FEATS OF STRENGTH

THE FUTURE OF INFORMATION SECURITY

DECEMBER 2015

WWW.KLOGIXSECURITY.COM

888.731.2314

K logix

Earning the right to be confident in Information Security

FEATS OF STRENGTH

DECEMBER 2015

PROFILES IN CONFIDENCE

FEATURES

CONTRIBUTORS

MISSION **STATEMENT**

Feats of Strength is a business-focused information security magazine.
We provide a platform for a diverse set of industry leaders to share their success and challenges.
By connecting people with thought leadership content, we examine different ways to build a confident information security program.

WORDS FROM OUR EDITORIAL BOARD

Chris Dunning, CSO, Affinion Group

Hussein Syed, CISO, Barnabas Health

Mike Newborn, CISO, Bloomberg BNA

Sumit Sehgal, CISO, Boston Medical Center

“THE CONVERGENCE HAS STARTED”

Says the CISOs of the *Feats of Strength* Editorial Advisory Board

At K logix, we strive to make our *Feats of Strength* magazine a voice of clarity, challenge, and discovery for CISOs, from CISOs. That is why we were grateful and excited when several experienced and engaged CISOs accepted our invitation to participate in our magazine as members of our Editorial Board. They help us decide on the direction of each magazine and guide us with insight into their own successes, but just as importantly, their challenges.

In this issue, we focus on the “Future of Information Security”, and our Editorial Board had a lot to say on this topic. One theme embraced by our Board is the idea that the security function is moving out of IT departments and closer to the business. The convergence of an increased focus on risks, the dominance of technology and cyber operations in business, and the “Internet of Things”, as well as our society’s evolving understanding of security practices and privacy concerns will lead to an elevated position for the CISO. Customer concerns, economic factors, and the strategic elevation of security as a competitive differentiator may all contribute to the CISOs maturation into the C-suite. Our Editorial Board believes future CISOs will be molded by MBA programs, more so than engineering departments. We feature a unique security MBA program at Idaho State in our article “Defining our Future Security Leaders”.

K LOGIX CONTRIBUTORS

Kevin West, CEO, K logix

Katie Haug, Marketing Director, K logix

Kevin Pouche, COO, K logix

Stephanie Hadley, Marketing Content Manager, K logix

LETTER FROM

KEVIN WEST

CEO

TAKING ADVANTAGE OF THE “SPECIAL OPPORTUNITY”

This issue of our magazine envisions the future of Information Security. It might seem premature to talk about the future when our industry is just emerging, but in today’s business environment, innovation moves at such a fast pace we must evolve even as we emerge.

Our industry is as young as computer programming was when Bill Gates was a student at Lakeside, a private high school in Seattle that happened to be one of the first to have access to a new generation of computers that shared processing power. As a result of this access, Gates was one of the first people to do computer programming in a way that was not painfully slow and arduous. Of course, Bill Gates is also exceptionally bright, extremely driven, and innovative. However, he made his mark on the computer industry because of a special opportunity that presented itself to a very small group of people. According to Malcolm Gladwell, author of *Outliers*, the combination of his skills, work ethic, and a special opportunity made Bill Gates an “outlier”, an exceptional person who changed his industry.

The technology revolution started by Gates has transformed business, creating vast opportunities but also a new set of risks that must be identified and addressed to ensure positive business outcomes. As a result, today’s CISOs stand at the intersection of business innovation and Information Security. This is our “special opportunity”.

CISOs are increasingly asked to come out of the IT department and participate in executive conversations. CEOs and CFOs are not going to give anyone additional business influence without first being confident in that person’s ability to positively contribute to the organization’s strategic goals and objectives. Like Gates did for the computer industry, our industry’s “outliers” will seize this special opportunity in front of them, and do the hard work to understand their value and deliver on a vision that aligns with business goals.

James Bradley, the best-selling author of *Flags of our Fathers*, spoke at our recent CISO Leadership Summit about value and vision. Bradley told us that more than 30 publishers turned him down before one publishing house agreed to sign him. His book became a national best seller. Through all the rejection, Bradley never lost focus. He strongly believed in his vision and the value his story would bring to all those who had seen the image of American soldiers raising the flag on Iwo Jima. While he was absolutely committed to his vision, he was flexible in adapting his story to achieve success. At each of his first 30 meetings, he left with a “no”. But many of those “no’s” came with advice or suggestions. He took those suggestions and perfected his work. As he evolved his story its value increased, but his vision remained steadfast. As a result, the 31st publisher said, “yes”.

