FEATS OF STRENGTH

PROFILES IN SECURITY

Earning the right to be confident in IT Security

JUNE 2015

KLOGIX

WWW.KLOGIXSECURITY.COM 888.731.2314

LETTER FROM

KEVIN WEST

CEO

DEAR READERS,

In this issue you will read several Profiles in Confidence, which is our series of interviews with CISOs at organizations across the United States.

Our mission is to give CISOs a forum to share their challenges, their approach to problem solving, and their perspective on the industry, so others may learn from their successes and failures. We have interviewed CISOs from financial services organizations, healthcare companies, the public sector, retail, and consulting, and a few distinct trends have emerged.

Continue reading below to learn more about these trends. I hope you enjoy this issue of Feats of Strength.

CISO Trends

Analytics from Interviews with Top CISOs

Competitive Advantage, CEO Access, Peer Collaboration, and a Desire for Better Communication with the Board are Emerging Trends Among CISOs

CISOs know security is a business enabler and they are working to make an impact

53% of CISOs state that one of their main objectives is to align security with business goals and 46% want to partner with business leaders to help them solve problems.

Long stymied by a reputation as "Dr. No", as Dr. JR Reagan, Global CISO at Deloitte (page 8) put it, security teams have had to battle an outdated reputation that casts them as drags on productivity. It is not always easy for CISOs to convince others in the company that security can be more than an operational defense system and an actual business enabler. Michael Newborn, CISO at Bloomberg BNA (page 12), originally met resistance when he let other leaders in the company know one of his main goals was to advance the business. The initial reaction from some of his peers was, 'we don't need you to focus there. Just make us secure.' However, Newborn was able to show how security could actually impact business goals, which helped set the foundation for how his team would work with other business units to achieve their priorities.

Some CISOs go one step further, and believe that security is a true competitive advantage for their organizations. "Today security is a real business enabler, and proves to be a competitive advantage," says Darrell Keeling, CISO at retailer Land's End. He believes that CISOs who perform due diligence to accept appropriate risks and instill thorough processes can impact the business in a manner equal to revenue.

Reporting to the CEO

Today, more than half of CISOs report to the CIO, and just 7% report to the CEO, with the rest reporting to the COO, or risk-related organizations. When asked about the future of the security organization, 50% of CISOs responded that the role will eventually report into the CEO.

Why is a structural move necessary? Some CISOs felt that reporting to the CIO introduced a conflict of interest as security teams assess the risks of specific technology systems and often recommend that technology be used to address the risk. Phil Curran, who reports into the Compliance Department as Chief Information Assurance and Privacy Officer at Cooper University Hospital, is one security leader who believes as much. His group reported to the CIO at first, but found that the structure limited their ability to effectively communicate risk to other business units. He states, "The move out of IT was among the biggest factors in the success of our information assurance and privacy program." (Feats of Strength, April 2015)

Other CISOs believe that the CEO needs to hear directly, and more frequently, about risk. Damian Laviolette, the CISO at Webster Bank

"Today, security is a real business enabler, and proves to be a competitive advantage."

- Darrell Keeling, CISO at Land's End

(page 14) reports to the CIO. He says, "The CISO needs to educate the CEO on cyber security as it relates to business risk. CEOs need to understand security at their level, and they need their CISO to be a right-hand-man."

While most CISOs still report to the CIO, it is notable that more experienced professionals – those with more than one CISO title on their resume – are most likely to report to the CEO today. It seems that when CISOs look for their next opportunity, they seek CEO-level sponsorship of the security organization. Steve Bartolotta, CISO at Community Health Network of Connecticut (page 16), and formerly CISO at Yale New Haven Hospital, is a good example. He states, "Community Health Network elevated the role of CISO to report directly to the CEO just prior to my coming on board."

CISOs have face-time with the Board, but desire more two-way communication

92% of the CISOs we spoke with report some level of interaction with the Board. Many reported that they have a quarterly or annual update in front of the Board, and others are called in front of their Board when incidents within the company, their industry, or the news pique the Board's interest in the security program.

Nearly all respondents suggested they would prefer more strategic, two-way communication with the Board. Newborn, of Bloomberg BNA, stated that the company does not have a traditional Board of Directors, but that his interaction with senior leadership is limited; "I have their support and I have a process to communicate our risk posture on a monthly basis, but we need to be more engaged in two-way communication about the strategic direction of the company and security."

CISOs are in this together – peer networking, mentorship programs, and associations prove valuable

CISOs are fighting many challenges: a lack of executive awareness, advanced cyber threats, limited budgets, and inaccurate perceptions of the role. It is no wonder that they have become eachother's best advocates, supporters, and collaborators.

All of the CISOs, regardless of industry, mentioned that peer networking, conferences, and industry associations are vital to their own growth. Jim Routh, now the CISO at Aetna (page 4), learned this lesson early. Years ago, in his first CISO role at a major financial organization, he called upon Steven Katz, the first ever CISO, to help him build a presentation for the Board. Routh took that experience to heart and now regularly mentors other CISOs who are newer to the role.

Information sharing, even among competitors, is common and vital

Daniel Conroy, CISO of Synchrony Financial (page 6) said, "The Financial Services Information Sharing and Analysis Center (FS-ISAC) plays a key role in [information sharing] and is serving as the primary channel for receiving timely cyber security threat notifications. All financial services organizations need the Internet to be secure because they need consumers and businesses to feel safe about their private data. It is in the best interest of all to share cyber threat information to maintain a safe and secure Internet experience for all businesses and consumers."

Each CISO we have spoken with has their own unique story to tell. They face specific challenges and have tackled them with their own plans and the resources available to them. We hope you will read each Profile and learn something you can apply to your own organization. Even though each CISO must work within the requirements and demands of their own organization, there are certainly commonalities and trends emerging across the role. We look forward to tracking the CISOs progress through more Profiles in Confidence.

50% believe CISOs will eventually report to the CEO

Currently, only **7%** report directly to the CEO

53% of CISOs top priority is to align security with business goals

46% want to partner with business to help solve problems

PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs

JIM ROUTH

CISO
Aetna

Headquarters: Hartford, CT
Company size: 49,000+
Annual Revenue: $58 Billion

"It is important to share information on your practices. I take calculated risks in order to manage risk and by sharing this, I not only enable the industry to improve their capabilities, but I receive validation of what I am doing and feedback to see if I'm on track."

