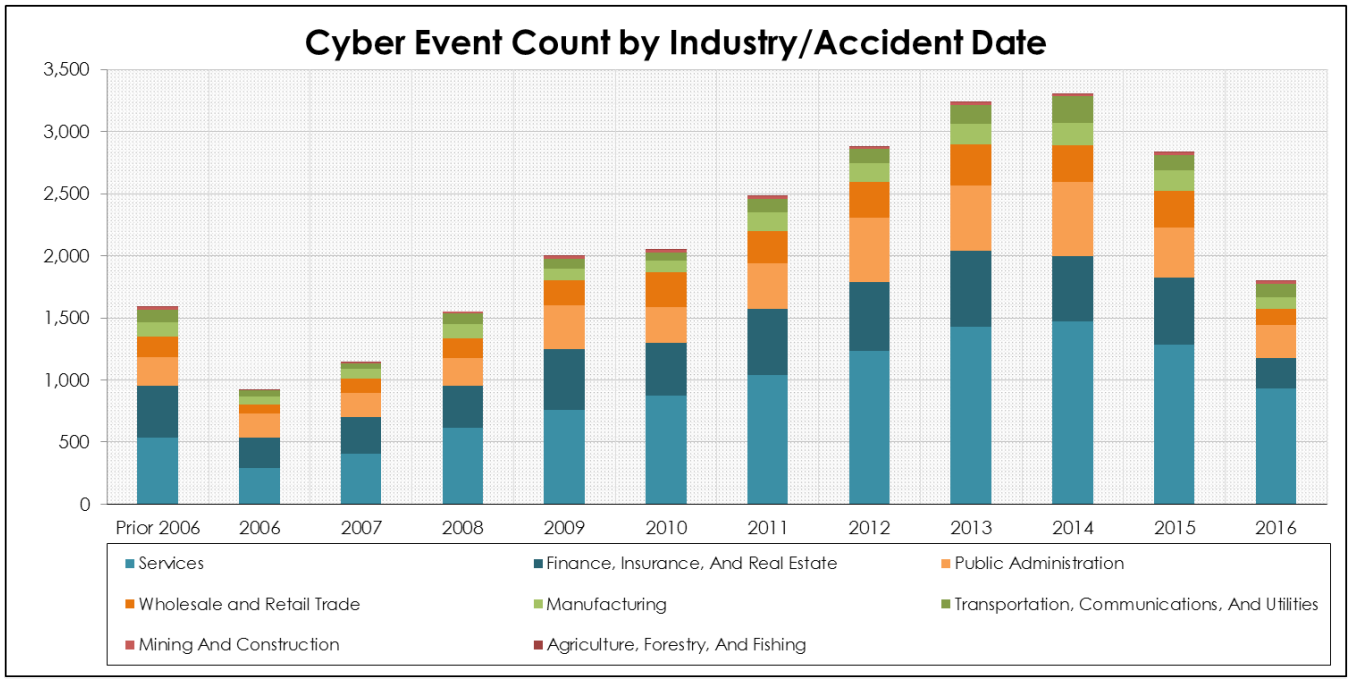
The Advisen cyber database includes more than 32,000 cases involving billions of unauthorized disclosures, thefts, or serious disruptions of customer and employee identities, corporate assets, and systems capabilities.

DATA FEEDS DELIVERY

Advisen's Cyber Data Feeds contain model-ready cyber data, married to current and historic company data. The intersection of loss and company data supports actuaries building sophisticated proprietary algorithms using multiple parameters, such as:

- Case Type
- Case Status
- Affected Count
- Accident Date
- Source of Loss
- Type of Loss
- Actor
- Loss Amount
- Company Size
- Company Type
- Number of Employees
- Industry Code
- Geography





Advisen's Cyber Dataset is constantly growing at a fast pace, and the Cyber Data Feeds will be refreshed on a monthly basis and delivered in Excel.

CYBER DATA FEATURES

Advisen has developed a comprehensive taxonomy for the cyber database that supports actuarial modeling and pricing analysis for insurance brokers, carriers and reinsurers, as well as facilitating cyber risk and trend analysis for cyber vendors.

A proportion of Advisen Cyber Data have been linked by interrelated root causes and been identified as related cases, allowing the user to model the aggregation of the potential risk across the portfolio.

Advisen leverages both Standard Industrial Classification (SIC) code system and North American Industry Classification System (NAICS). The latter provides a greater level of detail about a firm's activity and more accurately assigns the new technology or cutting-edge industries.

Advisen also provides denominator information through StatMaster, which supports more accurate frequency analysis. StatMaster provides time series business information for top level US companies with revenues over $1M that is further segmented into industry and size groupings.

About Advisen Ltd.

Advisen is the leading provider of data, media, and technology solutions for the commercial property and casualty insurance market. Advisen's proprietary data sets and applications focus on large, specialty risks. Through Web Connectivity Ltd., Advisen provides messaging services, business consulting, and technical solutions to streamline and automate insurance transactions. Advisen connects a community of more than 200,000 professionals through daily newsletters, conferences, and webinars. The company was founded in 2000 and is headquartered in New York City, with offices in the US and the UK.

THANK YOU TO OUR SPONSORS!

AIG®

K2 Intelligence

Investigations · Compliance Solutions · Cyber Defense