Security in the Boardroom

August 23, 2017

Palo Alto, California

THE CHERTOFF GROUP

Event Summary

KEY FACTS

165 Total Participants

40% Executives

70% Tech Industry

"While the focus of the conference was on how boards of directors could understand and approach their responsibilities for cybersecurity, the presentations and discussions were more far-ranging than the topic might suggest. Typically such conferences enjoin CISOs to approach the board with a business case for security, couched in language accessible to board members with a business background, and they urge board members to understand cybersecurity as an exercise in risk management, with due attention paid to the familiar range of threat actors and their tactics. This sort of advice is certainly valuable (and such valuable advice was exchanged during the Security Series) but yesterday's sessions covered some ground less often traversed."

– THE CYBERWIRE

"I had the pleasure of attending Chertoff Group's Security Series in Palo Alto, CA. The crowd was made up of CISOs, VCs and high ranking officials in government agencies responsible for our country's cybersecurity"

- 10FOLD COMMUNICATIONS

"I enjoyed all of the panels, the lunchtime dialogue, and the networking in between… well done! I appreciated seeing so many people wanting to learn more about government problems and so willing to solving them..it is why we are here"

– ATTENDEE

Table of Contents

Sponsors

AYASDI
Lumina
BeyondTrust
NEHEMIAH SECURITY
ivanti
SailPoint

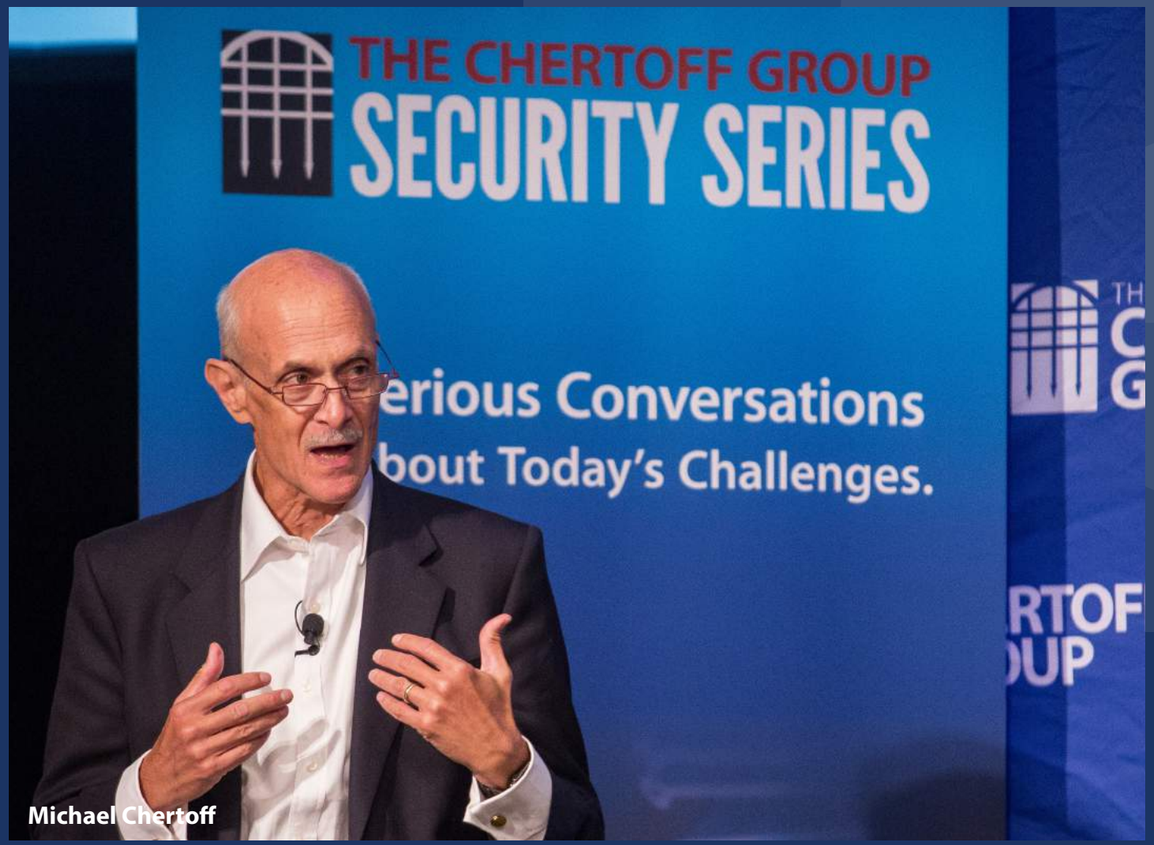
Event Partners

10FOLD
Innovative Capital Ventures, Inc
the cyberwire
SINET Security Innovation Network
theCUBE

Executive Summary

Given the critical role technology has in both creating and solving our security solutions, we thought it was critical that we host our tenth event in Silicon Valley. In 2017, The Chertoff Group Security Series focuses on "Security in the Boardroom" with a goal of providing practical tools to board members and management to improve their organization's cyber resiliency, and drive competitive advantage. Longer term our goal is to see cybersecurity become a core boardroom competency.

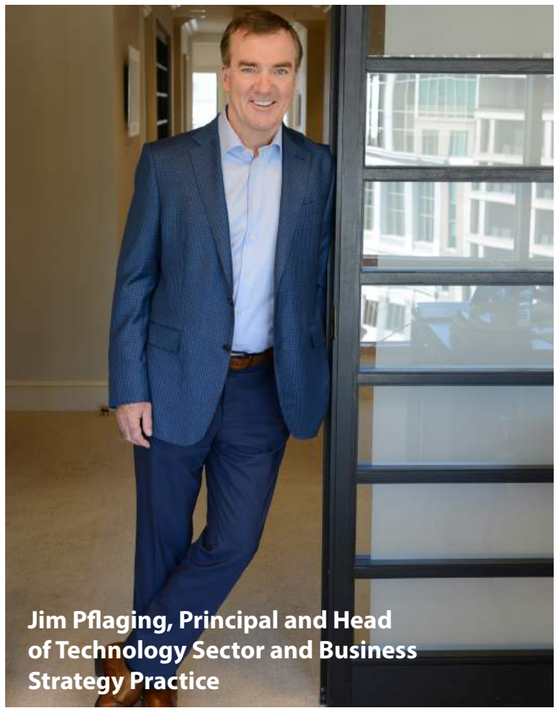
We are living in a period of remarkable change and opportunity enabled by profound tectonic shifts such as cloud, mobility, IoT, crypto currencies / ledgers, and artificial intelligence. In this golden age of innovation, every industry, organization, and government has the imperative to reinvent how they deliver goods, interact with stakeholders, and manage core operational functions. Unfortunately, this golden age has enabled a new class of bad actors to take advantage of security vulnerabilities in these platforms, creating new risk in the form of cyber threat. As a result, building increased resiliency to cyber risk is essential to any organization's prosperity and even survival. Many business leaders now recognize that cybersecurity is more than a technical risk, it's an enterprise wide risk, and often their top business risk. But how do we approach cyber risk from a management perspective? Is it part of the boardroom conversation?



With this in mind, The Chertoff Group Security Series convened over 150 leaders across the security, government, investment, and research communities to share their unique insights around this fundamental question, "How do we make security a boardroom competency?"

The following report offers a glimpse into these discussions. A full video of each discussion is also available from The Chertoff Group's website at www.chertoffgroup.com. We hope you find this report insightful and thought provoking as we seek to pave the road to effective boardroom security discussions and navigate the risk management issues that will be shaping our boardroom agenda in the years to come.

How do we make security a boardroom competency?



Jim Pflaging, Principal and Head of Technology Sector and Business Strategy Practice

Over the past two months, thanks to Petya — FedEx reported 'material' financial impact, Merck reduced 'its full-year 2017 GAAP EPS' and Mendelez, a snack and candy manufacturer, reported a 3% reduction in the company's second quarter growth. This seems like clear evidence that cyber is a top business risk. But is it part of the boardroom agenda? Is it a boardroom competency? We wanted to find out.