Jim Routh is a known name in the industry; between his contributions to numerous news articles and many high-profile speaking engagements, his drive to share information on practices and continue to improve the industry is evident. Currently the CISO at Aetna, Routh leads his team with clarity, openness, and purpose, creating an environment of continued growth and success.

THE POWER OF KNOWLEDGE-SHARING

On Routh's first day as an official CISO, he was working at American Express and encountered a situation that demonstrated the power of connecting with other CISOs. Routh saw a meeting on his calendar calling for a presentation on Information Security Strategy to the OCC (Office of the Comptroller of the Currency). Since Routh was new to the CISO role, he called upon Steven Katz (the first ever CISO) to help guide and instruct him on developing a strategy. Within an hour and with no previous relationship, Steven arrived with two other financial services CISOs, all of whom dropped everything to aid Routh in formulating the presentation and practicing his delivery. Routh says, "They taught me a valuable lesson, a lesson that I still pay attention to today - which is - the right thing to do is help each other in order to make the industry more resilient. That means making some sacrifices for the good of others."

With many years of experience under his belt since his first day at American Express, Routh now mentors and communicates with other CISOs on a regular basis. "There is a very common bond that is established, because when there is a major breach or a publicized attack, most of the time we already know about it, we know the trade craft, and often who the threat actor is. If we don't know right away, we get that information from people who we have trust-based relationships with," says Routh.

Routh spends time mentoring first-time CISOs, who often come directly to him for advice. This advice includes how to organize the security department, talk to the Board,

"Everyone should adopt a framework for their security program; my only caution is that frameworks alone don't stop sophisticated threat actors. There is a flurry of activity today to try to adopt and implement standards. Aetna chose to implement both the NIST Cyber Security Framework and the NIST 800-53 Standard. Adopting standards is positive for the industry and should be pursued. The trigger events are major public breaches by nation-state sponsored threat actors. Although the frameworks represent good, solid information security practices and should be pursued, more is necessary to deal with highly sophisticated threat actors. Changing the game for the adversary requires an in-depth understanding of their tactics from cyber security intelligence sharing and the use of "game-changing" control design that is innovative."

deal with business stakeholders, threats that are likely to impact them, and a multitude of further pressing concerns. In reality, Routh states that the hardest and most important decision that CISOs make every day is how to allocate resources to the highest risk. Every CISO has it in their best interest to do this, but it is a challenging thing to do because you have to constantly make trade-off decisions.

RECIPE FOR A SUCCESSFUL TEAM

Without a question, Routh wholeheartedly believes in the Professional Development Plan that is established within his security organization. This program allows each member of the security team to choose two skills or competencies that they would like to master, and they are provided with opportunities throughout the year to achieve this. "My job as a leader is to provide an environment that gives them what they need in terms of their professional development, and ultimately I want them to have the opportunity of choice or to have options available to them. We match their desire to invest in a skill or competency with development activities, in some cases adjusting their role to help them learn what they would like to master," says Routh. One trend Routh notices is his team picking a technical skill and a soft skill, such as choosing how to be an effective communicator along with learning how to interpret results from static analysis tools for application developers.

Paired with an extremely talented team, Routh has invoked a risk-based approach to running the security program. He shies away from a program geared only towards compliance, but one that focuses on understanding risk in order to make pivotal decisions in relation to allocating resources to the highest risk. This risk-based approach is transparent throughout the organization, resulting in a robust preparedness for security threats and vulnerabilities. This risk based approach to security works hand-in-hand with a robust privacy program, which is essential in a health care organization.

CYBER SECURITY LEGISLATION

The United States House of Representatives is taking up cybersecurity legislation which could grant companies protection from legal liability if they choose to voluntarily share certain cyber threat data with the government. "The basis for the proposed legislation is a problem long known by lawmakers to address constraints to sharing cyber security intelligence back and forth between federal agencies and the private sector. The information sharing capability needs to be facilitated to address two things. First, there must be sharing of threat intelligence from different federal agencies with the private sector. Second, it must encourage more free flow of cyber intelligence and information from the private to the federal sector and for those respective agencies to have the ability to do something with that information."

PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs

DANIEL CONROY

CISO
Synchrony Financial

Headquarters: Stamford, CT
Company size: 11,000+
Annual Revenue: $2.11 Billion

PRIORITIZING SECURITY AT SYNCHRONY FINANCIAL

Daniel Conroy, CISO at Synchrony Financial, is an engineer by education and brings an analytical and practical approach to all aspects of planning, delivering, and managing teams. His primary areas of focus are: intelligence collection, defending Synchrony Financial's network, effective communication, and providing the bank's clients with security assurance. According to Conroy, among the many institutions he has worked for, Synchrony Financial is the most focused and engaged in information security. He says, "The energy is different here. People are excited about the positive impact security can have on business, and use it as a true business enabler to provide a competitive advantage to Synchrony Financial."

Conroy states that Synchrony Financial's Board understands the value of security - including related threats, challenges, and opportunity. Information security is a priority for senior management. They ask informed and intelligent questions about the security strategy, which Conroy states is focused on enhancing and maintaining a proactive, agile, and adaptive security program that delivers a sustainable competitive advantage.

"We chose the name Synchrony for a reason – we are in sync with our clients and customers. That promotes a security culture as well." In addition to cyber intelligence and infrastructure defense, Conroy considers client engagement a key pillar of the security organization. "We share our security knowledge and cyber intelligence with our clients, who may not have the resources we have. By sharing information with them we are helping to protect the entire payment ecosystem, which not only improves our customer relationships but also better secures all aspects of our transactions." In addition, we engage with our customers to educate them on information protection techniques and regularly remind them to remain vigilant for incidents of fraud or identity theft.

Some of the information shared with clients

comes from the company's Cyber Intelligence group, which collects and analyzes threats by leveraging both internal and external resources. Action is key to this group's success. The group has prioritized threats and is continually evolving its knowledge of adversaries, who are improving their attack methods at lightning speed.