Bradley asked the CISOs gathered at our summit to assess their own value to their organization and to define their vision. He encouraged them to seek feedback on their plan from other executives inside the company, and to be open to incorporating the suggestions to ensure their vision comes to fruition. Those who succeed at this endeavor may just be the “outliers” who advance Information Security.

In this issue we look out to the horizon and ask what is next for our industry. What skill set will our future leaders possess? How will they fit into the enterprise organization of the next ten years? In the following pages leading voices from our industry and academia posit to define our future.

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

Clarity in Next Gen Endpoint Security

BY KEVIN POUCHE, COO **PART** THREE

The K logix Information Security Services team has completed a six-month analysis on the Next Gen Endpoint Security marketspace and subsequently delivered the results to over fifty organizations.

WHY? Today, it is vitally important for clients to define what endpoint security means to them in order to identify the appropriate solution for their organizations business needs. The market is still emerging, and therefore difficult to navigate, which is why we undertook this in-depth analysis, following our proven methodologies, to help clients make strategic and more informed decisions.

Here is what we learned from our first fifty Endpoint Security Market Evaluation meetings:

ENDPOINT SECURITY IS A TOP PRIORITY FOR CISOS. THEIR TOP CRITERIA IS...

1 EFFICACY: A solution must have high security efficacy

2 PRODUCTIVITY: A solution cannot impact the end user

3 CREDIBILITY: There must be no negative impact on security leadership

TRADITIONAL ANTI-VIRUS IS NO LONGER ENOUGH...

CISOs believe their current AV solutions are only 30-50% effective against advanced malware

90% of these CISOs plan to spend budget in 2016 on a **Next Gen Endpoint Security Solution**

AND THEY HAVE TROUBLE IDENTIFYING THE RIGHT SOLUTION...

75% of CISOs admit to being confused about how Next Gen Endpoint Security vendors differ from one another

K LOGIX PROVIDES CLARITY.

Over 90% of organizations that have seen our Endpoint Security Market presentation have asked K logix to participate in their decision making process.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

TIM CALLAHAN

CISO, **AFLAC**

HEADQUARTERS: COLUMBUS, GEORGIA

EMPLOYEES: 8,000 EMPLOYEES & 17,000+ INDEPENDENT AGENTS

ANNUAL REVENUE: $23 BILLION

In a business where one misstep can have serious consequences, it is no wonder that Aflac CEO Dan Amos has prioritized as strong a security program as possible. Take a look at Target and Anthem, two recent examples of what can happen if your system is hacked by unscrupulous criminals intent on damaging your brand. One thing has become increasingly clear, and that is that every company falls under two categories: those who have been breached and those who will be.

Aflac, the leading provider of voluntary insurance in the nation, takes its brand seriously. To that end, each and every employee feels like an ambassador of sorts – a protector of the company's hard-earned reputation.

> Our clients and the brand are inseparable, which has built a lot of synergy for our program.

"The employees here really take our brand personally. Everyone wants to protect it. It is among our most valued assets," said Tim Callahan, CISO at Aflac.

Callahan believes that the respect employees have for Aflac's image, one of the most recognizable brands in the United States, is a major contributor to the success of the company's security program.

"Our clients and the brand are inseparable, which has built a lot of synergy for our program," he said.

Aflac is consistently ranked by the Ethisphere Institute as one of the World's Most Ethical Companies, a designation that truly matters to the employees. Callahan sees his mission as CISO as doing everything in his power to help prevent a security issue from negatively impacting the company's record for ethics and accountability.

"I know people at Target, and the employees there value that brand as well. They took it personally when the company's data was breached," he said. “So when I hold awareness talks, I explain to our employees that as a well-trusted brand, more is expected of us. Client expectations are very high.”

According to Callahan, employee commitment to the brand and client trust are key components of security awareness. When employees see the importance of security in building that trust and protecting policyholders, they are more inclined to demonstrate the faith Aflac needs to provide the best services in the industry. A trusted relationship, built over time by always treating customers and partners with respect, has helped Aflac provide data security. In fact, Callahan says that the company regularly conducts social engineering tests and takes great pride in how well employees perform.

COMMITMENT TO SECURITY STARTS AT THE **VERY TOP**

As with any important initiative, success often hinges on executive buy-in. After a recent briefing about the issue, CEO Dan Amos proposed a security contest for employees as a means to maintain momentum that had been building with regard to ensuring data security. The contest ended with a generous reward for the best cybersecurity recommendations.

“We had some great ideas, including the creation of a Security Ambassador program comprised of volunteers from various departments who take on additional training and act as a liaison between the security team and the business unit,” Callahan said.