Prior to the conference, The Chertoff Group conducted an extensive set of interviews with over 100 executives. Nearly 40% of those interviewed responded in their role as board directors, 50% as C-Suite and the remainder as CISOs. We grouped our questions around things boards care about, netted down to three primary areas – risk management, value creation and metrics.

We found that two-thirds of respondents self-identified a cyber knowledge gap between current and desired knowledge. Most attributed their stunted expertise to overly technical media coverage and desensitizing ubiquity of breach headlines.

The Chertoff Group also identified a "Tale of Two Cyber Cities". In one smaller camp sits very large, public, US-based companies in sectors such as finance, healthcare and technology. Here, Directors are comfortable with security and report regular, productive boardroom security reviews characterized by a mature dialogue with clear metrics of success focused on risk management and business continuity. These groups had experienced CISOs with access to and respect from the board. The second camp, 'everyone else,' revealed a different, darker world. Here, despite the headlines and warnings, cybersecurity is rarely, if ever, on the board agenda. If discussed, it was briefly and in response to a breach or budget request. Many of these firms did not even have a CISO.

The Blueprint is a resource for board members and their respective firms to help position their organizations for success. The Blueprint achieves this by defining roles, key focus areas, and templates for questions to guide each step of the process. With this foundation in place, board members will be more effective in shaping and monitoring cyber risk management and related growth initiatives.

Based on these findings, we developed The Cyber Blueprint. The Blueprint is a resource for board members and their respective firms to help position their organizations for success. The Blueprint achieves this by defining roles, key focus areas, and templates for questions to guide each step of the process. With this foundation in place, board members will be more effective in shaping and monitoring cyber risk management and related growth initiatives. The Blueprint consists of three tiers that are primarily organized around distribution of responsibilities.

The first tier is management-led, with boards providing oversight and direction. The second is board-led, while the final tier is a shared responsibility. The management-led group contains core elements of a good risk management program: governance, measurement and response. The second focuses on culture and people. The third is about awareness of the world around us and foresight.

Key questions for board members include:

Tier 1
Risk Management Fundamentals

GOVERNANCE

Have we prioritized our risks?

MEASUREMENT

Do we know what success looks like?

enter

RESPONSE

Can we execute?

Tier 2
A Security-conscious Organization

CULTURE

Do we have a CEO-led cyber-conscious culture that respects and values security?

PEOPLE

Do we have confidence in the senior staff leading the security program?

Tier 3
Self-awareness and Critical Thinking

POLICY

Do we understand what is coming down the pipe and can we shape it?

FORESIGHT

Can we see around corners?

The Take-away

Through this study and our experience with Board directors, we learned the road to effective boardroom security discussions is easier if you follow The Cyber Blueprint and these 3 guidelines:

- Keep it **Relevant** – Don't underestimate the power to educate through current events.
- Make it **Risk-focused** – This is a language Boards understand.
- Stick to your **Role and focus on outcomes**.

Panels and Spotlights

Spotlight: Perspectives on Borders, Walls, and Opportunities for Mutual Aid, Commerce, and Security Eric Frost, Director, Homeland Security Graduate Program, San Diego State University

Governance, Measurement, and Response

Artificial Intelligence and Security

Spotlight: In Search of the Warrior Spirit Richard Strozzi – Founder & Co-Director of Methodology, Strozzi Institute

Fireside Chat: The Board's Perspective on Cyber Security: Risk Management & Growth Strategy

How Cryptocurrencies and Distributed Ledgers Will Transform the Digital Economy

Governance, Measurement, and Response

According to Forbes and BNC, nearly 70% of board members say digital transformation is forcing fundamental changes to their security strategies. What role should the CISO have in developing the larger security strategy? What is the boards role in cybersecurity vis a vis management? What can management do to help the board better understand their cybersecurity program and obtain their help on key areas which require board leadership?

Panelists:

Deborah Guild (CISO, PNC)

Joe Gottlieb (VP Corporate Development, SailPoint)

Brad Hibbert (CTO, BeyondTrust)

Vijay Jajoo (Senior Partner Cyber Practice, KPMG)

Moderator: Mark Weatherford (Senior Partner Cyber Practice, KPMG)

Mark: There are a number of interesting things we will be discussing today. Regarding security in the boardroom, as someone who has briefed boards for several years, Jim Pflaging' s number of approximately 2/3 of the board not feeling comfortable with responses to cyber issues and related information is accurate, or could even be generous. Those of us in the security community share some of the responsibility for this situation: we have spoken down to our boards in a way that is dismissive of certain technical issues. We need to push past that approach.

Legislators are increasingly concerned with cybersecurity. There are 127 pieces of legislation in the House and Senate that deal with cybersecurity. These possible policy changes can have long term implications. Senate Bill 536, the Disclosure Bill, mandates that every publicly traded company have at least someone on their board with cyber expertise and if the company does not, then at least one person who is advising the company on cybersecurity. It is not yet known whether this particular bill will go forward, but it is important to acknowledge these changes.

Question: What advice do you give to CISOs to get in front of problems to ensure that their companies are secure?

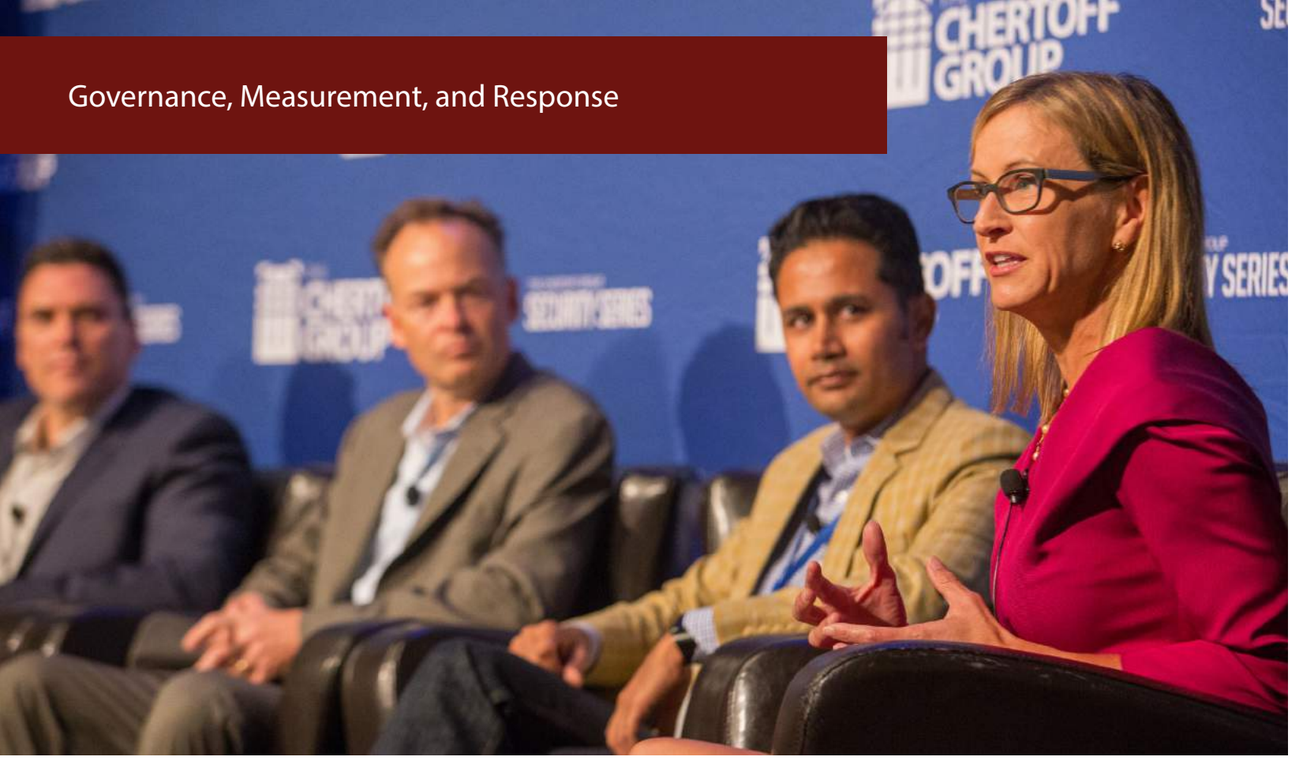
Vijay: I recall a company who had just been breached, but whose CIO was thanked by the board and by Congress. He was being asked to serve as an advisor on a steering committee and task force. This was because although there was a security breach, that specific organization had handled its response to the breach well. The board members were concerned that if a more sophisticated attack had occurred at that time, the company would likely not have been able to stop the attack as it had in this case. We can see that boards are "hungry for data."