For Conroy, much of security comes down to what he can control, and identifying and accepting risks associated with what he cannot control. "When I stopped playing rugby, I started doing triathlons. I quickly learned that there are only so many things you can control. You can't control the waves, your competitors, or the weather. What you can control is your training and your state of mind. You can study your past performances and make changes to your approach to improve your position. You can prepare yourself to address certain unplanned elements – like a flat tire, by bringing a spare. The more you prepare and the manner in which you address the things you can control can make the difference in your performance. You have to be laser focused on maximizing performance and minimizing risks in the environment. It's the same for information security. A successful security team is one that exercises control where it can. They should be able to minimize the impact of the unexpected by making decisions based on research, intelligence, practice and training."

THE FUTURE OF SECURITY

"Information security used to be an afterthought to systems and processes. Today, security needs to be inherent in the DNA of all systems to work effectively. Some information security issues exist because of flaws in the solution architecture, which was created 25 or more years ago. Technology was not architected with today's business in mind, so many are looking to retrofit security. There will be these types of threats until we get to a point where everyone is working from a secure architecture and following the same standards. It is going to take time, but we will get there."

SHARING INFORMATION WITH COMPETITORS

"In the financial services industry, we actively share cyber threat information and attack vectors with partners and peer banks. The Financial Services Information Sharing and Analysis Center (FS-ISAC) plays a key role in it and is serving as the primary channel for receiving timely cyber security threats notifications. 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."

PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs

DR. JR REAGAN

Global CISO
Deloitte Touche Tohmatsu Limited (DTTL)

Headquarters: New York, NY
Company Size: 210,000+
Annual Revenue: $34.2 Billion

Dr JR Reagan's definition of a Confident Security Organization

"Confident organizations make security part of their corporate culture, whether implicit or overt, without being draconian. With a confident security program, every member of the company feels like they are a participant in keeping information safe."

AN ADVANCED, CONSISTENT, AND CENTRALIZED SECURITY PROGRAM

Dr. JR Reagan, the Global Chief Information Security Officer for Deloitte Touche Tohmatsu Limited, began his career in the security industry, but he does not have the typical resume of a security industry veteran. An early boss who did not think highly of security encouraged Reagan to study innovation, marketing, and analytics. Reagan maintained his interest in security and saw how these areas could intersect. Today, Reagan is a TED speaker on innovation, a marketing and analytics professor at Johns Hopkins, Cornell and Columbia, and Global CISO at Deloitte.

In his TED talk, Reagan explains how innovation can come from anywhere – from children and from third world countries - not just Silicon Valley. He puts this belief into practice in his security organization. Being *"advanced"* is one of the groups three main tenants. "It is not enough to do what is just 'okay'. We don't have all of the answers, but we have to think about the future. How will we do things three or five years from now? What do we need to be prepared to address?"

Reagan stays clued in to advancement by tapping into a vast network of peers, CISO forums, and hot spots of technology innovation. "Innovation moves so fast these days you can start to get a feel for where things are going and better prepare for it. We architect our solutions today to be open to the innovation that is coming."

Reagan's security program is also *centralized*, which is no small task for a company with offices and clients across the globe. "We look for commonalities to set global standards while allowing for specific regulatory and data privacy laws within each country. Our customers require this of us, and my team works with member firms to articulate our security program to these clients. This is something that is happening much more today than in the past."

Lastly, Reagan's team strives to be *consistent*. Deloitte makes a brand promise, and part of that promise is that the client's information is secure with us. "We maintain consistent levels of security, and in a sense we are like the plumbing. You rely on us, but it doesn't really impact you. We are consistent in that way. But we are not just technology, in fact, I rarely talk about firewalls. We talk about the business. We need to enable new business models and support change and advancement. We do that by protecting information."

Does Security Have an Image Problem?

Since Dr. Reagan is a Marketing Professor in addition to a CISO, we asked him to weigh in on how security is positioned in the enterprise. "The security industry has a little bit of an image problem. It's viewed as geeky and technical. That was how security professionals valued themselves. But right now CISOs are going through a similar transition to the CIO. In security, this is causing an identity problem. Today it's not enough to talk about encryption. Tell me about the business. We are going to see rapid transformation in this regard. You'll start to see people entering the field without the typical technical background and that will change security's image."

- DR. JR REAGAN

SECURITY AND INNOVATION

"For the longest time, information security teams have been 'Dr. No'. We are overdue to think of new ways of addressing security with employees. That is where innovation comes into play. User behavior dictates whether security programs are successful. We have to find ways to embed security instincts in the natural way people work. This is something our industry is not good at right now. We cannot just have folks doing online awareness training. The airline industry is a great example. They have fundamentally changed how people respond to the safety videos by making them engaging, funny, and interesting. We are rolling out new training videos at Deloitte, "Don't Be that Guy". We are going to show the security mistakes everyone makes, in a funny way, and hopefully with humor change behavior."

ARE YOU PREPARED TO MAKE AN IMPACT IN THE BOARDROOM AS A SECURITY LEADER?

LEADERSHIP STRATEGY

BY MICHAEL SANTARCANGELO

You can make an impact in the boardroom if you prepare yourself first.

"The board wants to speak with you."

Finally. The opportunity you've been waiting for. As more executives turn their focus to security, you expected that eventually, you'd get to speak with the board. This is your moment to shine, to convince them of the importance of security.

Are you going to make the **RIGHT IMPACT?**

The answer isn't as simple as showing up. The key to making the right impact is preparation.

As Kevin West, CEO, K logix explained, "It is important for security leaders to separate the signal from the noise. The signal is the list of business goals and objectives as outlined by the Board. Maintaining focus on the signal means your security program will always be in alignment with executive priorities, which gains you greater respect in the board room."

A quick note about **THE BOARD**

Kevin shared a key insight on working with boards, "Board members are business people. They understand risk. What they want to know is how you are going to address the risk. They would rather know about risks upfront than be updated after an incident occurs. Bring the Board a plan that puts security in line with business goals to get the best response."

> "Board members are **business people**. They understand risk. What they want to know is how you are going to address the risk."