The Aflac team performs a number of standard security awareness programs within their “SAFE” program, which stands for “Security Awareness for Everyone” and is represented by a rendition of the famed Aflac Duck with a safety logo and uniform. The program includes lunch and learns, entertaining video clips and one-on-one educational sessions.

“We teach them how to protect themselves at home, and of course, all of those practices are transferrable to the workplace as well.”

Callahan meets regularly with the executives at the highest levels in both the U.S. and Japan. He co-chairs the Global Information Security Council and the U.S. Information Security Oversight Committee (ISOC) for the company. These two groups include senior leadership members such as the deputy general counsel, CIO, head of audits and chief compliance officer. Callahan meets at least monthly with the U.S. ISOC, at which time they review risk and policies.

SECURITY REQUIRES INDUSTRY-WIDE **COLLABORATION**

Callahan spent many years in the financial services industry and was one of the early members of FS-ISAC:

“We share information about preventing attacks, and from there each company is able to act on the intelligence within their own environment. I see retail and health care starting to adopt some of these best practices as well, and it is a good thing.”

In an industry like insurance, where any company can be the target of the actions of criminals it’s hard to argue against keeping data security at the top of everyone’s priority list.

> “We had some great ideas, including the creation of a Security Ambassador program comprised of volunteers from various departments who take on additional training and act as a liaison between the security team and the business unit.”

PROFILES IN **CONFIDENCE**

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DEB STEVENS

CSO, **TUFTS HEALTH PLAN**

HEADQUARTERS: WATERTOWN, MA

EMPLOYEES: 2,400

ANNUAL REVENUE: $4 BILLION

> “I am able to get the budget I need because I approached security as enabling the business lines in addition to meeting regulatory requirements. My job is to demonstrate what we need, when we need it based on what the risk is, and how security would enable the business”

ENABLING THE BUSINESS AND **PROTECTING DATA**

Deb Stevens is the CSO at Tufts Health Plan, a Massachusetts-based organization known nationally for offering high quality health plans. Serving all segments of the population, Tufts Health Plan’s private HMO/PPO plans received a “5” – the highest rating possible – from the National Committee for Quality Assurance (NCQA)*. Only eleven plans across the country achieved this rating. Their Medicaid plan received a 4.5 out of 5. Tufts Medicare Preferred HMO and Senior Care Options plans earned 5 out of 5 stars from the Centers for Medicare and Medicaid Services as part of its annual Star ratings for 2016**. Only twelve plans across the country achieved this rating.

Before the time of formal information security programs, Stevens worked in organizations to protect intellectual property for technology and clinical trials companies. “Early on in my career, my work was all about enabling the business and protecting brands at the same time,” she explains. While computers and any technology came very easy to Stevens, she was given opportunities to learn a variety of business verticals and technology and holds certifications in many security areas.

Stevens' keen leadership and business skills allowed her to quickly establish a successful cybersecurity program at Tufts Health Plan. "I have a passion for protecting data as well as reducing the risk to the company brand," she says.

Her passion enables her to work seamlessly across the business with leaders. Understanding the business strategy allows her to align the security strategy, which translates into her to receiving requested budget and resources. She comments, "I am able to get the budget I need because I approached security as enabling the business lines in addition to meeting regulatory requirements. My job is to demonstrate what we need, when we need it based on what the risk is, and how security would enable the business."

Not only does Stevens meet with the Board members to educate them on the security posture, but she also updates them on a regular basis. "I think about my audience when presenting to the Board and I make sure that I am not supplying them with data points that don't matter to them, something many security executives make the mistake of doing," she explains. They are required to be aware of the security posture of the company including risk are very interested in where we are going and what is needed for the future.

THE PEOPLE-SIDE OF **SECURITY**

"Everyone has been talking about the shortage of security professionals, which is nothing new. I have taken the approach that we need people who have soft skills and emotional IQs, so they have strong business acumen and are technically sound," Stevens explains. The cybersecurity program works within their security team to further develop this important set of skills. The goal is to truly understand the business they are working in, so they design solutions that ultimately enable the business. Innovation has played a major role in this program, because Stevens believes that being an innovative thinker is a key characteristic of a strong leader. This program is based on a model set up by Stanford University called "Design Thinking".

This November, Tufts Health Plan hosted its 19th annual cybersecurity awareness day. "We can clearly see in some areas, a 50% improvement [in security awareness], which is tremendous," Stevens says. By using creative ways to attract people, such as raffles and giveaways, many employees are able to benefit from learning about security for both their professional and personal lives. At Tufts Health Plan, awareness is not limited to one day; Stevens conducts ongoing education, whether her team is speaking at various department meetings or if employees take computer based training on the subject.