Question: What do CISOs do to educate the board in order to stay ahead of breaches?

Deborah: Information is distributed through "cyber dinners" and during board meetings, as well as annual reports in order to not overwhelm the board. In the annual report itself, specific regulations are highlighted. We also compare ourselves to competitors to ensure we are not weak in any specific area.

Question: Moving to the strategic rather than tactical, what are areas that boards need to understand better?

Governance, Measurement, and Response



Joe: This is a difficult question: governance is very difficult. We have to create the opportunity for wisdom and governance at the board level through education. Zooming out and seeing what others are doing, and introduce the concept of security portfolio management. There's been a great trend in response to prevention, governance is another area that is important in terms of who has access to what. One of the biggest areas is training, as many of these attacks start with phishing scams. These are increasingly well engineered, so we must train people how to gauge what is a scam or not, that should be a focal point. For a board, we want to present them with data and progress, not only prevention.

Question: What is the one item you discuss with CISOs to move this conversation back to the board level?

Brad: From an accountability standpoint, the board has to be held accountable. There is a pressure from regulators and business partners that add additional pressure. People need to have a very security driven culture, where the CISO is seen as a partner, as opposed to a technologist or 'necessary evil.' Think about this as a sales and relationship-building message that allows CISOs, vendors, and teams to all speak to each other. You have to understand what the level of communication is you need to talk to. And when you're talking with a CISO, in order to build that relationship with that CISO, you cannot build that once a year….I build my partnerships and trust with the team so when I'm actually in front of the CISO, I have the right message and trust of members of their organization.

Question: As Jim discussed, boards understand many levels and types of risk but not necessarily always security risk. How do you convey this to the board without overwhelming them?

Deborah: I become someone who helps to build trust and ensure I have a seat at the table. A taxonomy breaking down what risks are lower or higher, and bring to them points that are important and require their attention. Stratification of risks is important, and you have to be consistent in your taxonomy.

Vijay: Risk can be subjective and there are qualitative elements. The challenge to practitioners in the industry is that risks may not be communicated, and that you really have to quantify these risks. As practitioners, we should really provide that level of quantified information: that makes all of us better in this space.

Question: Boards are frustrated with budgets that should address security risks- how do you deal with that with your customers?

Vijay: There is a 'cyber fatigue.' Simplification is key in this area. There is something inherently that is important to this simplification: from a risk perspective, these are my crown jewels that are being protected, and do not surprise the board with ah-ha moments, that does not help. Provide context for what is being improved, control the conversation, and stay ahead of the game.

Question: The landscape is literally littered with companies that are providing security tools that provide solutions to everything. How do you work with CISOs and security teams to work with the vendor community to drive better security and accountability?

Brad: You have vendors in place today, and one of the challenges is proving ROIs on these tools. There are a few things to look at: how do you maximize the effectiveness of a product, and ensure it is being used in the right way? As you build a more strategic relationship with your vendor, vendors that you have selected will also change. What are the use cases you'll need to support next year, and can the current vendor actually serve those needs? You either end up with security teams that have some choices or you miss the deliverable, which isn't good. You can move ahead and buy another product to solve that specific use case, which isn't practical over time. When you're out there and you're talking with the board and you have that relationship with the board that I discussed earlier, where you understand the products and services you're trying to get out, and then you can talk to your vendors about how you're going to support use cases, that will allow you to decide if those investments you've already made can solve it, or whether or not you have to extend to some other products.

Joe: Yes, the practice of 'actively pruning' is important. The more you have, the harder it is to know whether you're achieving your goals here or not.

Question: We have established there are varied levels of 'cyber IQ' on boards. What do you do to educate your board?

Deborah: I do feel like that's my job- I try to explain things in terms and methods that meet them where they are. I have two focus areas: they are around identity, and confidently being able to distinguish between customers and criminals. If this is done right, there's less cleanup. Secondly, there is data devaluation. Almost everything I talk about with my board falls into these two areas: I do not get into technicalities, and it becomes clear. We connect those dots and make sure these are educational moments in time for the board to provide me with feedback and make sure we are on the right track.

Artificial Intelligence and Security

Executives are increasingly turning to artificial intelligence (AI) security solutions to protect their organizations and fight a growing cyber threat landscape. What is the current national security threat environment and where are the USG's priorities? Where are the investments being made by the government in private industry and what are the differentiators to the investment community? Hear from experts across government, industry, and the venture community on the state of the current and emerging technology.

Panelists:

Walid Ali (Sr. Director AI & Cloud Solutions, Intel AI Products Group)

Sriram Chandrasekar (Co-Head, AI Investments, Point72 Ventures)

Melissa Flagg (Fmr. Deputy Assistant Secretary of Defense for Research. DoD)

Bob Griffin (Chief Executive Officer, Ayasdi)

Moderator: Reggie Brothers (Principal, The Chertoff Group)

Reggie: AI has applications across all industry verticals, and goes back to the year 1308 to its first known reference. Big data is one of the main driving factors in AI, especially narrow AI. Because the space of AI is so large, we are going to focus on national defense and national security.

Question: What does DOD think about AI? What are some of the future challenges?

Melissa: Innovation and acquisition are not the same thing. AI is not necessarily the end result: it is in some cases still research, which is sometimes forgotten. We need to be clear on where we should be partners on prototyping, and where we know that a certain technology will be applicable and reliable in its application.

Question: How do you trust your machines in machine learning (ML)?

Bob: Any machine intelligence has to be able to do several things: firstly, discovery. This means understanding data, either supervised or unsupervised: they may have to teach it in some fashion, but the machine does it on its own. Secondly, it must have some prediction capabilities. Thirdly is justification: it is not just about the algorithm, but why it does what it does. It also needs to be able to act on what it has discovered. Lastly, it must be episodic: learn from events around it to discover new things. The reason Ayasdi has taken an application approach is because all applications will have to become intelligent or they will become irrelevant over time. This ensures that an application isn't being force-fed into trying to solve a problem that doesn't really work.

Question: How do you deal with some of the learning issues around the ML revolution?

Walid: With AI, unlike prior life cycles where you couldn't incur a decent ROI until a specific tipping point is reached, ML is different. Even if your data is incomplete, you can target a specific usage case with a specific class of users, and contribute a value-add to that specific case. This is a part of the challenge we are facing: it is hard to know what space to carve out as your own and ensure that products do not fail.

"It is extremely important to think of this new wave of technology as a compounded path: it will mature in multiple locations."

– BOB GRIFFIN

How do you know what the kinds of applications that companies may be building and VCs investing in- how is this conversation happening?

Walid: It is like non-supervised learning. You must be able to understand the gaps in your technology and hedge against them, with a specific degree of fidelity. How can you map out all of this projecting out five to ten years to absorb all of these shocks. That is why it is extremely important to understand the similarities between various industries, but what is essential is understanding the differences.

Question: How do new strategies that aren't necessarily coming from the top-down, but with bottom-up solutions approach relate to business models?