How it **WORKS**

Kevin shared a recent example of how effective this method of preparation is:

"One CISO I recently met with told the story of his board being floored when he told them that focusing on 100% prevention would basically put the company out of business - it would make it too hard to do work, too hard for customers to engage with the bank the way they wanted to, and too difficult to work with partners.

Once the board member saw how security was being respectful of key business goals, he had a much easier time understanding our focus on prevention, but also incident response. This conversation happened because that CISO was speaking from a position of strength, he didn't wait until a breach happened to explain to the Board that it was inevitable. He told them a breach may happen, but there was a plan in place to minimize its impact."

What are you **WAITING FOR?**

Whether you enjoy a good working relationship with the board or are waiting for the opportunity, invest the time now to be prepared. Consider the relationships you need -- across the organization -- to be successful. Gather evidence of success.

It helps to set aside our bias for breach prevention. Consider how to quickly detect and effectively respond to incidents and potential breaches. In the process, work to translate the technical aspects into functional understanding. Be ready to explain the value of your program to others, in a way they can understand.

While this takes time and effort, the payoff comes when it's time to speak with the board. Done right, the conversation is natural and not forced.

Do the work to distill your value, earn the recognition as an IT leader, and have your voice heard by the board. Make an impact that gets results.

This article was originally published in CSO Online Magazine. The author is Michael Santarcangelo - the catalyst to develop remarkable IT Leaders and high performance teams. He is driven to help IT leaders reconnect with their value; providing them counsel from someone who can help them build bridges and gain the recognition they deserve as a leader.

3 Ways to Prepare Before Speaking to Board

1. **Invest in relationships:** you should have at least one ally in the boardroom with whom your organization has completed a successful project. Leverage that person's commitment to security to introduce others in the Boardroom to its value.
2. **Translate technical jargon into functionality:** Effective security leaders discuss security in terms of its positive impact on achieving business goals and increasing revenue. Avoid talk of specific threats, technology standards and other items that move the conversation away from business goals.
3. **Provide proof:** Prove that you belong in revenue discussions by providing success stories, reports and testimonials that show how security impacted the bottom line. It helps to consider the security story you share (and practice to get it rightet it right).

PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs

MICHAEL NEWBORN

CISO

Bloomberg BNA

Headquarters: Arlington, VA
Company Size: Approx. 1500

"The role of the CISO is really evolving right now. The more security breaches are on the front page [of newspapers], the more the CISO is elevated in the company. Breaches are a real issue. The President declared a State of Emergency on Cyber Security, and rightly so. We cannot ignore the emergency situations, and we must react to threats. The key to success is identifying the actual threats to your business and making executives aware of them so you may limit your exposure. "

BUSINESS AND SECURITY TRANSFORMATIONS

Bloomberg BNA, a wholly owned subsidiary of Bloomberg, is a 75 year old print company that has transformed to an online, technology driven service. The company needed their security practice to evolve as well. That is why Michael Newborn was brought on board as the company's first CISO.

Newborn joined the company in December of 2013 after ensuring that Bloomberg BNA was committed to security at the executive leadership level. Prior to Newborn's arrival, Bloomberg made a strategic commitment to security, opening the CISO position and moving the security function out of the IT department to report directly to the COO. The CEO also showed an interest, passion, and understanding of security, which Newborn believes is key to establishing a successful and confident security organization. "I was brought in to re-establish and create a more holistic security program here, because the CEO understood security needs to be a priority."

A NEW APPROACH SURPRISES PEERS AND REAPS IMMEDIATE BENEFITS FOR THE COMPANY

"In my first days on the job I didn't even look at the technology. I focused on meeting the different business leads. I asked them, 'What are you trying to accomplish? What do you need from security, and what does security mean to you?" He said he received many responses about limiting exposure and negative publicity. However, the more Newborn spoke to the business leaders, the more he understood about the business itself. He learned that availability and reliability were key concerns and that customer data was critical to business success. Once he understood how the business leaders defined success, he could identify ways for security to enable the business.

"I reported back on my main goals, one of which was to advance the business. The initial reaction from some was, 'we don't need you to focus there. Just make us secure.' But I was able to show how security could actually impact business goals, which helped set the foundation for how I would work with the other business leaders."

Transforming a company's security program comes with challenges, and Newborn admits he has asked for a lot from some departments, especially IT. "I am asking IT for the most transformative change, so of course this new security approach is toughest on that organization. But, I treat them just like any other department in the company. I try to understand their key objectives and pain points and focus on security changes that will also help them meet their goals." While Newborn believes it is important for the security organization to function outside of IT, he does not diminish how much security relies on the IT department as a business partner. Newborn says, "Fifteen years ago we would have put the firewall in the security department, but now security is so much more than that. The firewall is a network program, so it needs to be managed from IT. IT needs to handle the networking issues so security teams can focus on business problems."

PARTNERING TO BENEFIT THE BUSINESS: A POSITIVE IMPACT ON PRODUCTS AND CUSTOMER SERIVICE

As Newborn studied the company and its service offerings to ensure security aligned with business objectives, he realized he could make an immediate impact by directly assisting Bloomberg BNA's business lines. One example was when he helped with the fine-tuning of its Privacy & Security service product to legal and business customers. He helped them build out the guidance and culled expert sources from his network of peers. Another immediate impact was standardizing responses to customer requests for vendor assessments. This saved a large amount of time, effort, and work for the other departments. As a result, Newborn now has the goodwill and support he needs from other departments to continue his progress.

Newborn knows that to be successful he needs to have regular communication with the CEO and senior leadership. "Right now, we have a workable process, however I am continuously refining it to improve both clarity and relevancy. I am still very focused on building the team up. I can get a reaction [from senior leadership] with a laundry list of risks we need to address. I have their support and I have a process to communicate our risk posture on a monthly basis, but we need to be more engaged in two-way communication about the strategic direction of the company and security."

