FEATS OF STRENGTH

THE YEAR OF ACTION AND EXECUTION

MARCH 2016

WWW.KLOGIXSECURITY.COM

888.731.2314

K logix

Earning the right to be confident
in Information Security

FEATS OF STRENGTH

MARCH 2016

PROFILES IN CONFIDENCE

6 Vanessa Pegueros, CISO, DocuSign

8 Ken Patterson, CISO, Harvard Pilgrim Health Care

14 Kevin Hamel, CISO, COCC

20 Jenna McAuley, CISO, Mercer

FEATURES

3 The CEO’s Year of Action & Execution

5 Q & A with CEOs

10 Sponsored Profile: Malcolm Harkins

12 All for One, One for All

16 Data Protection Programs

17 Sponsored Profile: Josh Douglas

18 Explore Before you Exploit

22 Addressing Risk with Frameworks

LETTER FROM KEVIN WEST

CEO

THE CISO'S YEAR OF ACTION AND EXECUTION

Get Your CEO to Vouch for Security by Executing on Business Goals

In our last issue of *Feats of Strength* we spoke about Outliers. We took Malcolm Gladwell's book about the attributes of innovative and impactful people and applied it to our industry to identify the traits required to be successful in Information Security. To borrow briefly from Gladwell again, it seems we have collectively reached a Tipping Point in 2016. Gladwell defines a Tipping Point as "the moment of critical mass, the threshold, the boiling point." We believe that in 2016 CISOs will reach the threshold of business impact. This is the year of action and execution for our industry.

Over the course of more than fifty interviews with CISOs, we learned that most have been in their role for an average of 16 months. Michael Newborn, CISO at Bloomberg BNA and a *Feats of Strength* Editorial Board advisor, states this is when people in any role, in any profession, reach peak confidence levels. Newborn says, "A typical trend for any employee is that in the first six months of a new role you assess and observe, over the next 12 months you plan, by 18 months you gain confidence to execute and make a real impact." Many CISOs are hitting their confidence and performance sweet spot right now, which is why this year has the potential to dramatically evolve information security's role in business.

ALIGN WITH THE CEO AND C-SUITE, AND UNDERSTAND THEIR PRIORITIES

We have had many discussions with CISOs about participating in Boardroom conversations. Many deem it a critical element to program success. Just as important though, and possibly a better starting point, is the CISO's relationship to the CEO. CISOs who align efforts closely with their CEO gain more than an ally; these CISOs now have someone to vouch for security across the company.

According to a KPMG survey, in 2016 CEOs are focusing on efficient growth and leveraging innovation to keep competitors and disruptors at bay. But the survey makes clear that the CEO's biggest concerns remain financial performance, followed closely by risk management. To gain attention and influence with the CEO, it is imperative to align with their priorities. CISOs help the CEO be successful by identifying and explaining risks that can impact innovation and revenue. With this focus, CISOs can avoid compartmentalizing risk as a business function.

To make an impact on the business this year, CISOs will focus efforts and interactions with the CEO, CFO, and other C-suite leaders around these core priorities – impacting financial goals, understanding and mitigating risk, and enabling efficient growth. Christopher Dunning, CSO of Affinion Group and another *Feats of Strength* Editorial Board advisor says, "For me, this year is really about business enablement. Our Executive Vice President of Sales needs me to participate in sales calls. Security is at the center of business visibility, decisions, and our focus as a company." Another *Feats of Strength* Editorial Board Advisor, Hussein Syed, CISO at Barnabas Health, says that his CEO is focused on managing risks to their brand reputation and mitigating financial losses.

HOW TO EXECUTE ON CEO PRIORITIES

Focus on the Risks That Impact the CEO's Priorities

CISOs that establish strong relationships with CEOs and CFOs approach risk management as an opportunity to educate and prioritize, rather than a reporting function. "On a quarterly basis, we perform a risk register across the whole organization. While all the data is there, this tends to be a dialogue, more than a report. I speak to the highlights that most impact financial performance and our CEO asks questions and we have a discussion," said Dunning.

Maximize Business Efficiencies

CISOs that align with CEO priorities put a focus on business operations that most dramatically impact revenue, to ensure that risks to continued growth are understood and addressed in a manner that supports new technologies and processes that will continue to improve efficiencies. By engaging business leaders early in the roll out of new service offerings or applications instead of at the tail end of a roll out, CISOs collaborate on business solutions, instead of constraining them.

AN EVOLUTION TAKES SHAPE, CEOS VOUCH FOR SECURITY AS A BUSINESS ENABLER

Kevin Hamel, the CISO of COCC, a financial services organization, is featured in this issue. For his company, security and compliance is a top strategic priority. In his profile, Hamel states, "Our CEO is one of the most vocal supporters of security and risk management as a top priority. It is absolutely true that the security mindset has to start from the top. It makes it easy to get security ingrained in corporate culture when the CEO and the Board are the most committed to the effort."

Many CISOs are not in Hamel's situation. Many CEOs have seen security as something they have to do for operational and regulatory reasons. CEOs have a fiduciary responsibility to safeguard the company, its data and protect shareholder value, and the security program helps them check those boxes. But as CISOs take action this year to evolve security from a position of compelled response to a strategic business enabler, the CEO's commitment to security will evolve as well.

Therefore, the CEO will also come to a security Tipping Point this year. The CEO's Tipping Point will be spurred by CISO actions. As CEOs realize the impact security can have on risk management, enabling business productivity and protecting revenue, they will evolve to become security's sponsors, vouching for the value of security initiatives and its strategic impact. We are excited to work with and support CISOs as they execute in this very big year.

KEVIN WEST is the founder and CEO of K logix, a leading information security company based in Brookline, MA.
K logix helps create confident information security programs that align with business objectives.

CEO Q & A

WHAT DOES INFORMATION SECURITY MEAN TO YOU?

THE TIME FOR ACTION IS NOW AND WE HAVE BEGUN TO ENCOUNTER CEOS WHO NOT ONLY UNDERSTAND THE NEED FOR INFORMATION SECURITY, BUT INTEGRATE IT AS AN IMPERATIVE BUSINESS DRIVER.

"Our customers trust us with their most important, often mission-critical business documents and transactions every day," said Keith Krach, Chairman and CEO, DocuSign. "Security is key to The DocuSign Global Trust Network and our customers tell us it is one of several key differentiators for us in the marketplace. I view myself as personally accountable for security and work to ensure that our Security team has the resources they need to earn our customers' trust everyday, for every transaction."

Keith Krach
CEO & Chairman
DocuSign

Rich Leone
CEO
COCC

"We recognize that our continued growth and success depends on COCC acting with integrity and protecting the information our clients entrusted to us. That's why security and regulatory compliance is our top priority as a company."

IN A RECENT STUDY*:

- **ON AVERAGE, IT SECURITY JUMPED FROM**

  8TH TO 4TH

  PLACE IN CEO'S TOP 10 PRIORITIES

- **BOARD MEMBERS HOLD**

  THE CEO

  PRIMARILY RESPONSBILE FOR CYBERSECURITY

- **CYBERSECURITY WAS ON THE AGENDA FOR**

  80%

  OF CORPORATE BOARDS

*2015 State of the CIO Research

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

VANESSA PEGUEROS
CISO, DOCUSIGN

HEADQUARTERS: San Francisco, CA
EMPLOYEES: 1,500
ANNUAL REVENUE: Undisclosed

TRUST - THE COMMON DENOMINATOR IN BUSINESS & SECURITY SUCCESS

Two and a half years ago Vanessa Pegueros took her background in security and technology in the banking and telecom industries to the rapidly growing eSignature software and Digital Transaction Management company, DocuSign, Inc. Pegueros was drawn to the CISO role at DocuSign because the company put a priority on trust. “Trust is a core principal of the company,” said Pegueros. “It is critical to the success of DocuSign and it is critical in the success of any security program. So there was great alignment there.” With trust as a priority, Pegueros knew she could build the program she needed to be effective.