Sriram: It is going well. Security is a huge opportunity for investment. Today's young people want to work on interesting problems: this is a space where there are many interesting problems. Fundamentally, you cannot start working on a problem unless you understand it. Those individuals at senior levels of government may have certain insights, but it is the "real worker experience" that you need to fully understand that problem and know what to build.

"Not understanding the problem makes that gap a very broad one, between the people who have the right technologies and expertise to build solutions, and the solutions that are needed."

– SRIRAM CHANDRASEKAR

Question: So how are you finding the problem?

Bob: There is no 'want' for problem opportunities. In the area of healthcare, we would get a development license to researchers and let them tackle their toughest problems. We looked at 40 year old data on Type II Diabetes: through the use of our capabilities, we were able to very quickly categorize. We were able to sub-categorize that data around Type II Diabetes that unlocked incredible insights. If someone falls into a certain category, they are more likely or less likely to develop other diseases. We are able to do that because we use topological data analysis: all data has shape to it, and that shape is relevant. Analysis is easier with data that is regularly shaped, but is difficult to unlock all of the insights when data is flared, for example. That is what I think is going to advance AI in the future.

Question: What do you think can and cannot be currently done with AI?

Walid: With AI, before we start thinking of building products, understanding the underlying supply chain of where the data is, understanding the wealth of data will govern your success and deliver value at the end. How to manage these multi-focal points in data, in reality, your underlying platform has to be able to adapt to new patterns of data processing. This is the challenge of hardware manufacturers.

Bob: That is an incredibly important point about data. Everyone will tell you content is king. But I will tell you, access and distribution is King Kong. That is what's going to really change [things].

Sriram: What has made deep learning so powerful is the ability to analyze unstructured data. There are great opportunities to have technology assist human beings making decisions.

Bob: Upscaling folks who may be skilled in one area but whose skills are enhanced by AI is a game changer.

Fireside Chat: The Board's Perspective on Cyber Security: Risk Management & Growth Strategy

In their capacities as CEO, Board Director, and Board Chairman, Steve Daly and Secretary Chertoff live on the front lines of the intersection of security and the boardroom. They shared their perspective on how security has evolved into a top business risk, source of competitive advantage and pillar of growth. Managing risk and creating value through this changing environment has far-reaching impact on culture, people, process, product, governance, and more. How has the boardroom security conversation changed? How does security impact shareholder value and brand? What advice do they have for board members and CEOs or CISOs? Steve and Secretary Chertoff will provide best practices on how security is central to both risk management and value creation programs.

Panelists:

Steve Daly (Chief Executive Officer, Ivanti)

Michael Chertoff (Executive Chairman and Co-Founder, The Chertoff Group)

Moderator: Jim Pflaging (Principal and Technology Sector and Strategy Practice Lead, The Chertoff Group)

Question: Ivanti is a new name, but it's a company that's been around for a long time. Steve, you've led the company on an interesting journey. To start, can you paint the picture for us?

Steve: Ivanti, the name, came about at the beginning of this year. Our DNA goes back to LANDESK. Historically, a part of Intel, the impetus for the LANDESK division was Intel's realization that the cost of owning a desktop was a lot higher than it was for a mainframe or a mini-environment, so reducing the total cost of owning one of these distributed assets was really the goal of LANDESK. We went through several iterations and were spun out of Intel in 2002 as they refocused on their core. Now independent, we pivoted towards the convergence of security and systems management, particularly in the patching area. At the time, patching was really a security function, but started to be done more and more by the IT Ops people. We came out with the first integrated patch suite integrated into a desktop systems management suite. We've since realized that when it comes to security end user computing, there's a fundamentally flawed model – a siloed one. IT teams are forced to stitch together all the technologies and pathways across teams, resulting not only in extra costs, but additional risks. Our vision is to unify IT, particularly when it comes to end user computing, and to bring together the technologies and teams to give us a 360º view of what the end user is trying to do.

Question: Even at break, I'm always at work. I received some real-time feedback: Ask him about Trump. So, Michael, from a security perspective for the Silicon Valley community, what do we make of this? What are the dangers, concerns, and opportunities with administration?

Michael: I thought you would rename the company Ivanka. That would really get you penetration into the federal market.

The administration issued an executive order, written by some folks in the White House and DHS who are pretty experienced in cybersecurity. There's been a discussion to moving the federal government to the cloud and upgrading the general level of security. That's good policy, it's a good strategy. I've heard that song before. It's easy to play the music, but it's really

Fireside Chat: The Board's Perspective on Cyber Security: Risk Management & Growth Strategy

hard to actually make it happen. The key question is, will there be implementation? Will the people that have the actual operational authority in terms of budget, purchasing and implementing have a unified theory, unify the purchasing and implement it?

This administration is willing to be more outside the mold in terms of traditional procurement, on promoting innovation. On the other hand, they get easily distracted at the top. So, is there going to be a focus on implementing the actual strategy or will it wind up getting lost?

In general, both in the cyber and the physical realm, we are going to see an uptick in security threats. There is a lot of anger globally right now. What we've seen electorally, in the US, but also in Europe and in other parts of the world, has been a manifestation of that. This will be reflected in more physical violence and acting out – Charlottesville, Barcelona – and I think you're going to see it online, too. For those of us in the security space, I think we have to raise our game to meet the growing appetite for novel, strategic security tools.

Question: Are there any tools that will be ascending more quickly?

Michael: Machine intelligence. We're collecting more and more data. How do we make use of it without slowing down our existing security procedures? Any sort of physical screening will be a major application. Identity will be a major issue, as well. In Europe, for example, their struggle is not in identifying a person of interest, but in identifying too many folks. There are technologies and tools to help conduct a focused tracking of what targeted individuals are doing online and in the physical world.

Question: Steve, can you talk about how you and your team have successfully implemented your acquisition strategy and how you've woven security into that?

Steve: when you're acquiring a software company, you're really buying the people, that intellectual capital, the expertise in the space. For us, it's about getting some DNA into the company that we don't have already and then doing everything we can to keep that talent. It takes a lot of discipline to do acquisitions. Staying disciplined on what you're going to pay for the company, what you're really getting, strategic fit, product overlap can be really hard. Finally, it's a team sport. We involve the entire executive team in the process early on and make sure it's a complete fit across the business.

Question: Both of you are board members. How has the security conversation at the board-level changed?

Michael: To preface this, I'm unusual in that the boards I'm on are security companies. That's our bread and butter. Bearing that in mind, we now spend more time thinking about risk, particularly cyber risk. If you do work with the government, that's part of your license to do business. The federal acquisition regulations do increasingly require that you and your subs demonstrate a reasonable level of security. More and more, it's not just your own security, but those of your subs and the people connecting to you that you must own too, and you have to be able to certify.

Steve: I've never been on a board that is in a highly regulated industry. However, we are starting to see in sales engagements across industries that we're being asked more and more, show us that you're secure. My experience is that this is an under-appreciated discipline at the board level. Most of the boards I sit on, we don't have regular conversations on it, to be honest. From my perspective as a CEO, if you wait for the board to do this, you're way too late. The reality is that people have become numb. Everyone throws around the phrase, 'it's not if you're going to be breached, but when.' But, then, no one hears about breaches, unless it's a Target, because nobody wants to talk about it and go public with it. So I think there is a lack of awareness of the real risks and it falls on the CEO to make it a priority.

Michael: Let's talk about three areas that boards should think about. One, I've seen boards consider this when they attempt to penetrate new markets. When you're going to China, what will you do for security? When you're going to Africa where the infrastructure isn't particularly secure, you get questions about that. Less frequently, but occasionally we've also heard from boards when they enter a new line of business. If you're in financial services and you're going to do a lot more online, you will be changing your attack surface area. Also, are you prepared with a Plan B if something went down, how would you service the transactions for important customers? Finally, the biggest problem with boards is partly that you get numb to it, but it's partly that you get besieged with so many different problems and products that they throw their hands in the air and pray.