THE FUTURE IS **NOW**

"The future is now. CSOs need to understand the business and enable it. Thinking in a strategic fashion is absolutely required," says Stevens. She believes an innovative mindset paired with innate problem solving capabilities in addition to managing risk are essential skills needed to be a leader.

As security leaders move further into board room conversations, CSOs must also prepare for these discussions. Stevens recommends preparing for questions about current and future resources and risk to your organization. She states that you need to align and differentiate what enables business versus regulatory compliance. Maintaining a vision and having a conversation with board members enables them to make decisions on risk, according to Stevens. Being well prepared to answer any question is a must.

Collaboration on threats now and in the future will remain constant to managing loss of data. Everything is connected. For example she purchased a vehicle this summer and received a USB drive to patch security vulnerability two months later. Who we are as people, our identities, roles and relationships to devices and other resources will become simplified.

* The National Committee for Quality Assurance (NCQA) Private Health Insurance Plan Rankings 2015-2016
** NCQA's Medicaid Health Insurance Plan Rankings 2015-2016

DEFINING OUR FUTURE **SECURITY LEADERS**

BY STEPHANIE HADLEY, CONTENT MARKETING MANAGER

WE ASKED CISOS AND INFORMATION SECURITY PROFESSORS WHAT THEY THINK THE MAKE-UP OF A FUTURE SECURITY LEADER WILL LOOK LIKE.

THE RESULTS ARE IN.

WILL AN MBA DEFINE OUR FUTURE SECURITY LEADERS?

What if I told you the next great security leader was a broadcast journalism major teaching high school students about video production last year? Are you dubious?

In our year-long conversation with current CISOs at enterprise organizations, the definition of a perfect security candidate has begun to emerge. Over and over again we hear CISOs say they are looking for team players who are strong communicators and advocates for security. They seek people who are capable of leading a discussion, and explaining the value of security in a simple and clear manner. Strong communication and business-savvy skills take priority over technical mastery. So, is a broadcast journalism major who teaches high school students really that unorthodox as a security leader?

This broadcast journalism student embodies all of the skills our future security leaders will need, according to her professor, Dr. Corey Schou, PhD, University Professor of Informatics, and a Professor of Computer Science at Idaho State University. Dr. Schou is also the Director of the National Information Assurance Training and Education Center at Idaho State University. The Center is shaping the next great set of security leaders via a partnership with the Federal Government. In exchange for a commitment to serve in the Federal Government, students in the program receive a scholarship to one of the nation's first security-focused MBA programs. The two year MBA program, which requires all of the traditional MBA coursework plus extensive time in Schou's security lab, makes passing the Security+ test and CISSP certification a requirement. After serving in the Federal Government, Schou reports most of his students have achieved CISO-level agency positions within five years and students are free to take their MBA and vast hand-on experience to the private sector.

BE PREPARED

WONDERING WHO WILL BE CISO IN 2040?

You might want to check your local **Boy Scouts of America** organization. Professor Schou reports that in his program more than 80% of all his students were in the Boy Scouts or an equivalent scouting program, such as the Girl Scouts. Boy Scouts are taught to be leaders. They are knowledge seekers, able to adapt to any situation and capable of addressing challenges as they present themselves. Sound familiar? Security professionals are wise to adopt the program's motto, "Be Prepared".

THE VALUE OF AN MBA IN INFORMATION SECURITY

Just four years ago, 3 out of 4 CISOs said an MBA was not needed to be an effective CISO, according to an informal survey by The New School of Information Security. While it still may not be a requirement, business skills are an increasingly larger part of the equation for a successful CISO. Professor Schou states, "If a security project is necessary, you don't have to explain that to another computer geek in the company, you have to explain that to senior management, and to finance. So we make {our students} learn finance." When it comes to carving out an executive management position, Schou says, "You have to have business skills or you will forever be a technician."

In addition to Idaho State, other Universities are now providing technical students with the business skills they need to be CISOs, and providing business students with critical Information Security knowledge. Bill Clements, Dean at Norwich College, which has a nationally recognized cybersecurity program says, "Cyber awareness is a contemporary issue and we need to be educating all of our students about it, not just those in our information security program." James Madison University, Worcester Polytechnic Institute, and several other universities also offer graduate level course work or MBAs focused on cyber security.