Soon after coming on board, Pegueros announced that DocuSign would build out a “bank grade security program”, a measure that took off within the company along with sales and marketing, as customers increasingly expressed interest in understanding DocuSign’s security program and controls. This level of customer interest in her program has enabled Pegueros to carve out a role as a business enabler.

> “Our enterprise customers want to know about security. It is usually among their top three questions.”

Pegueros is often brought into the sales cycle and attends prospect and customer meetings. “Our enterprise customers want to know about security. It is usually among their top three questions. They especially like our leadership in delivering ‘bank grade security’,” she said.

In the time Pegueros has been at DocuSign, the company has tripled in size, from 500 to 1,500 employees. The security team has expanded from two to 20 people. Security has become a competitive advantage for the company, but Pegueros is quick to point out that more can always be done in this regard. “I continue to emphasize the impact security can have with our product teams. Security is one of a handful of key areas where we can truly differentiate [from competitors] so that DocuSign is the only company and platform within the customer's consideration set." In 2016, Pegueros will work to further advance the idea that security is not a check box item, but that it must continue to be integrated overall to positively impact performance, revenue, and business goals.

TACKLING THE HARD CHALLENGES

DocuSign is experiencing tremendous growth, and the security industry is evolving at a rapid pace. Pegueros admits that the two can combine to present significant challenges. But, she has a plan in place to tackle those challenges, and has built a trustworthy team capable of meeting them.

Pegueros reminds her team that accepting risk is okay. "Security teams need to be more business-focused and not get emotional. Maybe the risk is high, but it is not the security team's decision to make. Our role is to highlight the risk and ensure people have the facts and analysis to understand both the impact and likelihood of fruition for any given risk. For example, we might be 80% sure that an incident will happen in the next five years, but can't pinpoint exactly when. Representing risk to the board is the most difficult thing because it is not science." Pegueros believes the industry could be better served by more sharing of data. This would make understanding probabilities and presenting risk much easier. "In insurance they can give you a great understanding of risk. If you are 60-year-old man who smokes they can tell you exactly how likely you are to get heart disease. We don't have that level of analytics in security. In our industry, companies do not share any more information about breaches and incidents than is required by regulations." What is the right level of information sharing? Pegueros is asking that question of her peers and her team.

Prioritization is another challenge for Pegueros. She focuses on security projects related to revenue-impacting programs first in order to align with business goals. Non-revenue impacting programs are prioritized based on risk. To implement security effectively, Pegueros partners with other business leaders. In many ways this collaboration is made easier because Pegueros reports into the General Counsel through the Chief Risk Officer, instead of the CIO or COO.

Her team previously reported up through the Chief Operations Officer, which meant it was grouped with other departments who had different needs and priorities. It made it harder to get things done. Now as a part of the Risk Organization, reporting to the General Counsel, Pegueros partners with business units. Since the move, Pegueros reports, "My relationship has improved with many in operations because now we are allies. Now we can go to the Board as a consolidated team. I am able to help teams get the resources they need to focus on security from within their organizations." As a result, Pegueros has stronger partners and access to dedicated security resources in other departments.

THE CISO'S OBLIGATION TO THINK STRATEGICALLY

Her other challenge for 2016 is to advance her team strategically. She is asking herself, "How do I build up the thinking capacity of my team?"

Pegueros says, "At this point, tools are an afterthought. How do I get ahead of [risks]? For example, I am thinking quite a bit about incident response. How do we build the resiliency in our team around incident response? If a team is well prepared then they will not be shocked when [an incident occurs]. This does not mean doing a few practice exercises. We need to make response second nature, so that we can react very quickly." She is working to make incident response less of a process and more of a reflex.

"My team has tactical priorities. They are focused on the steady things we have to do. As CISO I have to build out our broader capabilities and address what is missing. The CISO's obligation is to think strategically, and the need for strategic leadership is greater than ever. It has to be our priority."

CEO SUPPORT

"Our chairman and CEO Keith Krach is one of my team's biggest supporters. Security is a top priority for Keith and he ensures we have the time, attention and resources for success. We meet regularly where I brief him on the latest on our security program and efforts, as well as more broadly on best practices and threats across the industry. He helps ensure that security remains a top priority for every employee at DocuSign."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

KEN PATTERSON
CISO, HARVARD PILGRIM HEALTH CARE

HEADQUARTERS: Wellesley, Massachusetts

EMPLOYEES: 1,400 employees; 2,900 workforce

ANNUAL REVENUE: $2.5 Billion

> "We have seen many examples of data breaches occurring at other companies, especially those in health care. We know, as hard as we try to prevent a data breach, if someone wants us bad enough, they will most likely get us. To this end, we make every effort to be prepared to ensure we continue to earn the trust of our members. To me, that's what it is all about."
>
> **- KEN PATTERSON**

TRUST - THE COMMON DENOMINATOR IN BUSINESS & SECURITY SUCCESS

At Harvard Pilgrim Health Care since 2000, and CISO during that time, Ken Patterson has the benefit of historical knowledge and years of reputation and relationship building to help advance the company's security program. During his tenure, his ability to align security imperatives with business goals through risk management has resulted in strong support for the security program within the organization. He says, "Since I began working at Harvard Pilgrim in June 2000, my security staff has grown from one person to seven people, with additional support from co-ops and summer hires. The executive leadership is aware that healthcare is a highly regulated industry and compliance initiatives must be met, as well as protecting against a major data breach. As a not-for-profit healthcare organization, the privacy and security of our members' sensitive information is a part of our culture, and continuously reinforced through the privacy and security training of our entire workforce, including our employees, contractors, consultants and temporary personnel."

EXCEEDING STANDARDS

Harvard Pilgrim recently completed its five-year IT strategy in which security played a major role. Patterson is now focused on a three-to-five year roadmap at Harvard Pilgrim. To accomplish these goals, Patterson starts with ensuring he is fully integrated into the business mission, goals, and approach. "We have a top down push of our objectives; our CEO pushes down to our CIO, and she pushes these goals down to

her direct reports. We all try to understand how we can align with those performance goals," says Patterson.
Patterson has put the work in with his executive-level peers to ensure the program exceeds standards. Patterson says, "Today's CISO needs to be a strong collaborator with all of his or her business units within an organization and needs to integrate their work successfully into the fabric of the enterprise. To help the business make optimal risk-based security decisions, the CISO must have a solid understanding of how the business operates. Leadership, collaboration, communication, and the ability to establish and nurture effective relationships are required for today's CISO to be successful."

UNDERSTANDING CORPORATE GOALS

Patterson says, "The mission of Harvard Pilgrim is to improve the quality and value of healthcare for the people and communities we serve." The Harvard Pilgrim Corporate Business Strategy is:

- INNOVATE - Grow membership in selected market segments by using pragmatic innovations in product and network design, provider partnerships and payment models, and customer decision-support and wellness programs.

- DIVERSIFY - Continue to diversify by expanding our business geographically and demographically.

- MANAGE COSTS - Strengthen our competitive position through a campaign of disciplined cost management.