When I talk to boards, the biggest thing I try to do is empower them. Tell them it's not hopeless. Set reasonable expectations. If you do, there's a disciplined way to manage the process and hold people accountable. Then, you'll have confidence, not that you'll never have a problem, but that you'll be able to manage the problem, come back, and be resilient.

Question: What are some of the lessons learns during your internal journey building your security risk program?

Steve: I should have taken this seriously a lot earlier, frankly. When we hired our first CISO, it was one of the best hires we've made. He went out and conducted his first risk assessment. We were horrible. A quarter of our people were clicking on phishing emails, worse than the general public. That's when it started to worry me. We've got a much bigger risk here than I ever thought. But, over the last few years, we've reduced it to low single-digit click through rates because we put the investment and focus into that. My advice is for anybody that doesn't have a CISO, get one and figure out how to fund him. It doesn't take a lot of funding, but it can have a really high impact on the security posture of the company. Then, get him involved. We use our CISO, Phil, in the sales process. He's been a resource for us to show our potential customers that we're serious about security, that we have an expert that can speak the language, to give them confidence about our posture and our investment. He can speak from his domain expertise to say, "here's how I use this product." He can help demonstrate ways to use our product to drive the business, not just as a cost center.

Question: Another question has come in – Ask Secretary Chertoff about tampering in elections. What can or should Silicon Valley do?

Michael: Let's separate out two things. One category is actually affecting databases and voting machines. The other issue is so-called fake news, putting out things that are inaccurate and driving them up the search engine using automated botnets or teams of people clicking to deliberately drive it up. The latter is a complicated set of issues. Germany just passed a law that will fine companies that don't take down hate speech or fake news. For those of us that believe in the First Amendment, it becomes a question of in whose eyes is the news fake. However, there are some things that can be done. You can

prevent impersonation. Without imperiling the First Amendment, you can respond to these automated efforts to influence search engines. This gets trickier around hosting white supremacy sites. Having been a judge, I get nervous about where the line is on that. On the security of the databases themselves, there's some work to be done. We've benefited by the widely distributed way in which we do voting in this country. The bad news is it means you have really uneven security depending on the nature of the particular jurisdiction, down to the county or city level. The good news is it's hard to have one type of problem that affects everybody. To change the outcome of the election, you would have to be very specific about where you made changes. But, here's the real danger. The Russians have been trying to undermine confidence in democracies for the last several years. When the Russians see the Orange Revolution and things going on in Central Europe, they see that as a direct threat to their security. What they want to say to the Republic is that "democracy stinks. You don't want that. The West is full of it." The best way to do that is to undermine the solidarity and confidence people have in their own institutions. So you wouldn't have to actually affect the election, all you have to do is create enough doubt about whether the election results were accurate to create a crisis of confidence. They tried to do this in 2014 in Ukraine. They didn't affect voting machines, but tried to affect the media that were reporting on the vote so that the media would falsely report that a fascist had won the election. Although they knew this would be corrected, they thought they could create uncertainty and disorder. Focusing on how you secure voter registration, voting machines, and reporting results will become a very big topic going forward.

Question: Should government be leading the charge on innovation?

Steve: I think if there's a market need for something I don't know if we need the government to help. Smart people and smart investors will figure out how to capitalize on that opportunity. I think in the case of blockchain there's enough smart people thinking about this. I mean we've been thinking about how it applies to things as mundane as asset management. There's enough opportunity here that we don't need the government to drive it for us. There may be places where it makes sense for government to get involved, but in this case the private sector should lead.

Michael: What government can help with is to create a market to spur initial investment. Look at the development of GPS or The Onion Router. These were driven because there was felt to be a governmental need and a marketplace for it. For the government to play the role effectively, you need to have stability and predictability in what the government's investing in. This comes back to implementation. There's been a lot of talk about government spurring innovation, but talk is cheap, implementation is really hard.

Question: What are some of the regional challenges and opportunities as you guys are making those pivots towards security and the cloud?

Steve: Internationally, The Patriot Act causes folks' head to pop off because they don't want their data available to the US government, same with GDPR out of Europe. They're all trying to get to the same thing – data privacy is important to everyone. So, we jump through a lot of hoops. But, doing so helps us. We're viewed more as a partner. We become separated from the American part of being an American company.

Michael: On the flip-side of that, there's a growing sensitivity about any kind of investment in security that exposes a foreign-owned company to American data. Even if you're doing commercial work only, there is going to be a security issue and a foreign influence issue that you have to manage. The right way to do it is to think through, in advance, how you're going to architect yourself, instead of waiting for objections and trying to backfill.

Under Trump, and it's hard to predict, I think there will be more of a focus on economic nationalism. If you're closing plants in the US, you're going to have

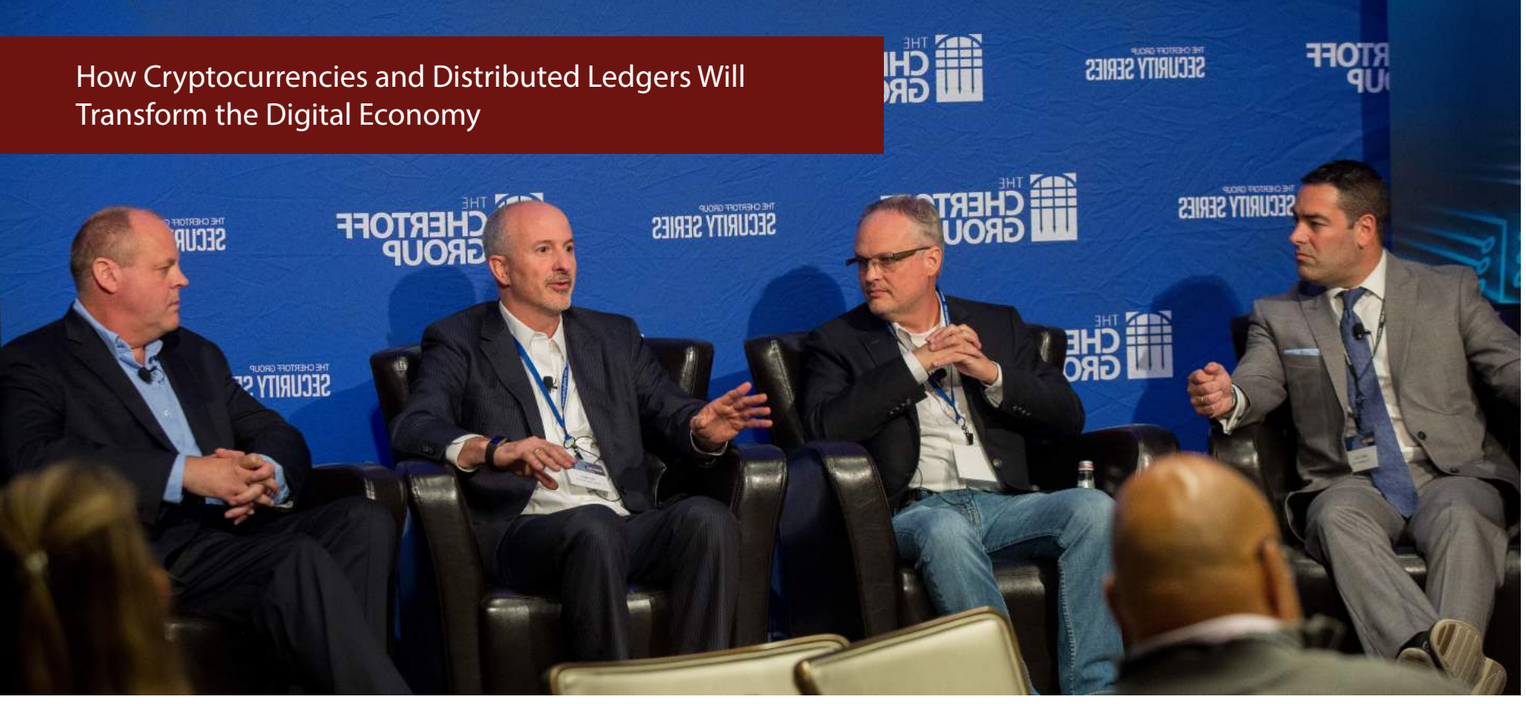
a problem. If I can make the case that I'm going to be investing in creating jobs in the US, the economic departments of this administration may actually be more interested in promoting that. There is an opportunity to turn the issue of jobs in the US on its head and make it a positive.