TRANSLATING ACADEMIC TRAINING TO BUSINESS SUCCESS

Many of today's cybersecurity practitioners lack formal training or security-focused degrees, and have had to learn on the job. In large part they have been able to tailor the role to fit their unique skill set within the IT organization. Increasingly, the CISO role has gained prominence, with greater access to the executive team and the Board, and greater visibility within the company as a whole. With greater visibility, expectations for the role have increased as well. Executives now expect the CISO to participate in strategic conversations as a business leader with technical acumen. CISOs, like those who attended our CISO Leadership Summit, are making significant advancements in moving the security conversation from one of technology tactics to risk-based business strategy.

Young security professionals have an advantage in that critical success factors of the role have been articulated for them. While learning on the job will remain an essential component of CISO training, they will also benefit from years of classroom-based education and review of the case studies that came before them. Those emerging CISOs who are able to relate security practices to business goals and correlate security functions to business risk, will be the professionals most likely to be welcome in the Board room and become the next wave of security leaders.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DARREN CHALLEY

VICE PRESIDENT ENTERPRISE INFORMATION SECURITY, **EXPEDIA**

HEADQUARTERS: BELLEVUE, WA

EMPLOYEES: 14,570

ANNUAL REVENUE: $5.7 BILLION

THE DIFFERENCE BETWEEN **A LEADER AND A MANAGER**

During his four year tenure as Vice President of Enterprise Information Security at Expedia, Darren Challey retained a team of top caliber talent in an increasingly competitive market, improved capability of delivery, and increased transparency.

Some of this success may stem from his firm belief that he is not just a manager of employees, but he strives to be a leader of people. It is a concept he recently presented at an Evanta event. “I want our team members to feel that I’m approachable, and always have both their best interests, and our company’s, at heart,” he explains. Challey avoids getting wrapped up in a role or title, and focuses on relationships, allowing people to feel valued and empowered, not just like cogs in the proverbial wheel.

I want our team members to feel that I’m approachable, and always have both their best interests, and our company’s, at heart.

During his Evanta presentation, Challey spoke about the importance of making deposits to an individual’s “emotional bank account,” where people store and retrieve trust. “From my point of view, when I started at Expedia, my account was already in a deficit because no one knew me or trusted my role, and because of the prior ways our team and leaders had operated,” he explains.

To make “deposits” into the emotional bank accounts with stakeholders, Challey started showing up at their offices to simply ask how he could help. While it took time to rebuild each positive “balance,” he understood his objectives and trusted his approach. To further increase the “balance” with both stakeholders and the team, he carefully scheduled recurring meetings to address concerns, educate and ultimately forge and maintain important relationships.

> “AN EFFECTIVE LEADER HIRES TALENTED PEOPLE WHO ARE CAPABLE OF IDENTIFYING AND SOLVING COMPLEX PROBLEMS - THEN GETS OUT OF THEIR WAY, SO THEY CAN BE GREAT AT WHAT THEY DO BEST.”

He often jokes that a leader’s greatest ROI is the simple act of taking a key stakeholder out for dinner or drinks. Taking the time away from the office to get to know someone and to understand each one’s goals is time well spent.

STEPPING TOWARD THE **BOARD ROOM**

While Challey currently has no direct visibility with the Board Room, he recognizes this challenge and plans to work on ultimately achieving this level of responsibility. “Eventually, as a leader I need to be directly accountable to the Board of Directors,” he explains. Even with a lack of face time in the Board Room, Challey is satisfied with the level or support and budget he is given. “I don’t feel that budget is a constraint,” he says, “I know that my leadership is engaged and they actively support me, our team, and our mission.”

EDUCATION INCREASES **RETENTION**

Challey is most passionate about educational opportunities. He says, “I often explain to my finance counterparts why my team members have to take certain workshops or classes beyond what is customary for IT. From my point of view, education is essential for personal growth, and it’s also a great retention tool, especially in information security because it is moving so fast.” Challey uses education to reward his team members and allows the top talent at least one to two weeks of training each year. By investing in human capital, Challey is able to retain people by increasing their value, and job satisfaction. Making every person on his team more valuable at the end of the year, so they choose to stay (and are not forced to stay), is one of his primary goals as a leader.

FOSTERING A SENSE OF **COMMUNITY**

Even in informal settings, Challey gets together with like-minded leaders, and occasionally their spouses, for dinner to foster friendship, trust, and collaboration. “At the end of the day, we should share knowledge that could help us each be successful in the areas we are most concerned about. We face similar challenges and common adversaries who are already exceptional at information sharing. We know this is a highly asymmetric contest because we as the protector must account for all pathways, while the attacker only needs to find and exploit one gap in the defenses.”