Patterson aligns security goals with the mission and organizational goals of the company. Patterson states, "Our security goals are to align risk management, governance, and security programs to business goals; and establish principles that executives and business managers can recognize and support during market segment expansions and new healthcare programs. We listen to business stakeholder needs and engage stakeholders in the planning process. We are focused on improving the ability to react to (and potentially prevent) unforeseen security risks and events."

ADVICE FOR THE NEW CISO

Patterson's career in Information Security dates back to the late 1970s. He stands out as one of the first pioneers in the industry. When speaking about the leadership role of CISOs, he says, "Empowerment comes from experience, if you don't have leadership or communication skills you are not going to make it, those are the skills CISOs need to be effective." He suggests new CISOs should:

- Integrate with the Business - Listen to business executives and understand what they want to get done and be a facilitator - help them get to their goals.

- Increase your Business Acumen – Similar to what others in the industry have recognized, Patterson points out that CISOs are often promoted for their technical background, but it takes a different skill set to be a successful CISO. New CISOs need to master the skill of business communication and place security within the realm of business goals when articulating strategy and advocating for security budget and priorities.

- Work your way up to the board - For many CISOs there are still at least one (and often more) layers of management between them and the Board. CISOs who do not have direct access to the Board should focus on making their case to other executives. Patterson suggests CISOs prove their communication skills and value to CIOs, CEOs, and CFOs to gain access to the Board.

- Be Prepared - Patterson says he meets with his CEO before presenting anything to the Board. This way he is prepared for questions, and he has the support of the CEO in the room.

SECURITY-FOCUSED CULTURE

Patterson and his team work hard to improve privacy and security around compliance with regulations, which has helped instill a security-focused culture. "My executives send me emails concerning recent articles they read about security because it often captures their attention. They understand the importance of being prepared and have helped me advocate this to our entire workforce," says Patterson. Harvard Pilgrim requires security training for all employees, resulting in an organization-wide understanding of the consequences of a breach in terms of financial loss or reputation. "We make good use cases to demonstrate what could happen here and how we build a process to rapidly detect and respond to any incidents that occur. Even if something minor happens, the workforce knows about it," comments Patterson.

> “Listen to business executives and understand what they want to get done and be a facilitator - help them get to their goals.”

Q&A WITH MALCOLM HARKINS

GLOBAL CISO, CYLANCE

> Most of the security industry is focused on profiting from the insecurity of computing - which means they profit at the expense of their customers because they are left reacting to issues and trying to minimize damage.

As Global CISO of Cylance, Malcolm Harkins oversees all aspects of information security and risk, security/privacy policy, and peer outreach to drive improvement across the world to understand cyber risks and best practices to manage and mitigate those risks. A true industry leader, visionary, and driving force behind advancement, Harkins instills his passion with the Cylance team to deliver cutting-edge malware prevention.

Cylance focuses on preventing malware with high efficacy to lower risk in a way that lowers cost and improves the user experience. Harkin's book, *Managing Risk & Information Security*, is subtitled "Protect to Enable," one of the core values of Cylance. "Most of the security industry is focused on profiting from the insecurity of computing - which means they profit at the expense of their customers because they are left reacting to issues and trying to minimize damage. Our core business is focused on preventing issues and truly protecting computing, and if we do that, we make money," said Harkins in a recent interview with Kevin West, CEO of K logix.

The Cylance user experience ties back to three things Harkin's believes are important parts of any security solution:

1. Lowering the risks to people, data, and business
2. Lowering the cost of controls
3. Lowering friction and improving experience and velocity towards business goals

Harkins says, "When I speak with CISOs about how you make a business case for security solutions, you must look at all three of these things. One of them might be good enough to buy a product, but when you achieve all three, it's a 'wow' moment."

Kevin spoke with Malcolm Harkins about leadership, taking action, and experience.

Kevin: We have spent a lot of time focusing on educating CISOs to have executive conversations with CEOs and CFOs. We now believe it is the year of action for CISOs, so what do CEOs and CFOs need to bring to table to make it relevant for the CISO?

Malcolm: It all comes back to understanding the risk by considering what the biggest potential current and future systemic risk issues are. There are three lenses through which people must do this:

1. Risk to the business
2. Risk to the customer
3. Potential risk to society

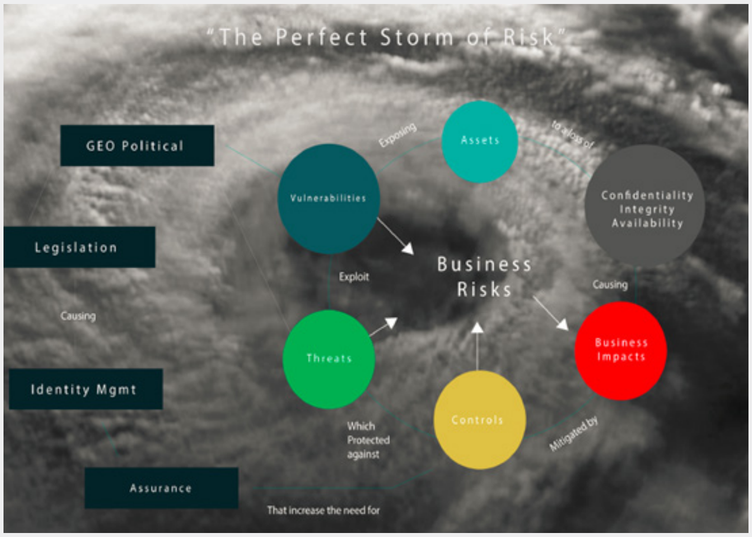
You cannot stay focused on only the risk to the business; you must get to the core and twist the risk issues on these three lenses. Security professionals need to get out of just looking at it from the point of view of a typical IT infrastructure and recognize that even if you are in a brick-and-mortar company, you will eventually become a technology company, or else you will become irrelevant.

Security professionals cannot only focus on specific internally-focused systems, because those may not be part of the technology evolution from a revenue-generation perspective. CISOs need to expand their views and have a very strategic discussion within the context of their organization. This is also something the boards needs to start thinking about from the infrastructure side, product and service side, privacy angle, and link to physical security. They must understand the threading on that Rubik's cube of risk around the information, technology, and how it manifests those risks, as well as the opportunities new technology creates.

Kevin: You spoke at our recent CISO Leadership Summit and shared how CISOs can become great leaders. What is your leadership style and how can others learn from you?

Malcolm: I spent the first decade of my career working in various business roles, from managing credit risk as a call center agent, to running

> One success measure I am proud of is my ability to move the needle on looking to the future for information security. In 2002, I drew “The Perfect Storm of Risk.”
>
> At the time, people thought it was a few-year effort to upgrade security solutions and insert controls. If I look at what I realized when I drew this, I saw an emerging perfect storm of risk and the elements of security, privacy, business continuity, and disaster recovery. I was able to move my company into recognizing what was coming and how to stay on top of it, but I also galvanized what was coming for the security industry. I spoke about these things in business conferences long before many security conferences even existed.
>
> The success factor that really matters the most relates to the people I have touched who have worked for me or indirectly worked for me. Being able to gain their trust and respect, to me, is the biggest success factor. I still speak with many former employees and maintain their trust. I have always pushed myself to align my beliefs with the work I am doing, something that has helped enable my success. This is also my biggest challenge because there are so many dynamics and pressures that swivel, sometimes from externalities and sometimes from people you work with. You must assimilate their values and views, but also make sure you are clear on your own, and I think this is a struggle for most information security professionals.



a customer service team. I was able to experience a wide-range of communication and business challenges that built acumen. I got my technical acumen from working at technology companies in procurement and finance, as well as working in some new business ventures at Intel and more recently as Intel’s Chief Security and Privacy Officer prior to joining Cylance.