Question: What are your top 3 recommendations for board members?

Steve: As a CEO, I want my board to know more about it than I do. Have somebody in there that has some expertise and some domain knowledge to be able to help me. Second, focus on the long-term strategy of security. Help me craft it and if you don't know it, get me in touch with someone who does. Our board made the introduction to The Chertoff Group because none of them had experience in security and, frankly, hadn't cared for a long time. Having expertise on the board or being able to connect me with the right people is the most important thing.

Michael: As a board chair, I don't want to overmanage. But I do want to make it clear that security is a priority to our board, that we will invest in it to a reasonable degree, and that we have accountability. It is valuable to get the CISO up to the board to present and walk them through what we've been seeing over the last quarter in terms of nature of attacks, reconnaissance, security trends, how we rank in terms of maturity. It helps the CISO feel like he's being taken seriously and it drives the CISO to make sure that he or she has got a good story to tell. When I was at DHS, I met with President Bush every week to go over the threat matrix. In preparation for the meeting, everybody in the relevant departments – the IC, DHS, FBI – made sure that word went out that we were going to be meeting with the President. It energized people to get stuff done. As a management tool, having someone come in to report to the board with metrics, even if it goes over the board's head, is a good way to motivate folks to do something.

How Cryptocurrencies and Distributed Ledgers Will Transform the Digital Economy



The massive digital transformation of the last several years has turned all companies into digital ones. These new technologies present sophisticated threats, but also afford us new opportunities. One technology that is and will continue to challenge our digital world in profound ways is blockchain.

In the finance sector, $10 billion has been spent on blockchain projects in the last 18 months. Within that sector, there are over 140 blockchain projects underway. Blockchain is real and is disrupting the digital economy right now. We could discuss blockchain in many contexts, but today we focus on educating the boardroom – What is blockchain? What isn't it? What are its realities and challenges? What do you need to know to have a board-level conversation on blockchain?

Panelists:

Rich Baich (Executive Vice President & CISO, Wells Fargo & Company)

Dave Jevans (CEO, CipherTrace)

Mance Harmon (CEO & Co-Founder, Swirlds)

Moderator: Jason Cook (Managing Director, The Chertoff Group)

Question: Let's set the scene with initial perspectives.

Dave: Blockchain began with Bitcoin. This morning, cryptocurrencies hit $150B market cap. The growth rate is 1000%. If this continues for another year, cryptocurrencies would be a $1.5 trillion market, making it the 10th largest economy in the world pushing Canada out of that place. Blockchain fuels ransomware and data extortion of companies, but it also fuels innovation through initial coin offerings which have raised over $2B already this year funding new blockchain projects.

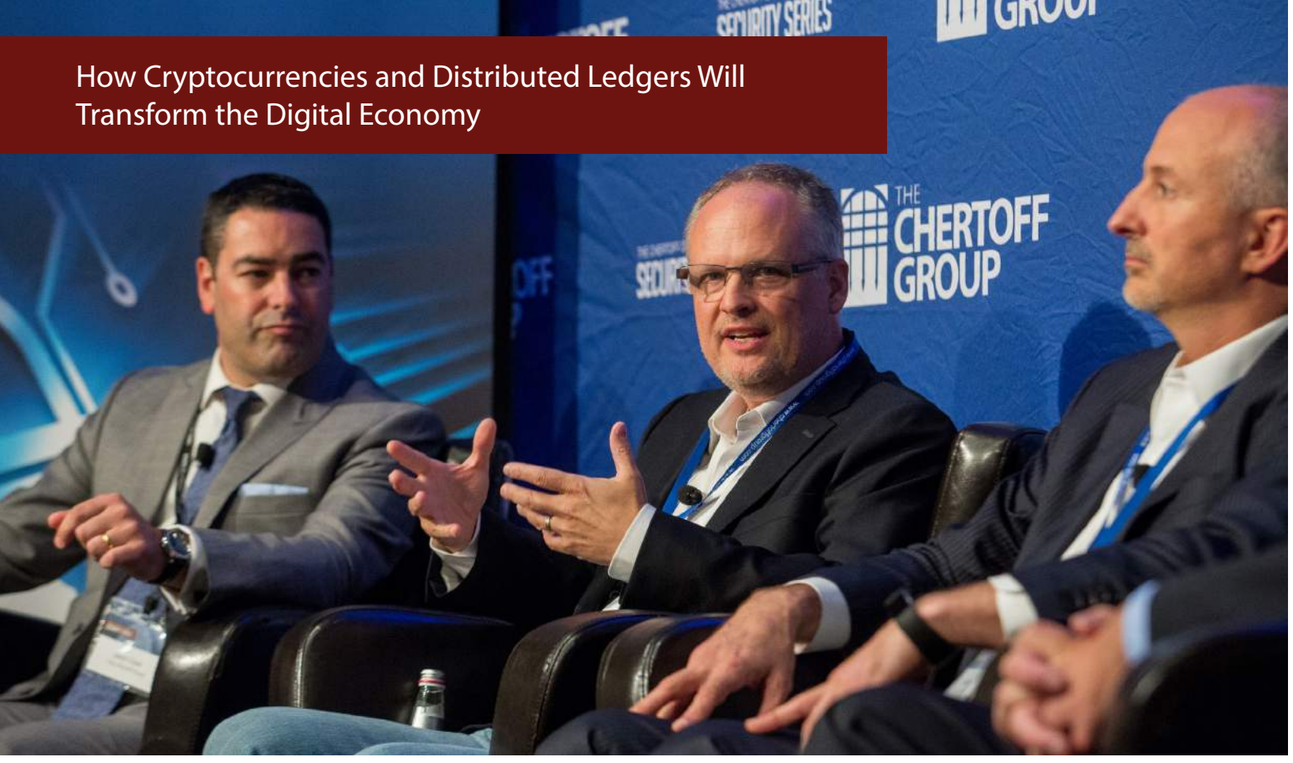
Rich: At the board-level, there are massive misunderstandings of this particular topic. I would encourage you all to take a step back, go to your board and educate them on what cryptocurrency is, what blockchain is, identifying where it's at in its maturation and be ready to talk about potential regulatory infractions. I might even suggest bringing in an outside advisor. Taking the time to educate your board is a very important thing and most boards appreciate it greatly.

Mance: Cryptocurrencies and the public markets are hot right now. There's a lot of press on those. But, ultimately, I think what will be more influential is this trust layer that gets put on top of the existing internet. Every organization would use blockchain or consensus algorithms to run distributed applications connecting these organizations, taking advantage of the improved security model in these technologies.

Question: As an active practitioner Rich, help us separate myth from fact.

Rich: Blockchain offers an innovation opportunity in global payment systems, but right now we see it more in the innovation mode than the execution mode.

Dave: I don't know of any enterprise production blockchain programs that are in real full deployment. Certainly, projects are underway, but I agree with Rich. Right now, it's in the inventing and testing phase. I agree with Mance, too. If we wanted to bring these systems into production and transfer billions or trillions of dollars on blockchain, security will be a massive requirement. For example, today money moves between banks on the SWIFT network. That's a highly



secured network. If we distribute this with blockchain, every bank would have to be as secure as SWIFT. This is an unsolved problem today.