Challey believes a powerful exercise is to learn from the experiences of CISOs at other organizations to help understand what works, where to focus, and how to best communicate at all levels. As security leaders, Challey says the most important thing to do is ask the right questions at the right time; he explains, “The question I find myself asking most often is ‘what is the problem you’re trying to solve?’” This surprisingly simple question can lend great clarity and purpose for teams that may be intent on deploying a technology or program — without really understanding the goal.

According to Challey, an effective leader hires talented people who are capable of identifying and solving complex problems – then gets out their way, so they can be great at what they do best.

PROFILES IN **CONFIDENCE**

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

SUMIT SEHGAL

CISO, **BOSTON MEDICAL CENTER**

HEADQUARTERS: BOSTON, MA

WORKFORCE: 10,000 +

ANNUAL REVENUE: $4.1 BILLION

TODAY IS ABOUT **PEOPLE**

Sumit Sehgal, the CISO at Boston Medical Center (BMC) has seen many changes in the last ten years in Information Security. “Years ago, the priority was to set up point security solutions to get an adequate idea of what was going on in your network. Over time, the focus for me was less on tools and more on how we influence and change behavior to improve security – the human side of security.”

Sehgal and his team do not rely on presentations and “top down” security awareness training. They work to make security more relatable and personal for the workforce at BMC. “We give them a choice, and we engage with departments to customize training to their interests, needs, and requirements.” He believes they are more receptive to the training, creating effective results. “Each member of the workforce has the option to complete 3 out of 5 security training modules per year, allowing them their own choice,” he says. The modules focus equally on security at home and security at work, including topics like social media and cyber bullying. When the workforce learns about things that apply to their personal life, it increases their engagement in what they need to learn professionally.

He also believes it is important to partner with organizational influencers, not just executives and business leaders. “Find those people who have an infectious cloud around them, and engage them. They will help foster the message in the community. When it is presented this way people take security precautions because they want to, not because they have to do so.”

THE FUTURE: **CONTEXTUAL ADAPTIVE RISK**

While people will always be the most important part of the security equation, Sehgal states that emerging technology will play a big role in the next evolution of security. He is interested in the impact technology innovation will have on the future of security efforts, specifically whether artificial intelligence technology has the ability to help with contextual adaptive risk, or the idea of real-time awareness of the specific risks data is exposed to at any point in time. Sehgal believes the next innovation will be security systems agile enough to communicate changes to the risk threshold based on changes to the data in the environment.

HOW TO GET **THINGS DONE**

Sehgal has this advice for newcomers to the CISO role:

PRIORITIZE

Focus on no more than two priorities at a time. “Anything more than two priorities is too noisy. Some organizations do not even have the appetite to address two, maybe one is all they can handle,” says Sehgal. Also, be flexible and adaptable with your priorities. Sehgal suggests aligning your priorities with business goals. If priority number three is a bigger priority for other executives in the company, then work to achieve that goal, because it is likely to help you in the long run, both with your other priorities and to engender loyalty and trust with the other executives.

INFLUENCE

“Take the time to know who the influencers [in your company] are. Talk to peers, talk to leaders, and network with the people who make stuff happen. Once you have established their trust, they will help you.”

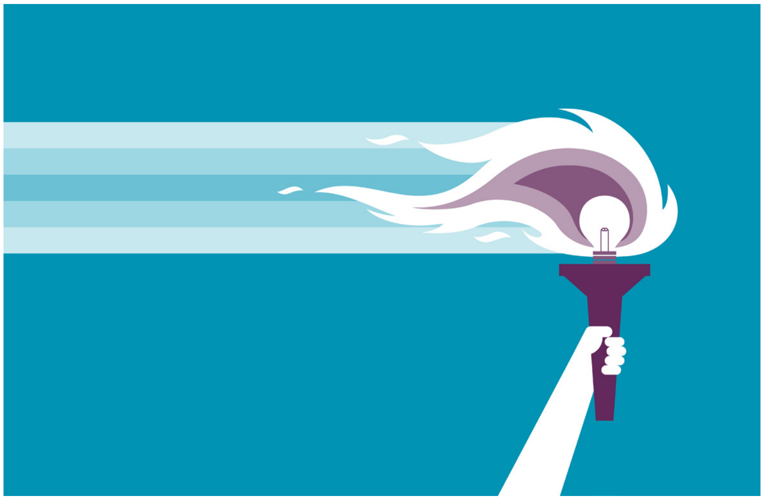
ROADMAP

CISOs that need a guide for their first 100 days should look at the SANS 20 CSC as it is a good roadmap of things to think about and evaluate. “SANS covers the breath of everything a CISO should consider from a control perspective and it will help you prioritize your efforts.”