I have always had a strong sense of mission and fell in love with the people, issues, and challenges aspects of my work. Because I have done such a wide variety of things, my way of approaching leadership is i hope a bit unique; I am more open to different approaches and a diversity of thinking that helps me lead in my own way. I believe in the three laws of leadership:

1. If you don’t believe in the messenger, you won’t believe the message.
2. You can’t believe in the messenger if you don’t know what the messenger believes.
3. You can’t be the messenger until you’re clear about what you believe.

To go along with these three laws, Colin Powell once wrote, “You have achieved excellence as a leader when people will follow you anywhere if only out of curiosity.” This stuck with me a long time ago because the power of curiosity is not positional or authoritative power, it creates a different kind of leverage.

A quote I believe to be the best definition of leadership is, “Leadership is the art of motivating others to want to struggle for shared aspirations” (Kouzes & Posner, *The Leadership Challenge*). I believe it is important to recognize there is a strength that comes through struggle.

Another aspect of leadership is trust. In order to create trust, you must also be vulnerable and transparent on who you are, what you believe, and why you believe it. In sum, trust is a function of two factors:

1. Competence – Competencies are not only skills. You must have skills and knowledge, but you also have to do something with them to demonstrate competence.

2. Character – You must show how you have integrity, values, and principles.

When you add all of these up, the leaders who have the most influence are the leaders who are closest to us.

FIVE THINGS TO REMEMBER ABOUT LEADERSHIP

1. Leadership is a relationship
2. The best leaders are the best learners
3. Leadership development takes deliberate practice
4. Leadership is an aspiration and a choice
5. Leaders make a difference

*The Leadership Challenge (Kouzes & Posner)

ALL FOR ONE, **ONE FOR ALL**

BY STEPHANIE HADLEY
CONTENT MARKETING MANAGER

Information Security Executives Are Partnering with the Competition to Move the Needle on Security in 2016

One theme resonates consistently across all the CISOs we speak with: networking and information sharing are powering successful security programs. In fact, a PWC survey found that 82% of companies with high-performing security practices collaborate with others to achieve their goals. A similar industry survey reported that 56% of security professionals rely on peers at other companies for information exchange related to threats and security best practices. But what does that mean exactly? In hyper competitive industries like financial services, retail and manufacturing, how do security professionals share and collaborate without losing competitive advantages?

THE FINANCIAL SERVICES INDUSTRY LEADS THE WAY

The Financial Services industry, long the standard-bearer for information security practices, leads the way in terms of formal industry associations and more informal networking. The Financial Services Information Sharing and Analysis Center (FS-ISAC) is the leading center for cyber threat and security incident reporting and sharing. In fact, the Retail Cyber Intelligence Sharing Center recently signed an agreement with FS-ISAC to duplicate FS-ISAC's model and processes for the retail industry.

ISACs serve an important function in helping organizations identify, and more quickly respond, with industry-proven methods to threats and incidents on their own networks. While membership in an ISAC is increasingly becoming standard practice for day-to-day security, other avenues provide the level of sharing and collaboration needed to elevate security teams from "in the trenches" operational programs to revenue-impacting, goal-supporting business.

More impactful than the threat reports and data sharing between financial services companies is the peer-to-peer collaboration among the group. In this issue of Feats of Strength we profile Kevin Hamel, CISO of COCC. Hamel belongs to the CISO Executive Network. Membership provides him with unfettered access to his peers, who are always only a phone call away and ready with solutions or suggestions to address the latest security issue.

The higher education market is also working more collaboratively to address security issues. Deborah Gelch, CIO at Lassell College in Massachusetts says university security officers regularly collaborate via listservs sponsored by higher education associations like Educause. Gelch says, “The Financial Services industry really set the benchmark for effective information sharing, but in education this is our near future. We are often smaller organizations, so we need to be able to leverage each other for expertise and best practices.”

IN A RELATIVELY NEW INDUSTRY, SECURITY LEADERS SET THEIR OWN RULES OF ENGAGEMENTS

According to K logix research, more than half of all CISOs are in the role for the first time. A 2014 survey from PWC showed that only 28% of organizations had a CISO. That means a large number of CISOs are filling roles that previously did not exist. This trend will only continue in 2016 as many more companies add the CISO position.

The relative newness of the role means the position is still being defined. That is likely a big reason CISOs turn to each other for advice and input, more so than other C-suite executives. Another reason is the nature of their business. While sales executives, for example, can easily identify their competitors and create counter-positions to defend against them, CISOs must navigate a maze of foes including cyber threat actors, hacktivists, rogue employees, and standard business risks. In addition, CISOs recognize that a more secure Internet will enable their company to compete more effectively. In a previous feature of Daniel Conroy, CISO of Synchrony Financial, he said, “All financial services organizations need the Internet to be secure because we need consumers and businesses to feel safe about their private data. It is in the best interests of us all to share cyber threat information to maintain a safe and secure Internet experience for all businesses and consumers.” It is no wonder CISOs are far more likely to share openly and honestly with executives at otherwise competitive institutions.

OPPORTUNITIES TO ENGAGE YOUR PEERS

Jenna McAuley, the new CISO at Mercer is also profiled in this issue of the magazine. She picks up her best advice and finds opportunities to mentor and to learn through the Women’s Executive Forum. Hamel says the CISO Executive Network is more valuable than any trade show or industry event. Others, like Conroy, made connections through FS-ISAC that lead to personal relationships. More than 20 Boston-area CISOs participated in K logix’s CISO Summit to share best practices and ideas for elevating security in the board room and aligning security with strategic business goals.

All of these security leaders found associations and organizations that put them in the same room as security executives who shared their common interests – whether similarly sized organizations, in the same industry, or other attributes – and they are able and willing to share security-related information without risk of exposing trade secrets. Robert Duncan, a professor of Cybersecurity at Columbia says that this level of information-sharing happens informally among the largest banks on Wall Street because they each see benefit in the exchange, and they are able to do so without exposing company secrets.

Join the CISO Conversation: K logix *Feats of Strength* CISO Summit NYC

CISOs from diverse industries come together for peer-to-peer networking, brainstorming and to share action plans at the K logix Feats of Strength CISO Security Summits. At the last even in Boston, MA CISOs worked in roundtables to address issues like collaborating with CIOs and other executives, business enablement, finding, hiring and supporting the right talent and security awareness training.

Join the conversation at our next CISO Summit in New York City, on April 28th, 2016.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

KEVIN HAMEL
CISO, COCC

HEADQUARTERS: Southington, CT
EMPLOYEES: 400
ANNUAL REVENUE: Undisclosed

SECURITY: THE NUMBER ONE CORPORATE PRIORITY

Kevin Hamel is not the typical CISO, nor is he in the typical corporate environment. As a 12-year-veteran CISO at COCC, one of the industry's leading suppliers of technology for banks and credit unions, Hamel greatly outpaces the industry average of 16 months in the CISO role. COCC exemplifies one of the few companies in the world that lists security and compliance as the number one corporate priority. In fact, this has been the company's guiding principal for 15 years. Hamel states, "We recognize that security and regulatory compliance are vital to our business. If we have perpetual regulatory problems or a security incident, that would be a real threat to our success. Where other companies in other industries might prioritize profit, market penetration, or shareholder value, our top priority is security and regulatory compliance." Hamel points out that this priority is client-driven. As a cooperative, COCC is owned by its' clients, and CEOs from a select group of clients comprise COCC's Board of Directors.