Mance: What is distributed ledger technology? The best way to consider this is in terms of databases. Today, you all know what a database is. Within your organization, you will have a master database and a slave database. You write information to the master and it gets replicated to the slave for disaster recovery. If you had two masters, you'd be writing to the same place at the same time and you'd run into a write conflict. You would have to determine which won wrote first. The community would have to make the decision on which order to write those transactions. The innovation that Bitcoin brought to the market was that it demonstrated that it was possible to take the master out of one organization and give administrative control of that master to a different party. In fact, you can take all the masters and put them under administrative control of different parties in total that are mutually untrusting and they can run a node and do so securely. Security means three things: no single party should be trusted to make decisions; no single party should be able to disrupt the flow of transactions across the community, no DDoS attacks; no single party should be able to unfairly influence the order of the transactions. Cryptocurrency is just one application, of thousands, that runs on blockchain.

Question: Dave, do you agree?

Dave: I agree that there will be thousands of applications … eventually. I would posit that there are other security risks. One that is common to every distributed ledger technology is protection of private encryption keys. If encryption keys are copied or stolen by malware or by an insider, they can effectively become that company.

Dave: The criminals today are in it for money. They will turn their guns towards blockchain. These bad guys, I guarantee you, will move to this area because the opportunity to disrupt at the nation-state level or the opportunity to make money will be massive.

Mance: I agree 100%. That's why I think it's important not to try to use policy or business process to provide protection. What's required is that the math itself provides the protection. Make it not possible to execute entire categories of attacks.

Question: What advice would you give to take back to the boardroom?

Rich: Step one is education in a baseline understanding. Step two is a reality check of where it is at in the ecosystem. Step three is understanding the risks that's associated with it. Highlight which risks can be mitigated and which are outstanding. From the board perspective, before you wade into this, you'd want to understand all these facets because of the inherent and residual risks associated with this.

Dave: There are many innovation groups out there focused on blockchain that have great solutions but no problem. You have to determine what the value proposition is for your organization or economy.

Question: What do we think about the future of blockchain and cryptocurrencies?

Mance: Public blockchain networks are the wild west. There is little regulation nor governance. I think the community will mature. I predict a governing or regulating body, like the Fed for cryptocurrency, will emerge. The SEC will get involved.

Dave: There are two constants in cryptocurrency – change and growth. Change has been a constant since the beginning as has astronomical growth in valuation and in use cases. Here, I'll give you an enterprise use case that's real – intergovernmental payments. If you wanted to do a military procurement or transfer money between funding agencies, that is at least 12 steps as it stands. It's a nightmare, it's slow, it's a massive overhead. Now, distributed ledgers are being used to streamline this to have automation of checking so it's not all done by hand. This is a real project saving real money and because it's a federal program it can be driven with one common governance and one common funding mechanism.

Rich: When you're talking about blockchain, you're really talking about efficiency and effectiveness, reducing workflow checkpoints. In this way, you could say blockchain-like activities have already occurred in the financial space. We've reduced the steps needed to get a loan or loan into your mobile app. Blockchain, stepping back from cryptocurrency, is really an efficiency play. Affiliating blockchain with cryptocurrency as if they're synonyms causes the biggest confusion in the industry.

Mance: When we think about blockchain five years down the line, we should think about the generations. The first generation was Bitcoin. The second generation was that ledger that was used to record those transactions can actually be used to record ownership rights of other things – general purpose ledger services. Third generation was putting complex agreements that govern when we transfer ownership rights of things on top of those ledger services. That was Ethereum. Bitcoin addressed generations one and two. Ethereum and smart contracts were three. The next phase, the fourth generation, is distributed markets. To do this, we need an evolution of the technology. The Bitcoin nor the Ethereum code base can do this. This will help IoT unlock its full potential. When things need to engage in commerce with other things.

Dave: Smart contracts are prone to security problems. There have been hundreds of millions of dollars stolen in the last six months due to bugs in the contract's code. Security will be of the utmost importance, not just in operational security or cryptographic security, but in the code that's written. Also, cryptocurrency will affect enterprise security. All ransomware is powered by bitcoin. WannaCry is not commercially motivated. It's motivated by other reasons. But, dark web marketplaces sell your data through cryptocurrency, it's how they monetize that theft of your data. All of that ability brings more of a criminal element that targets our enterprises and our data.

Spotlight: In Search of the Warrior Spirit Richard Strozzi – Founder & Co-Director of Methodology, Strozzi Institute

Who are the people behind the technology, behind the arms?

As both a psychologist and martial artist, Strozzi approaches threat from a different angle – the people. Who are the people behind the technology, behind the arms? Strozzi channels Aristotle to remind us that “you are the product of your practices.” in this dynamic and volatile environment, you must ask yourself: are our people, our leaders and our management training and practicing in the right way to move most skillfully along our desired path?

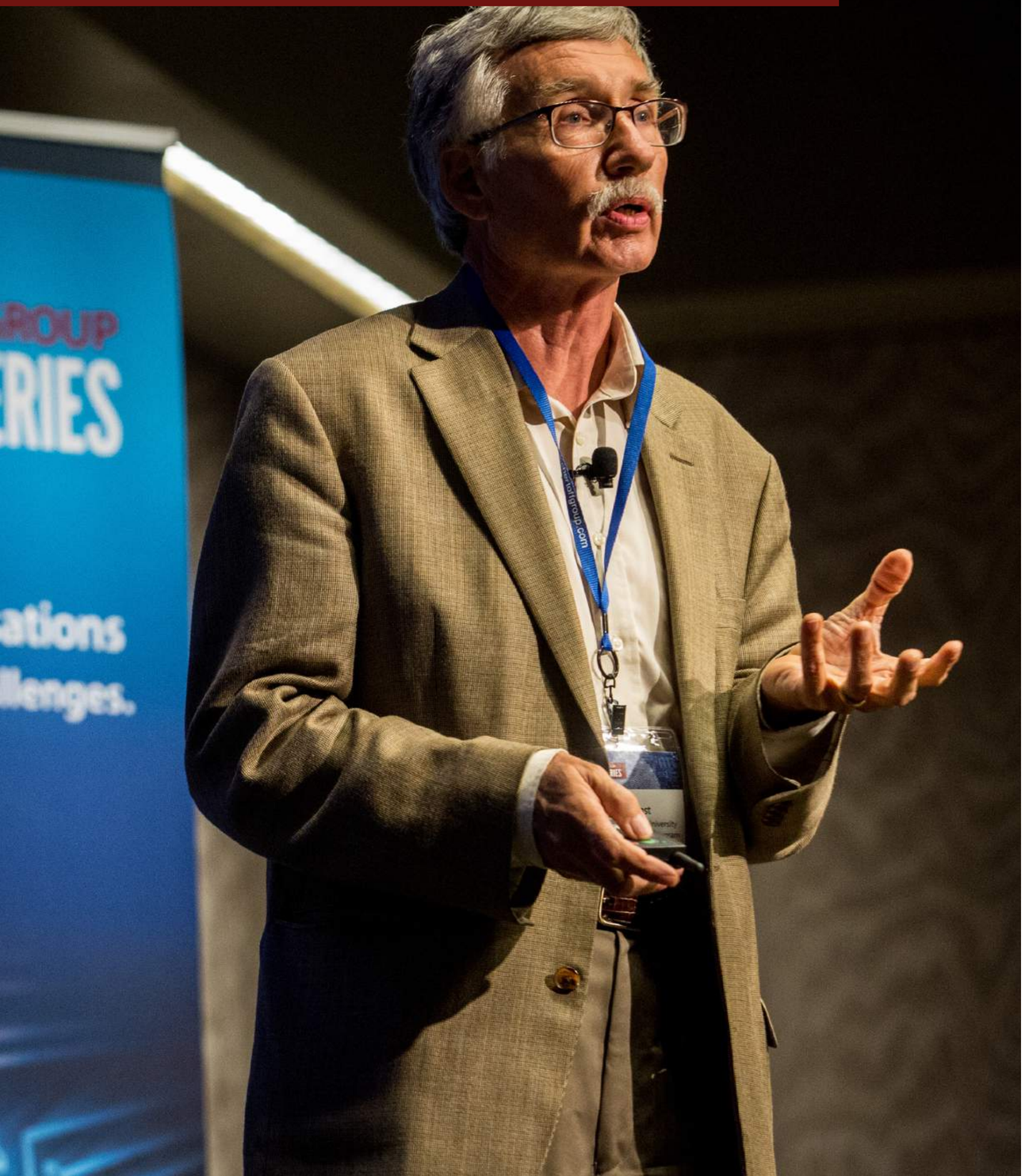
Strozzi’s knowledge of neuroscience and aikido taught him that we can train our attention. People that are successful and fulfilled train their attention to focus and concentrate in the midst of real or perceived threats and distractions pulling them in different ways. To navigate tricky or dangerous situations, you must train, as martial artists call it, to come back to center.