- MICHAEL NEWBORN

TRANSPARENCY HELPS PROVE VALUE

"Security has had a history of secrecy, where some have been hesitant to share program details and objectives with the business, but I believe we need to be transparent. Showcasing our wins builds up my team and highlights how security can positively impact the business. Likewise, we have to admit our failures and outline our plan for addressing those issues. There was no CISO role before me at Bloomberg BNA, so I need to be as open and trustworthy as possible, to help establish credibility and highlight the true value of the program."

PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs

DAMIAN LAVIOLETTE

CISO

Webster Bank

Headquarters: Waterbury, CT
Company Size: 3,000+
Assets: $23 Billion

DIVERSE EXPERIENCE LEADS TO A BALCANCED APPROACH TO SECURITY

Damian Laviolette, CISO for Webster Bank, a regional bank headquartered in Waterbury CT, cites balance as the key to success in security. At multiple points in his career, Laviolette has been able to blend two very different viewpoints to be successful in security.

Laviolette spent 20 years in technology and information security for the US military before retiring from active duty and taking a role at one of the most forward-thinking and quirkiest banks in the United States, Umpqua Bank in Oregon. Umpqua Bank is known for hosting yoga and even weddings in its banking centers. It would be hard to find a company culture more different than the military. While he acquired most of his technical training in the military, Laviolette took just as much of an education away from Umpqua. There he learned the importance of differentiating the business from competition and was able to apply that to his security programs. For example, at Webster Bank, Laviolette has helped the company differentiate its mobile offering from his competition by providing different security parameters based on the sensitivity of the transaction. Simple transactions require minimal security actions from the customer, which improves the customer's overall experience.

Laviolette's security philosophy calls upon another dichotomy. In referencing *The Godfather*, Laviolette explains that ten years ago most companies were looking for a peacetime consigliere, someone who focused on compliance, audits, and exams. In recent years the focus has switched, companies needed a more aggressive or wartime consigliere. The wartime consigliere is focused on defense in depth, DDOS, and other aggressive defensive technologies. Today, organizations require a more balanced consigliere one that is capable of understanding business requirements and wartime efforts. That is where Laviolette tries to focus.

CAPITALIZING ON THE BOARD'S INTEREST IN SECURITY

Information security and cyber security are the top concerns for Webster Bank's CEO and the Board, so Laviolette gets plenty of face time and interaction. Fifty percent of the time, meetings focus on threats and questions that the Board has about incidents, both within the company and in the news. The other fifty percent of the time, the group relies on Laviolette to educate them on his plan and forward movement. Still, as smart and security-savvy as the group is, they were surprised when Laviolette explained that "focusing on total defense and protection would put us out of business". Laviolette explained that to be completely secure, the Bank would have to forego critical technology advancements, which would result in losing customers to competitors in the process. Instead, Laviolette focuses his team on reasonable prevention and incident response. "An attack is going to happen, it's how quickly we can recover and be back on our feet that will determine how much damage the breach does to our bottom line."

WHERE WILL SECURITY BE IN FIVE YEARS?

Even though Laviolette has a great working relationship with the CIO of Webster Bank, to whom he reports now and previously at Umpqua Bank, Laviolette believes that in the near future there will be an industry-wide shift that will bring CISOs out of the IT department. "The most positive and effective shift happening right now is the CISO starting to report into the CEO. Most CEOs realize that information security has to be a top focus. They are fooling themselves if they do not realize it. But they are unsure of the cyber security world – they need a translator and that is what the modern consigliere (CISO) has to be. The CISO needs to educate the CEO on cyber security as it relates to business risk. CEOs need to understand security at their level, and they need their CISO to be a right hand man."

EDUCATING THE NEXT GENERATION OF SECURITY PROFESSIONALS

Like many in the industry, Laviolette is challenged to fill staff positions with security professionals who can balance technology acumen with business skills. So, he set out to do something about it.

"Webster Bank is involved in the local community, and our CEO has a close relationship with the leaders of Naugatuck Valley Community College (NVCC). NVCC invited me and Webster's CIO to speak about Information Security as a career path, and from there the CIO and I helped the college develop a two-year program for future security professionals. The training includes technology skills, but we made it clear that those interested in cyber security have to understand that they cannot expect to sit around in a dark room with a Mountain Dew and minimal social interaction. That's what the bad guys do. Good security professionals need to know how to talk to senior business leaders about risk management and policy, and deliver user awareness training, in addition to technical know-how. We emphasized to NVCC that the training program must include communication and presentation skills, along with technical certifications. The new program is designed and expected to produce entry level security professionals who can jump right in to today's security organizations."

PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs

STEVE BARTOLOTTA

CISO & Vice President
Community Health Network of Connecticut

Headquarters: Wallingford, CT
Company size: 500+

"We maintain protected health information (PHI) and other regulated data, so our information security efforts are high priorities. In fact, a major breach could have a significant impact on our business, and to the State of Connecticut. Information security is so important that Community Health Network elevated the role of CISO to report directly to the CEO just prior to my coming on board."

WITH A SEAT IN THE LEADERSHIP FORUM, CISO ENSURES SECURITY IS INVOLVED FROM THE START

Community Health Network of Connecticut (CHNCT) is an Administrative Services Organization (ASO) in Connecticut. CHNCT's job is to effectively manage member healthcare and provider participation while lowering costs for the state. Since they are governed by HIPAA compliance and other state regulations, and are also determined to reduce risk of exposure to the business, CHNCT puts a priority on information security. In fact, Bartolotta believes CHNCT is one of the few organizations in the healthcare industry where the CISO reports directly to the CEO, holds positions on the leadership team, and has a presence in the Board Room.

A CEO with the foresight to install the CISO position as a direct report is very aware of the importance of security. Bartolotta says, "Our CEO is very knowledgeable when it comes to security. Our conversations are typically about establishing an acceptable risk profile and minimizing exposures." While the CEO partnership is important, it is Bartolotta's participation in the senior leadership meetings that he most values. "Since I am in those senior leadership meetings, I am able to ensure that security is a consideration from the get-go of a new process, program, or project. It makes the entire process much more efficient and collaborative."

Putting a Good Plan into Action

"If you are a CISO, you must be a business person first. Learn the business inside and out. Meet with every VP and line of business manager to understand their goals and priorities. From there you should be able to create a good plan to ensure you are protecting the necessary information and systems," said Bartolotta.