> "Our CEO is one of the most vocal supporters of security and risk management as a top priority."

CEO PUTS A FOCUS ON THE CUSTOMER

Hamel states, "Our CEO is one of the most vocal supporters of security and risk management as a top priority. It is absolutely true that the security mindset has to start from the top. It makes it easy to get security ingrained in corporate culture when the CEO and the Board are committed to the effort."

Hamel clarifies it is not necessarily a passion for information security specifically that is driving the CEO's attention to the topic, but it is his passion for the company and client satisfaction that dictates the security and regulatory compliance emphasis within COCC. Hamel says of the CEO, "He has been CEO of COCC since 2002, and CFO before that. He is passionate about the company as a whole; the clients, the employees, the work environment, our products, etc. His commitment to customer satisfaction helps him recognize the importance of regulatory compliance and security."

Because COCC's CEO is focused on security, Hamel has a closer working relationship with him than other CISOs might have with their CEOs. In regular conversations, Hamel and the CEO focus on the client base. "COCC is focused on delivering the best service possible. That includes the best and most appropriate security. We talk about what is right for the organization and our clients from a security perspective, just like he talks to the CFO about what's right for the organization and our clients from a financial perspective. We are in constant communication, and the focus is always on delivering the value we are supposed to be delivering to our client base. That keeps us focused on our mission and strategic goals."

Hamel continues, "You might not see us talk specifically about security as a competitive advantage, but I think that's implied and our clients understand it that way. From a customer service perspective, the message to our clients is that we care about the safety and security of the information you have entrusted to us. That is one part of our value offering as a co-op."

Hamel focuses on integrating security into the business at every level, which requires as much business skills as technical and security competency. He says, "As an organization, we are here to provide banking services. We are running a business and you can't be an effective executive if you don't have a solid understanding of your business and general business concepts."

Hamel believes his MBA and business background have been helpful in enabling him to align security with the organization's customer-centric business philosophy and to work more collaboratively with other executives in the company to achieve their goals. He states, "For me, the organizational behavior courses in my MBA program were most beneficial. These courses put a focus on interactions with co-workers, how to build relationships, and how to communicate with people at all levels of the organization."

ADVOCACY LEADS TO ADVANCEMENT

Given the emphasis the company places on security, it is very easy for Hamel's team to align with business goals. After 12 years of advocating for security he is now focused more on guidance. "We spend little time promoting security as a concept or getting people bought in to the idea of security, and more time helping to ensure we make the right security-focused decisions as a company."

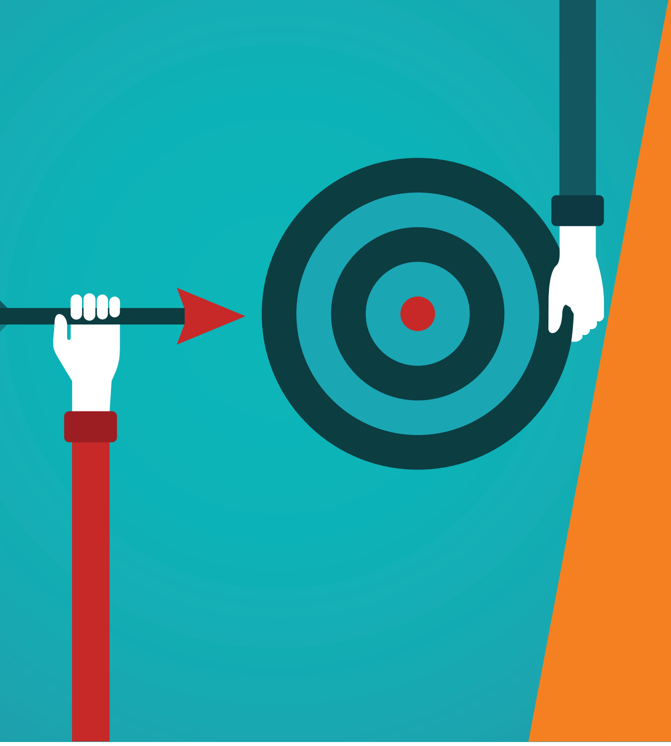
A RESOURCE FOR OTHER BOARDS

While getting time in front of the Board is a challenge for many CISOs, Hamel has significant opportunities to present to his own board, and many others in the financial services industry. As a successful veteran CISO at an organization that emphasizes security to its banking and credit union clients, and as a member of the Massachusetts Banker's Association Cyber Security Task Force, Hamel is often asked to present to the Boards of other financial institutions. "With the release of NIST's Cybersecurity Framework and President Obama's Executive Order on cybersecurity, there is a lot more interest in security at the Board level. In the past year I presented to the Boards of 17 financial institutions. They wanted to learn what they need to do from a cyber security perspective to fulfill their fiduciary duties," said Hamel.

Hamel says, "It is important that Boards recognize cybersecurity is much more than just a technical issue. When there is a cyber incident, your technical teams will be working hard to resolve that issue. In the meantime, what will you be communicating to your customers, your partner, the local media, your Board, etc.? Who will be communicating to those groups? How will you continue to provide your services if your systems are unavailable? There are a multitude of non-technical issues that need to be managed by the organization."

WHERE DOES A VETERAN CISO GO TO LEARN?

While experienced in his industry and considered an expert resource by many, Hamel values education and is constantly seeking new information and knowledge to continue to innovate his security program. While the internet and conferences provide good resources, Hamel says he learns the most in peer-to-peer interactions. Hamel says, "I belong to one organization that I feel is invaluable – the CISO Executive Network. There are ten chapters with one in Boston, one in New York, and hopefully one in Hartford soon. We meet about six times a year. These are closed-door, half-day sessions about specific topics. It is a great chance to learn from other CISOs in your local area. The networking opportunities are phenomenal. I can always pick up the phone and say to a member 'hey what are you doing on this particular topic'?"



K logix Project Advisory Service will Bring Clarity to **Data Protection Programs**

BY KEVIN POUCHE
CHIEF OPERATING OFFICER

PART ONE

REPLICATING OUR ENDPOINT PROJECT ADVISORY SERVICE FOR DATA PROTECTION

K LOGIX PROJECT ADVISORY SERVICE GUIDES INFORMED DECISIONS

Just like K logix did with our Endpoint Security Project Advisory Service, we will bring clarity to the frustrating and cumbersome Data Protection market in the Spring of 2016. **Within our methodical, scientific process we will identify the real data protection issues our clients need to solve and help them build a practical data protection framework. We will help clients cut through the clutter of data protection solutions to make informed decisions that make sense for their specific business.**

In the decade since the technology was first introduced few Data Protection implementations have been successful. In fact, many in the industry refer to Data Loss Prevention (the pre-cursor to Data Protection) as the most expensive shelfware in the security industry's history. The space was still emerging, the technology was positioned inaccurately, and sold to organizations unequipped to effectively support it. Roll-outs failed for a few reasons, namely:

- Security organizations were not prepared or staffed to support a time-intensive solution.
- Most organizations had yet to establish an effective Data Ownership program.
- There was limited understanding of data discovery and classification in the industry, and no holistic data protection strategy.
- The market viewed data protection as a technical challenge instead of a business risk.
- The "prevention" aspects of the solutions were primitive, so instead DLP was a futile exercise in detection.

In April of 2007 all six companies in the Leaders Quadrant of the Gartner Magic Quadrant for DLP were privately-held start-up security companies. Today the Leaders Quadrant consists of mature, publicly held security companies who bought and integrated those 2007 technologies into their eco-system. As we study data protection in 2016 we have important questions to answer. Have the original technologies matured within these large, and well-funded companies? How do we account for current considerations like cloud security, permissions management and unstructured data? How do these new solutions fit into an overall data protection strategy?