KEEP CALM & REMEMBER WHY

“I have had very good mentors from a leadership perspective. They helped guide me and understand how the business functions. I’ve been in healthcare my entire career. My mentors helped me learn to focus less on the minutia of security and instead remember why we are doing this. We do this because someone is getting treatment here. We need to care for them, and part of that is safeguarding their personal information. Stuff [incidents] happens. Things break. People will get upset. Focus on the solution, not the anger. My first motto is ‘keep calm.’”

IN YOUR OPINION



QUICKFIRE Q&A WITH EXPERTS

Sumit Sehgal
CISO, Boston Medical Center

HOW DOES SECURITY IMPACT REVENUE?

Align with Business Projects from the Outset - When you align security with projects from the outset and you align governance to those projects, then you are building security into those frameworks. When you provide a method by which the way information flows from Point A to Point B to achieve a business function in the quickest and most secure manner, you are providing revenue impact. You positively impact revenue by taking away the traditional security controls that would have put hindrances or road blocks on processes.

WHAT WILL A CISO LOOK LIKE IN 5 YEARS?

The CISO Will Not be in IT - About 5 years ago [Cooper University Hospital] came to the realization that information was the second most valuable asset we had, after employees. So once they (the executives) saw that information was the lifeblood of the organization, they considered what we are doing to protect patient information and keep it proprietary. They looked at structure of the health system. They made the determination - with gentle nudges - that Information Assurance should be on the same level as the CIO.

Phil Curran
Chief Information Assurance Officer, Cooper University Hospital

Robert Duncan
CISO, Euronext

WHAT WILL A CISO LOOK LIKE IN 5 YEARS?

The CISO Might Not Exist – If security as its own department doesn't disappear altogether it may be much smaller. Security will not go away but you will see security layered into every business department. The Security Ambassador program that many organizations are building out is a first start to this concept.

WHAT ONE THING WILL HAVE THE BIGGEST IMPACT ON INFORMATION SECURITY IN THE NEXT 10 YEARS?

Government & Private Company Partnerships - The government can bring scale to the issue of cyber threats and tracking. Certain things will be handled via a back line to the government. Private threat exchanges exist [today] across some industries, like financial services. The government will expand on those and provide more information to companies across sectors.

WHAT WILL **SECURITY** LOOK LIKE IN **2025?**

What innovations can we expect in 2025? How will information security shift? We asked experts about their thoughts on the future of information security.

BY KATIE HAUG, DIRECTOR OF MARKETING

JOHN PESCATORE, DIRECTOR, EMERGING SECURITY TRENDS, SANS INSTITUTE

One key area will be to have meaningful security metrics that can be related to business impact. Let's look at the retail industry - the oldest vertical that was around way before any technology. Retail has a history of metrics around crime and theft, essentially security incidents. With over 100 years of statistics, retail has been able to settle on what a reasonable business loss is due to shrinkage (shoplifting, employee theft, etc.). This is around 3%, meaning 1.5% of revenue to keep shrinkage down and a loss due to shrinkage of 1.5%. CISOs need to be able to track similar metrics for cyber theft impact.

In 2025, CISOs will still be putting out fires like they are today, but they must connect what they are doing in security to the impact it has on business. Shoplifting has not changed much over the years, however in cyber security, not only do threats change, but technology also changes, so we must have an adaptive process. The real key is making that connection to the business bottom line and focusing on things that will protect the business from negative impact and enable the business to focus on their objectives.

JAMIE HERMAN, CISO, GELLER & COMPANY

CISOs need to balance operational efficiencies with future deliverables, which is a challenge given the lack of security professionals available to fill open roles. Michael Brown, CEO at Symantec was quoted as saying "The demand for the (cybersecurity) workforce is expected to rise to 6 million (globally) by 2019, with a projected shortfall of 1.5 million." A large portion of that shortfall can be attributed to not just a lack of security talent in the workforce, but also employee retention, continuity within the security team, and professional development within the organization as a whole. Retention and employee development are fundamentals that CISOs should have their eyes on when planning their departmental growth strategy in alignment with the business.

There are a lot of talented people across other departments that really understand the organization and its operations, who with some technical training can be amazing welcome additions to the security team.

SCOTT SUMNER, CISO, TORY BURCH

In the past, in a lot of organizations, security was an afterthought and brought in as a reaction to something happening. At times, it was difficult to justify to business stakeholders for security investment, until something that actually impacted the business occurred. Due to the recent high profile breaches, we are seeing a lot of organizations stepping away from this, and involving security as a stakeholder in the business.