Bartolotta follows a philosophy that incorporates teamwork, leading by example, collaboration and respect, among other things, to ensure the security plan is successfully implemented.

- BE A ROLE MODEL

It was once a manager's job to simply draw a line of sight from the employee to the organization's mission, value, and success criteria. Today, that is still important to do, but you must also lead by example. As leaders, we have to show them, through our actions and interactions, how to approach security from a business perspective.

- BE RESPECTFUL

It is important to respect the contributions of everyone, including our teammates in security, the greater organization, our vendors, and our partners. "When others succeed, it is easier for us to succeed."

- BE BUSINESS-FOCUSED

In building the best team, Bartolotta prioritizes integrity and business acumen as much as technical skills and security certifications. How candidates fit into the team and the culture matters most of all. "I look for flexibility, business awareness, and the unique talents they can bring to our team."

- BE OPEN AND PERSONABLE

On Bartolotta's third day at CHNCT, the security team received a request from a business unit. The security team's existing procedure was to review the request and possibly approve, but usually deny it via email. Instead, Bartolotta requested a meeting with the business unit. Together they discussed the business challenge behind the request and Bartolotta's team made suggestions for approaching it in a secure manner. As a result, the business unit gained a better understanding of security's motivations and the impact their operations may have on corporate security, and also received a satisfactory solution to their issue.

- BE CALM

In security, it is easy to react loudly and forcefully; it is a fast paced and intense industry with a lot of uncertainty. However, a calm manner is one of the main characteristics of a confident person. If you are a calm security person, you are well-prepared and focused on your mission, not on distractions.

- BE A CHAMPION

Security does not often receive many accolades in an organization, and has limited visibility when things are going well. That is why Bartolotta believes in the importance of championing your own program. Bartolotta branded the "Office of Information Security" (OIS), complete with its own logo, when he arrived at CHNCT. This helped establish an identity for the security organization. The "OIS" holds regular training sessions, breakfast meet and greets, security events, and lunch and learns, so the larger company remains up to speed on security's value and initiatives.

LEARNING FROM OTHERS OUTSIDE OF SECURITY

Years ago, Bartolotta was working at a hospital in Connecticut when his wife went to an emergency room at another hospital. Bartolotta was so impressed with the service that his wife received and the manner of the caregivers, he commented on it to the nursing staff. "How is it possible you have made this negative event a positive experience for us?" he asked a nurse. "We hire good people," she said. From that experience Bartolotta learned to value integrity, as much as technical skills and business acumen, in building a successful team.

Who are the most **SOCIALLY ENGAGED** Chief Information Security Officers?

#CISO

If you work in information security today, you're on Twitter. Or are you? These CISOs are leading the way.

Dr. JR Reagan, CISO Deloitte
@IdeaXplorer

Alex Stamos, CISO Yahoo
@alexstamos

Phil Agcaoili, CISO Elavon
@Hacksec

Kees Leune, CISO Adelphi University
@leune

Diego Aguirre, CISO peerTransfer
@diegoku

Jared Carstensen, CISO CRH
@jaredcarstensen

Tim Youngblood, CISO Kimberly Clark
@youngbloodtim

Richard Rushing, CISO Motorola
@SecRich

Chuck Kesler, CISO Duke Medicine
@chuck_kesler

Darren Argyle, CISO Markit
@D_Argyle

Find out how they **made the cut** and see even more social CISOs on our blog: klogixsecurity.com/blog

MAKING SENSE OF A CROWDED ENDPOINT SECURITY MARKET

HOW WE HELP OUR CLIENTS BUILD THE RIGHT SOLUTION

BY RICK GRIMALDI
DIRECTOR OF TECHNICAL SERVICES

Everybody is concerned about the endpoint. Study after study states that the endpoint is the top concern of CISOs and CIOs, and the biggest growth sector within security. As a result, every security vendor that touches the endpoint is staking a claim to the market, joining the traditional anti-virus players. The segment is crowded, noisy, and confusing.

How do you select the right endpoint security solution for your organization? Which factors will impact your decision? How will you quantify success?

At K logix, we are applying our technology on-boarding process to this market. With this process we take a step back from product features and functionality and we evaluate the endpoint security space through the lens of our Project Advisory Service. Our Project Advisory Service helps clients establish clear goals and requirements before determining if a specific technology is needed to solve a security problem. We involve business stakeholders and technical team members to ensure that the groups are in alignment before any investments are made. With regards to endpoint security, we identified key requirements that are common among both business and IT security stakeholders, including:

- Productivity – The product cannot impact productivity. Drags on productivity negatively impact revenue and make it difficult for security teams to gain the buy-in and respect of executives and the organization.
- Competitive Advantage – The solution must deliver business impact and ensure a competitive advantage.
- Malware Defense - The solution must effectively address advanced malware.

Whether you need K logix to lead the investigation into your requirements with a Project Advisory Service, or if you need assistance with vendor selection and implementation, K logix can help you make a smart decision. If you would like to learn more about our approach to endpoint security, or the results from some of our initial testing and its relevance to your business, please contact K logix.

Sponsorship message from LogRhythm

WHITE PAPER DOWNLOAD:

Surfacing Critical Cyber Threats Through Security Intelligence

A Reference Model for IT Security Practitioners

A CyberEdge report indicates that 71% of organizations were compromised during the 12 months preceding the survey. *Is your company one of those?*

In 2015, companies have been comprised an average of 229 days before detecting the attack according to the Mandiant 2014 Threat Report. *How quickly will your organization detect & respond to an attack?*

A 2014 report from the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cyber-crime is more than $400 billion. *What will a breach cost your company?*

LogRhythm's award-winning security intelligence and analytics platform is designed to significantly reduce the time to detect and respond to cyber threats, enabling organizations like yours to neutralize them before they can cause a damaging cyber-incident or data breach.

This white paper provides key insights on security intelligence, the evolution of cyber security, and an in-depth review of the Security Intelligence Maturity Model (SIMM) - a compelling framework to help organizations improve their time to detect and respond to cyber threats.