For more information about our upcoming Data Protection Project Advisory Service, please contact us.

Q&A WITH JOSH DOUGLAS

CTO, FORCEPOINT

Josh Douglas is currently the CTO of Forcepoint and former CTO of Raytheon | Websense. During his tenure at Raytheon over the last ten years, Douglas oversaw the cyber security intelligence operations, malware concepts, security infrastructure operations and research technologies tasked to produce effective forward-looking cyber software solutions to contain and control advanced threats.

> We are now talking about what matters when a breach does occur, how you reduce the impact to business.

Q) TELL US ABOUT THE RECENT LAUNCH OF FORCEPOINT.

A) We have a new joint venture built on the successful integration of Raytheon Cyber Products, Websense and Stonesoft companies which is now called Forcepoint. Forcepoint brings advanced cyber security technology built within Raytheon to the global market, providing organizations with a unified software platform that defends against attacks, rapidly detects insider and outsider threats while providing today's security professionals the ability to make decisions to limit damage and theft. I see many benefits from Forcepoint, especially when it comes to our customers and employees. We have amazing customers as part of our joint venture, who drive and challenge us to be better as a company. We have industry expertise both from the defense and commercial space which provides a solidified approach to tackling threats affecting us all.

Q) WHAT DOES THE FUTURE OF FORCEPOINT LOOK LIKE?

A) The technology goal of Forcepoint is to create a unified platform that will eliminate the point product fatigue our security teams are facing today while utilizing existing technology enterprises already have in place. By integrating disparate solutions, and applying automation and correlation via analytics to the alerts, the idea is to reduce volume of alerts down to the handful that are actually noteworthy and actionable, focusing on highest risk ones first to save resources and provide return on investment. The Forcepoint platform will produce a common foundation for the protection of users, networks and data. Key focal areas include insider threat protection, cloud data protection, and network security. This year we are introducing the beginning of our analytics platform which will look more into user entity behavior and analytics of our products as well as other products in the market. The benefit is to quickly identify risk, not only based on machine behavior, but also user behavior.

Q) WHAT HAVE BEEN YOUR BIGGEST SUCCESSES?

A) My biggest success was my ability to be a part of the Raytheon team who helped create this Joint Venture, while bringing Raytheon Technology to a larger commercial market. This has included our Threat Protection Appliance, Insider Threat and Analytics. These products help detect and combat advanced internal and external threats in real-time. Working on innovative strategic initiatives like this, are one of the reasons I have stayed at Raytheon for over ten years.

Q) HOW HAVE EXPERIENCES WITH CUSTOMERS INFLUENCED YOUR WORK?

A) I meet with customers often. Some common concerns I hear from small to mid-sized organizations is the lack of staff and a desire for simplicity with an expectation of high efficacy in products. For larger customers, they want simplicity but the challenge is to ensure they have a high level of efficacy. Our products cannot require them to lift, replace, or interoperate with a monolithic security infrastructure designed by one security vendor, we have to work with their practices, policies and existing products.

Many customers talk about budgetary concerns. In my experience the real leveler is when it comes to speaking with the Board on dwell time – containing cyber dwell time is to ensure the hackers have as little time as possible to wreak havoc – and extricate important assets from the organization. People are starting to admit that regardless of what products they have in place, there is going to be a breach of some sort. We are now talking about what matters when a breach does occur, how you reduce the impact to business.

Q) HOW WILL THIS AFFECT THE INDUSTRY, AND CISOs?

A) With the goal of how quickly a CISO can get a business back on its feet, we are now discussing business continuity versus a fear approach with the Board. As we move forward, we are going to see a lot more sharing of information as everyone starts to realize this war can't be won with a single piece of technology. Vendors must become partners as opposed to competitors. At the end of the day, we are all getting targeted, so a community-based approach and a collective sense as product manufacturers, will only help to figure out how to tackle our industry's problems. Not only will this help us, but it will more importantly positively impact our customers and ecosystem we protect.

SECURITY LEADERS NEED TO EXPLORE BEFORE THEY CAN EXPLOIT

By Michael Santarcangelo

Excerpted from an article originally published in CSO Online

"I mean, you can't manage something until you know what you've got. So, before you can exploit, you explore."

That's how Robert Ballard -- best known for discovering the Titanic -- explains his current focus. He is mapping the vast expanse of water that comprises the United States.

Ballard is exploring uncharted waters to inventory and understand how to exploit the value. Much like the modern security leader.

As security leaders, how do we earn our position in the executive suite? How do we ready ourselves for the position?

Many organizations consider security leaders as "security resources with teams."

It's a journey to develop the foundation and competencies necessary to prove leadership. The CISO is a new position in most organizations. With less definition in the position itself, have you earned the recognition as a leader?

Have you earned the right to report to the CEO?

The CISO position is immature

As an industry, we're struggling with the CISO position. We're working to define what it is, required competencies, reporting structure, and the like.

By contrast, consider the still-evolving position of the CIO. In most organizations, the CIO handles the information. In recent years, an expressed interest in security evolved into a top-level concern. Their interest in security is influential on the role of the CISO.

A CIO might delegate security to the CISO so they can focus on enablement and productivity. In the process, does that elevate the position of security? Does the CIO have a responsibility to protect the information? Do they have a natural and vested interest in keeping security under their purview?

The question to consider is whether security plays a broader role than just technology. What about integrating physical security? Where does fraud control fit? Compliance? And as more companies move to the cloud, the importance of governance increases.

Dr. Robert Ballard's visit to Titanic Belfast, 20 March 2014.
Credit: Titanic Belfast

Do you want to be on your own?

The growing importance of security reveals a struggle with vision and business alignment.

Kevin West, CEO of K logix, shared a trait observed in successful CISOs. They "enable the team to execute on the business plan -- with a technical mindset."

Many in security advocate for a leadership role that reports to the CEO. Kevin's research suggests "it's not smart right now for most to separate it out."

Few organizations are ready for a CISO in the executive suite. In reality, few security leaders are ready for it today.

For example, Kevin shared a hospital CISO he worked with that fought to get out of CIO/IT. He cited the direct conflict of interest (familiar approach?). He immediately learned the job got harder, not easier. It forced him to rebuild. He needed to start over.

In my experience, leadership is a journey.

It starts by understanding where we are. As individuals. Within the organization. And as an industry.

With an accurate picture we ask, "what do they

CISOs are Focused on Making an Impact

- CISOs average **16** months in their role
- The majority of CISOs are in their **first** "leadership" role
- **76%** meet with the Board on a regular basis
- **29%** believe they impact business strategy
- **15%** of CISOs report to the CEO
- **80%** value business acumen over technical skills in hiring

need?" Then we have a goal. A direction to progress. That's how we advance from practitioners to leaders. How we earn our spot in the executive suite.

That means security leaders must explore before they exploit

A security leader needs to rank assets and efforts to create value. To protect the right things means knowing what matters. Accurate insights and understanding lead to better decisions.

Security leaders face pressures no other leader in the organization has. Or understands. But they are not alone. The key is mapping opportunities and engaging the right people in the right way.

That's where the advice from Ballard comes into play. Security leaders need to explore before they exploit.

Exploit? Isn't that what our attackers do?

Without a doubt, exploit holds a negative connotation in the security industry. Yet the verb "exploit" means to use a resource completely, in a way that creates the most value.