Two stories best illustrate this. Lt. Phillip Duncan, a student of Strozzi’s, was leading his platoon through the rough neighborhoods of Fallujah. Lt. Duncan and his comrades happen upon a funeral procession. The crowd, angered by the presence of an occupying force at this occasion, swells, begins to yell and wave sticks. Quickly, the somber gathering becomes belligerent and armed. Lt. Duncan orders his men to take a knee, remove their helmets and bow their heads. This counterintuitive decision neutralized the aggression and averted the conflict. For the rest of his deployment, Lt. Duncan’s platoon experienced a minimal amount of violence and conflict.

Nancy Hudson, SVP at Pfizer and head of R&D department, worked with Strozzi to prepare procedures and protocols in the event of a chemical plant explosion. Instead of simply reviewing documents in an office, they practiced the actions and conducted walkthroughs. Two weeks later, the scenario they had prepared for occurred. Hudson executed their response plan with calmness and assuredness, minimizing both human and structural damage.

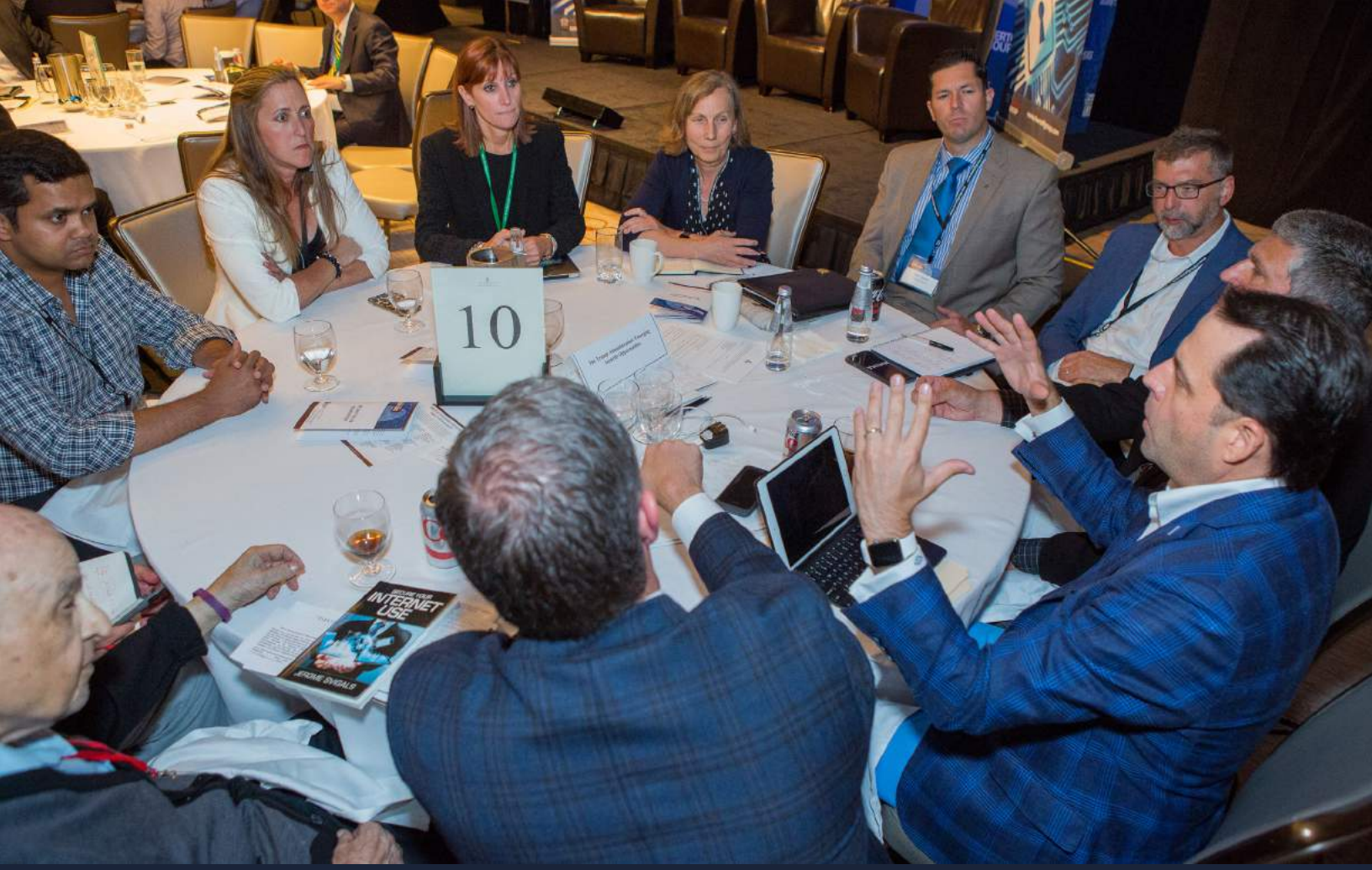
Neuroscience has taught us that when we’re under pressure or threat, we don’t rise to our level of expectation or desire. We precipitate to our level of training. Through repetition and discipline, even in the most trying of times, you can come back to center. This is more than an idea; it’s a way of being. Training to recognize and to manage your tendencies and emotions under duress will enable you to act with choice in times of crisis. A moment of clarity to bring yourself back to the present. Narrow the moment of hesitation. With a clear mind, you become connected to what you care about – your commitment to your stakeholders, your ethics, your long-term strategy. Come back to center.

Spotlight: Perspectives on Borders, Walls, and Opportunities for Mutual Aid, Commerce, and Security Eric Frost, Director, Homeland Security Graduate Program, San Diego State University



A fieldtrip to the wall

Identity is of extraordinary importance in the boardroom: the protection of information and prevention of breaches can allow companies to prevent the loss of both invaluable information and revenue. Eric Frost demonstrates this concept via a “fieldtrip to the wall” as an important analogy to the broad range of security issues that board members face. If officials only focus on patching up small holes within the wall along a border, they will likely miss the bigger picture of securing the wall in its entirety that ranges from issues related to monetary damages, security breaches, and inefficiencies. Within the Department of Homeland Security, one of the major components of analytical work is analyzing massive amounts of data while linking the physical realities to cyber. This was particularly relevant along the California-Mexico, as Frost explains. When information comes across a border, it is important to protect the identity of the individual, and the same applies to the cyber realm as well. There are many components that come into play with physical borders, such as relationships, infrastructure, trade, and transactions across a line. Officials on both sides of a fence each want to solve problems of how to process enormous amounts of data in a productive way. Boardrooms face analogous issues, and thus offers opportunities for great reward. It is essential for board members to notice any gaps in security, and remedy them as soon as possible to protect the crown jewels of their respective company. The importance of a board changing its focus to cover a broader range of issues will be helpful in the long term, and help prevent any breaches to the company’s networks.



MENLO PARK
68 Willow Road
Menlo Park, CA 94025
650-294-4821

NEW YORK
183 Madison Avenue,
Suite 903,
New York, NY 10016
646-289-6840

WASHINGTON, DC
1399 New York Ave, NW
Suite 900
Washington, DC 20005
202-552-5280

www.chertoffgroup.com