DOWNLOAD
THE WHITE PAPER TO LEARN:

1. How Security Intelligence and threat information enables companies to clearly see the threats that matter
2. The End-to-End Threat Lifecycle Management™ and how it can decrease your time to detect and respond to threats
3. How the Security Intelligence Maturity Model (SIMM) measures the effectiveness of an organization's security capabilities and its Mean-Time-to-Detect™ (MTTD™) and its Mean-Time-to-Respond™ (MTTR™)
4. The critical capabilities that a Security Intelligence platform must deliver toward the goal of becoming impervious to cyber threats

Key Findings Include:

The number of detected security incidents keeps growing year after year with a 66% (CAGR) increase from 3.4M (2009) to 42.8M (2014).

Recent estimates by one cyber security company reported that as many as 71 percent of compromises go undetected.

By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches – up from less than 10% in 2013, according to Gartner's report, Prevention is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence.

Contact a K logix Sales Rep to get a copy of the white paper and learn how K logix and LogRhythm can help assess your security posture

LogRhythm®

SANS CRITICAL CONTROL 14: AUDIT LOGS

By Duane Elbrecht Solutions Architect

Each issue, an expert provides analysis on one of the SANS Top 20 Critical Security Controls. To see past Controls, visit our blog klogixsecurity.com/blog

Whenever I think of audit logs, I think of the great Clifford Stoll and how he uncovered an espionage ring while working as a systems administrator at the Lawrence Berkeley National Laboratory. One of my favorite books, *The Cuckoos Egg*, details his story.

In this true story, a former astronomer takes on the position of sys admin when grant money runs out. One of his new responsibilities in this role was accounting for billing time on the university mainframe and assigning the cost to the correct department. One day while reviewing system access logs (really a mish mash of custom scripts that cross referenced various accounting information), he discovered a very small discrepancy of only a few minutes of unaccounted time on the system. And thus begins his story of digital forensics and tracking a Soviet hacker through the early years of a burgeoning internet. Since then, audit logs have dramatically matured along with the SIM platforms that manage them and provide valuable forensic information and real time insight. **So, why do audit logs matter and how can you make sure they are working effectively?**

The first part of that last question seems to have an obvious answer, but let's take a closer look.

Audit logs create an **(1) accountability factor**. The information that is logged can tie specific events with specific accounts thus creating a digital finger print. If enough of these "finger prints" are collected, we can then **(2) reconstruct a time line of events that occurred before and after the event of concern.** This is crucial when understanding what action needs to be taken to address the event. Is the event simply a restart of a service through normal maintenance activities or more importantly, did someone intentionally turn off the service to hide their activity and identity while doing something malicious? Thus, logs provide **(3) intrusion detection and insight into what might be considered unusual activity.** That activity may present itself as: failed login attempts (someone trying to hack an account password), high memory utilization (malware running in the background), or scans being run to detect open ports (someone looking for a hole to exploit). Audit logs also provide information for problem detection and root cause analysis, another critical piece when troubleshooting difficult problems.

How can you make sure your audit logs are working effectively?
This can be a tough one to get correct and it often takes several attempts to adjust what the logs are reporting. Many logging systems these days are reporting exactly what they need to report on, right out of the box. Things have come a long way since Clifford Stoll's early days and in most cases, simply "checking the correct box" enables the correct logging. However, sometimes these logs need to be customized for the system. In short, are the logs you are looking at collecting and reporting the information you need to know? "Who, what, and when" are very important questions to ask in this effort. Securing access to the logs on a hardened system, thereby ensuring their integrity, is paramount to maintaining confidence in the information being analyzed.
Some things that should be considered to make sure you are getting the most out of your audit logs are:

(1) What are the compliance requirements for your business, such as SOX, HIPAA, PCI-DSS, ITAR, etc? Though there is often significant overlap with these standards, it is important to understand which are vital to your business.

(2) How long are you keeping the logs versus how long are you required to keep the logs? These are often different and the reasons for this varies. Sometimes, logs are kept longer than needed because of the fear of "what if?" Trending analysis is another reason to keep logs for an extended time. What ever the reason for keeping them, remember the more logs you gather, the more resources it takes to perform an analysis. This may become costly, so there is often a cost benefit tipping point that management must buy into to support this effort.

(3) What is your log analysis process? What good are logs if they are not being reviewed on a regular basis? Alerting must be tied to events that are considered critical, and a process for handling critical events must also be in place to give them the proper visibility and response.

As SANS Critical Security Control 14 points out, *"Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files."*

The Case for Information Sharing

BY ARMAND BOUDREAU CISSP

2015 might be the year that threat intelligence is finally taken seriously. The community has been abuzz recently over several bills making their way through the House Senate Committee that focus on the need for increased information sharing between both organizations and the federal government. Congress will hopefully come to agreements around establishing a framework, albeit light, for information sharing and affording legal protection for those who choose to share.

While these bills have a long way to go, I certainly think they are a step in the right direction to help promote visibility into an intimately complex issue that many organizations are bumping up against. The need for infosec data sharing seems to have reached critical mass, as most organizations are clueless as to what types of attacks are being used against their industry peers and more importantly other organizations with similar network topologies and application stacks.

We need a standardized method of exchanging threat intelligence and vulnerability information across organizations and between toolsets.

Many subscription based threat intelligence feeds have come to market over the past few years and are positioning themselves as a solution to help bridge these visibility gaps. Unfortunately, these types of feeds often have limited value as the data is typically very specialized by industry or vertical, and outside of additional SIEM visibility and context, require manual processes to incorporate them into preventative toolsets often losing out on the true value of this time-sensitive data.

Some products address this issue by incorporating the threat intelligence data collected across their customer base and automatically providing it to the rest of their customers. Solutions like these unfortunately operate in a closed ecosystem resulting in valuable information being compartmentalized to a single toolset or system. In a perfect world this critical data would be shared across platforms in real-time and even with other organizations for the greater good of security. In reality, as there is no financial benefit for building this level of integration between vendors and technologies, we will continue to see significant visibility gaps.