Start by exploring, discovering, and mapping value to the organization. Start by finding out the answers to three basic questions:

- Where does the company make money?
- How does the company grow?
- What puts our ability to make money and grow in jeopardy?

Security is unique. We gain insights into the corners of the business. We know what got swept under the rug. We learn about what challenges people face.

We also see the brilliance of the organization. The successful programs. The work of people to protect information and advance the business.

We are an untapped conduit to bring people together. Use the exploration as an opportunity to establish trust and credibility with

The good news is organizations realize the growing importance of security. The struggle to understand the role of the security leader creates opportunities. It is time for security practitioners to journey from technical resource to recognized leader.

What can you learn in the next 100 days?

Instead of a call to "think like an attacker," act like a leader. Embark on your own exploration. Learn about your organization and the people that comprise it. Explore how the business works. Identify protections and areas for improvement.

Go a step further. Find out what assets, resources, interests, and talents are available.

Then step back and consider how to best exploit what is available to you to create the most value for the company. Align your energy and efforts with what you discover. All while improving the security and protection of the organization.

One more step on the journey from security practitioner to recognized leader.

How to Take Action and Execute in 2016, Advice from K logix

At K logix we help CISOs develop security programs that explore data, environments and business processes so that organizations can exploit their critical information and practices to maximize their revenue potential.

These strategic security programs go beyond tactical and operational functions to Explore, Advance, and Innovate in order to confidently and positively impact business performance.

EXPLORE
- Identify risks and vulnerabilities to prioritize security efforts around strategic goals
- Discover where data resides, what data is most important, who accesses it, and where it travels
- Analyze data and system performance to add value to business processes

ADVANCE
- Engage with business executives to align security priorities with business goals
- Increase security awareness through regular communication, training and Security Ambassador programs
- In the Boardroom move beyond transactional reports about specific threats to analytical analysis of how security enables growth

INNOVATE
- Leverage new technologies to handle mundane security tasks
- Focus your team's efforts on higher-level analysis of threats and opportunities
- Transform security from an operational focus to a business enabler by creating strategy and response plans that meet business needs

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JENNA MCAULEY
CISO, MERCER

HEADQUARTERS: New York

EMPLOYEES: 20,000+

ANNUAL REVENUE: $4 Billion

Jenna McAuley is eight months into her role as CISO at Mercer, a global consulting leader in talent, health, retirement, and investments. She says, "At Mercer our mission is to advance the health, wealth, and careers of 110 million people. We do that through talent development and learning programs. The mission of Mercer is tightly entwined with my approach to security. I believe in the idea that security is a corporate culture. It needs to be in the fabric of everyone's interactions with clients, customers, and data. So this human-focused approach to security is really just a natural extension of the Mercer mission." She continues, "My biggest objective is expanding ownership of security. I want to empower people in accounting, HR, and executive assistants – everyone in the company – to realize that they can be a part of the security solution."

COMMUNICATION, REVENUE ALIGNMENT, & EFFICIENCY GAINS

McAuley employs a number of security awareness training programs. One successful program was a blog campaign tied to Cyber Security Awareness Month. For 31 days she posted a new, easy-to-understand blog post each day about a different security topic, such as two-factor authentication to better secure your Amazon account. Her users truly embraced the learning because it was communicated in an easy-to-understand and engaging manner. By the end of the month she was able to impart more advanced security topics, like threat modeling. As employees felt empowered to protect themselves outside of Mercer, they felt, in turn, more empowered to protect Mercer as well.

McAuley takes security out of the back room and makes it something everyday users can understand and talk about. Bringing security out of the back room means technical team members have to be competent communicators. "Communication in general is so important. We need to translate the technical aspects of what we are doing to a non-technical audience. This is likely the most important factor for career growth for security professionals. You have to be able to translate battlefield to boardroom. The ability to communicate how security impacts sales and revenue in a business manner is critical."

Prior to Mercer, McAuley worked in consulting, where she had to prioritize financial impact for her clients. She says, "As a consultant I was forced to think about driving profitability. As a CISO you need to be competent in all

> “For a CISO, the CIO can be a very powerful ally so long as the organization they are running is not solely a technology shop. Information Security and Cybersecurity are broader than IT. Security is based in risk and it has to be something that is aligned to business strategy. As long as you have a broad enough perspective into these business functions, then the security program can be effective under the CIO. When the CIO function starts with information, not technology, the CISO and CIO functions can be highly collaborative and successful.”

technical domains. I need to be competent as an incident responder, as a SOC engineer, I need to understand threat intelligence. But layered on top of that is the sense of driving profitable growth.”

Another way McAuley is instilling a security aware culture is by saying “Yes”. She says, “These days clients are buying with security as a consideration. They need to know that their information is protected, and used appropriately. This is a great opportunity for our team to show our impact on growth. Instead of viewing security as a cost-center, we aim to present security as a key business enabler that can drive profitability and client experience. We need to take down some of the challenges and frictions between security and process in an organization and focus on how to be more operationally efficient with our security. We need to make it easier for employees to be productive. We do that by saying yes instead of no and figuring out how to securely enable those functions.”

DRIVING THE CONVERSATION WITH THE LEADERSHIP TEAM

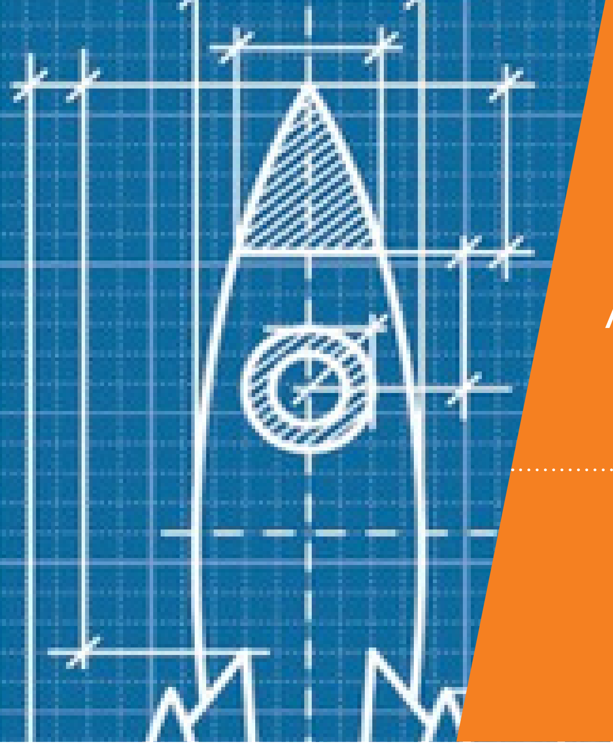
“Transparency is a big part of how I communicate to my leadership team. I present a realistic portrait of where we are and where we need to be. If you want the CEO and CFO to understand the technical risks and the value of a solution you want to implement, then it behooves you to articulate the ROI. That means answering questions like ‘How are we mitigating risk?’, ‘What is the commercial viability of a solution?’, ‘How does this solution drive the growth agenda we have as an organization?’. Understanding our growth agenda is of critical importance. If I don’t understand where we need to grow then I don’t understand how to securely enable it.”

As with many companies, growth will come from innovation, a large priority for Mercer. McAuley needs to be in lock step with the CEO’s vision in order to align security appropriately to enable innovation. To do so, McAuley says she follows the military concept of “two-up/two-down”. This means the team needs to have an understanding of the priorities, challenges and decisions being made two levels up, while teaching and coaching those same priorities and challenges two levels down the organizational hierarchy. This approach allows her team to understand motivations and drivers across the organization and effectively communicate and position security to be successful.

McAuley has open dialogue with her CEO and the rest of the executive team. While being open to any questions or concerns they have, McAuley makes an effort to drive their conversations by proactively providing educational information. “Rather than waiting for a question from my CEO, I try to keep the leadership team well-informed. I send a weekly communication explaining what has happened in the industry and the potential impact it can have on Mercer.” By driving the conversation, McAuley is able to better direct the CEO and various executive committees’ questions and areas of attention.

STARTING EARLY WITH CYBER SECURITY AWARENESS

It is no surprise that a CISO who values the human element of security would want to start early with security training. As a member of the Executive Women’s Forum, McAuley regularly participates in the Cybersecurity Schools Challenge. In the challenge, security professionals teach kids as young as five to think about online safety and security.



Addressing Cyber Security Risk with **Frameworks and Controls**

BY STEPHANIE HADLEY
CONTENT MARKETING MANAGER

THE YEAR OF ACTION AND EXECUTION STARTS WITH HAVING A PLAN, SO WE ASKED EXPERTS ABOUT ADDRESSING CYBER RISKS WITH FRAMEWORKS AND CONTROLS.

USING THE NIST FRAMEWORK AND CONTROLS FOR MAXIMUM BENEFIT; A STANDARD APPROACH TO TALKING ABOUT RISK AND SECURITY

According to Gartner, 30% of all public and private organizations began to implement frameworks such as the NIST Cybersecurity Framework (CSF) in 2015. Participation will increase to 50% by 2020. This prediction is backed up by conversations K logix has with CISOs today. Kevin Hamel, CISO of COCC reports that NIST's high profile within Boardrooms across the financial services industry is driving faster adoption of the framework.

Everyone in the organization needs to be aware and part of the successful implementation of the Framework. Therefore, security teams that have begun to use a Framework like NIST may want to evaluate how well it has been communicated and leveraged throughout the company. An effective Framework will support security efforts outside of the technology department and spearhead conversations around business process, business goals, and risk management. The framework may provide everyone in the company with a playbook and a common language to discuss risk.

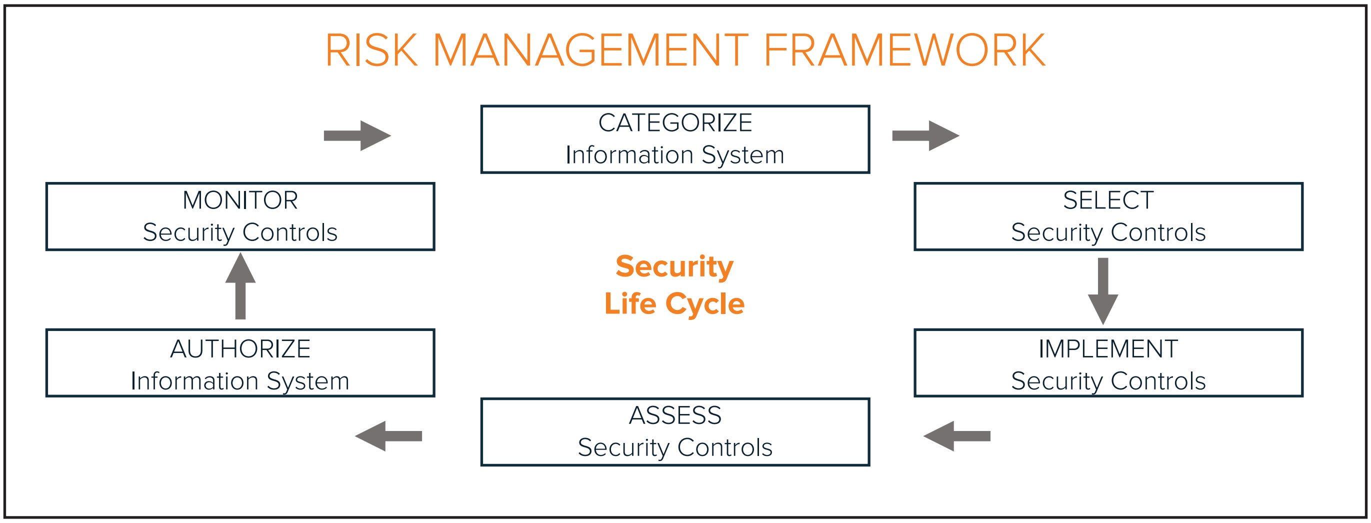
Matt Barrett, Program Manager for the NIST Cybersecurity Framework says, "There are no conversations at the executive level in business where cybersecurity isn't a dependency. It could be cash-flow, accounts receivable, customer service – everything is underpinned with cyber, and that means cyber security. That's the number one reason everyone in the organization needs to understand cyber security."

Eric Hussey, CISO at UNFI explains why they use the NIST framework, "The adoption of a cybersecurity framework gives you the guidance on how to implement a comprehensive information security program in any organization."

HOW TO GET THE MOST OUT OF YOUR FRAMEWORK

1. DEFINE RISK IN COMPANY-STANDARD WAYS - NIST encourages organizations to define their own profiles and coalesce as an organization around standard language to ensure that everyone is on the same page when talking about risk – whether cybersecurity risk, financial risk, or another type. Ron Ross, the creator of the NIST Risk Management Framework says, “A standard allows technical and non-technical executives to be in the same room and have a conversation that enables action. The C-suite doesn’t open their checkbook without a valid reason. The NIST framework allows everyone to understand how cyber security risk impacts their organization. It gets everyone talking the same language.”

While the NIST CF is agnostic in terms of risk management approach, Ross and Barrett both point out that the NIST Risk Management Framework works well to address cybersecurity risk.


RISK MANAGEMENT FRAMEWORK
CATEGORIZE Information System
SELECT Security Controls
IMPLEMENT Security Controls
ASSESS Security Controls
AUTHORIZE Information System
MONITOR Security Controls
Security Life Cycle

Adapted from the NIST Risk Management Framework (RMF) Presentation Slides

2. ALIGN CONTROLS WITH BUSINESS GOALS - CISOs adopting cyber security controls should look at how the controls impact and align with business goals. John Pescatore, Director of Emerging Security Trends at the SANS Institute says, “Don’t do it [a control] if it is not tied to a business requirement. Before you look at the list of controls you must understand the critical business processes – these are unique per industry and company. Once you understand the value of those processes you can prioritize how to tackle the standards.”

Pescatore points out one adopter of the CIS CSC is a major public university. While one might think tuition or fees is its number one revenue generator, it’s actually public grants. In order to be eligible for grants universities must show they are protecting student information. So, since obtaining grants is a major goal for the university, PII security becomes a major initiative as well. That is an example of how you tie security controls to business goals.

3. DON’T LISTEN TO THE NOISE – One of the most important aspects of framework adoption is commitment. That means, CISOs cannot let the Board get distracted by fear-driven news reports on threats and attacks. Pescatore says, “Security executives can find a million things to do, but the controls help CISOs educate management on priorities and why certain security issues must be addressed before others. Often, the *Wall Street Journal* is telling business executives what is most important in security. There might be a big threat in the news, but is it a big threat to that company? If you don’t have an existing process and rationale, how can you explain what does and does not matter? You can use standards to prioritize with the Board.”

To maximize the effectiveness of Framework and Controls in your security operations remember to always align with business goals, communicate effectively, and stay committed to the approach.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

FEATS OF STRENGTH

THE YEAR OF ACTION
AND EXECUTION

MARCH 2016

K logix

WWW.KLOGIXSECURITY.COM
888.731.2314