This is where some emerging frameworks and toolsets such as Stix, Yara, Open IOC, and Taxxi come into the picture. These solutions help organizations share both IOC data and higher level threat intelligence amongst each other in a standardized format. As these technologies have not been widely adopted and some compete against one another, IOC and threat intelligence data sharing on these platforms becomes a bit murky, especially when you factor in a researchers personal preference of a particular toolset.

We need a standardized method of exchanging threat intelligence and vulnerability information across organizations and between toolsets. In the real world, most companies still do not leverage threat intelligence services, let alone consider contributing to them. Anything we can do to help automate the process of sharing information is a good thing.

While data sharing is a complex issue, sometimes some of the best strategies are the simplest; by creating meaningful relationships with industry peers at other organizations and fostering a culture of collaboration within your team, you will greatly increase effectiveness of your security program.

Armand Boudreau is a Security Solutions Architect with over 14 years of IT experience.

Sponsorship message from Raytheon | Websense

Defense-Grade Cybersecurity

WHITE PAPER:

DATA THEFT PREVENTION

The Key to Security, Growth & Innovation

Industry and world leaders are calling upon the C-suite and governing boards to drive the much-needed change toward making cybersecurity a top priority. At the same time, security leaders need to keep their teams focused on the overall objectives of their cybersecurity investment. Fixating on the latest "cool technology" or getting distracted by the latest media-hyped threat does not help IT teams raise their organizations' level of data security.

IT teams need to adopt a more holistic approach to protecting their critical data. Cybersecurity from a Data Theft Prevention perspective is broader in scope, more intelligent in application and more effective in defending your critical data. Such a data-centric posture is an enhancement to data defenses, as it ensures that data is secured from inbound as well as outbound threats. Thus, Data Theft Prevention encompasses the entire security posture, not simply data loss prevention (DLP).

Learn more about Data Theft Prevention and **download the white paper** at websense.com/DTP

DATA THEFT PREVENTION ADDRESSES THESE CHALLENGES:

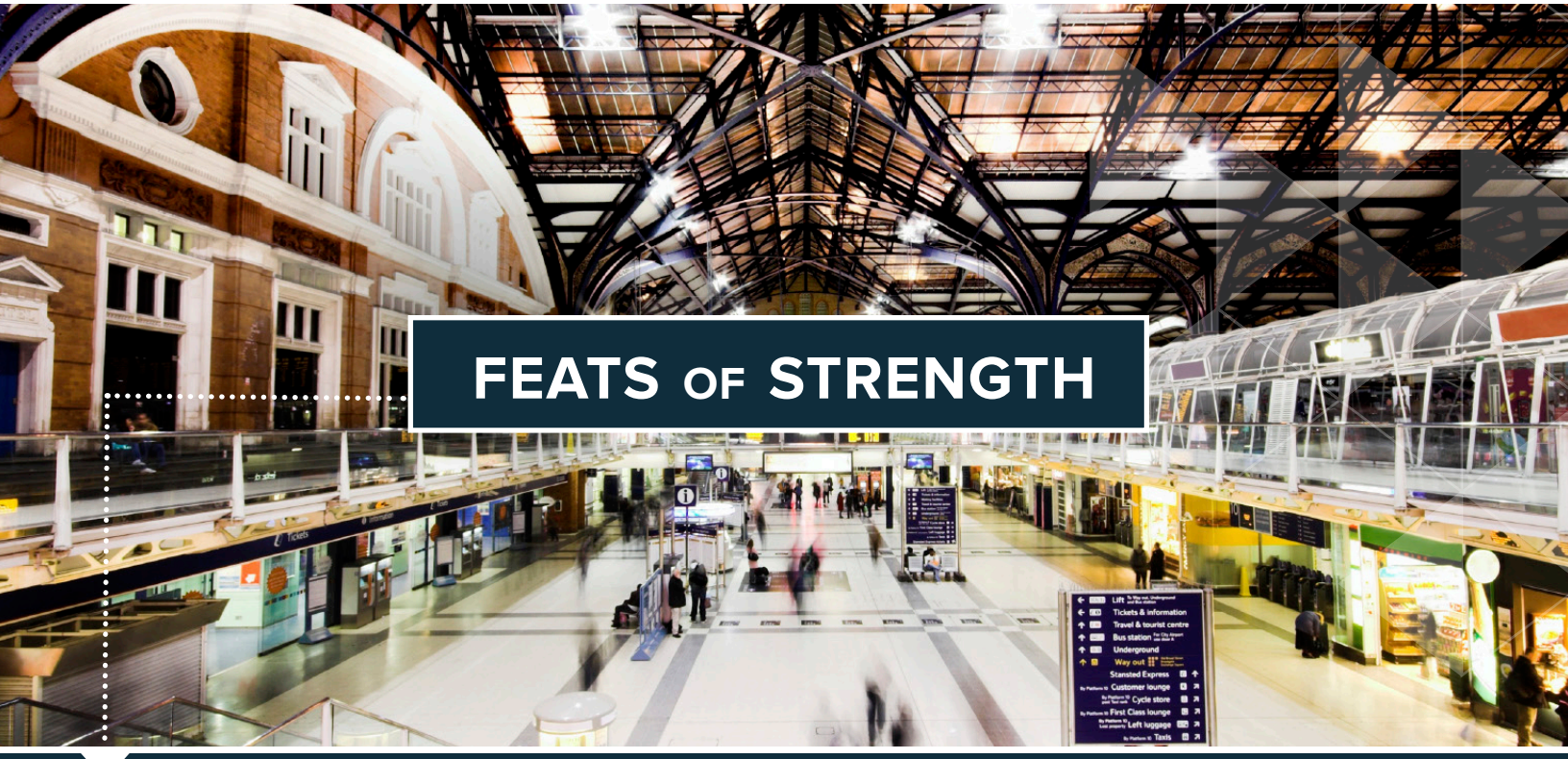
- Rapidly changing technology and threat landscape
- Explosive growth of off-network users and cloud data
- Growing insider threat and security professional skills gap

ENTER A NEW ERA OF CYBERSECURITY

Raytheon | websense

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446



FEATS OF STRENGTH

PROFILES IN SECURITY

JUNE 2015

K logix

WWW.KLOGIXSECURITY.COM
888.731.2314