In the future, security needs to come in at the ground floor and make sure is it part of the architecture and business decisions. As we look to the future, security must think about their 3-5 year plans and lay out a strategy that is supported by the Board. These types of leaders will communicate with different business channels and have a visible presence in the business.

Looking ahead, security awareness will also evolve into more than just making people sit at a computer and watch a video or hang a poster. Security needs to be present, not only in the business itself, but in forums where decisions are made. This will help install a sense of responsibility for everyone to protect the assets of an organization.

PROFILES IN **CONFIDENCE**

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

CHRIS DUNNING
CSO, **AFFINION GROUP**

HEADQUARTERS: STAMFORD, CT

EMPLOYEES: 3,700

WHAT IS IN A TITLE? THE DIFFERENCE BETWEEN A **CSO & CISO**

Christopher Dunning holds the title Chief Security Officer, instead of the more common Chief Information Security Officer, at Affinion Group, one of the largest providers of customer loyalty programs. He explains the difference between the two roles, “A CISO lives in the IT department, whereas a CSO influences all aspects of security – from information security, to privacy and physical security. A CSO is a peer to the CIO, while typically a CISO reports into the CIO.” It makes sense to Dunning that Information Protection or Security is run outside of the IT department, he states, “security is not just a technical problem, it is also a business challenge. It cannot be solved with just a technical solution. You have to also take a business-centric approach.”

With that being said, Dunning has a strong working relationship with the CIO and other leaders in the company. “Without good communication between the C level executives, it may become a battle of command and control. In my first days here, I sat down with many of the leaders and asked about their risks and concerns. I established myself as their consultant, and made sure to include legal, HR, and Internal Audit .”

> “There are two camps when it comes to employees and security. Some believe that people are the biggest threat, and others believe that people are the best security asset. I say to the workforce, ‘raise your right-hand and be deputized.’ I would rather have 3,700 security deputies than just my security team members tasked with making sure that 3,700 people do not make a mistake that exposes the company.”

The Future: Security Takes the Lead

"I think that five or ten years from now, CISOs will be much more involved with the actual defining and development of business solutions, instead of being at the tail end of the development process, where we often are today. It all comes down to how quickly businesses need to move in order to be successful." Dunning has some experience in this type of security-led development. In an earlier role as Director of Information Security for a Fortune 500 retailer, his team worked with the development team to create a security-aware development process.

FINDING THE RIGHT BALANCE IN **REPORTING**

Dunning's goals are to protect the brand and shareholder value, right-size the security efforts to provide appropriate defenses, provide a security program that meets the needs of the business, and protect critical data, applications, and systems. The organizational structure matters when it comes time to gain executive level mindshare and buy-in to help him achieve these goals. "As CSO, I report into the COO and participate in monthly status meetings with the CEO," he says.

Dunning states that many CSOs are challenged with reporting and presenting metrics that resonate in these executive meetings. Over a number of years spent in several security leadership roles, and with input from mentors, Dunning has fine-tuned his status reports for leadership. However, he believes that even his current reports provide more information than the executives are able to digest. "The bottom line is to keep it simple. There are so many granular issues with risk management it can be like boiling the ocean. I take a very simplistic view when reporting at the senior level. I ask, 'Are you solving a business problem or just reporting on results?'"

Dunning reports on four categories: Security Incidents, Compliance, Vulnerabilities, and People. Brevity and clarity are keys to his presentation. "My goal is to produce a one-page status for each that could be understood by anyone." His one-pagers include:

- Security Incident Response 'The First 48' - a monthly security incident report that documents all security incidents that have been reported, evaluated, and responded to following the first 48 hour process.

- Compliance Tracker - an overview on the company's status with PCI, SOX, and other compliance mandates.

- Vulnerabilities Quadrant - a method for tracking existing and remediated vulnerabilities and risk.

- Security Awareness Calendar – a high-level view of on-going employee security training and awareness activities.

NO BOARD VISIBILITY, **NO PROBLEM**

Dunning reports he does not meet regularly with Affinion Group's Board of Directors. "Is there a strong interest in security from the Board? Yes, it is a very strong interest," he says. Even with this interest, Dunning does not have an annual meeting on the calendar, although he does meet as needed with the Audit Committee and speaks regularly with the CEO. "There is a process in place for the Board to be updated on security through the Audit Committee and the CEO. I think it makes sense to have this reporting structure. If they need me, then I am here as their consultant," says Dunning.

Advice from a Veteran CSO

Because he has almost 30 years in the security industry, and two CSO roles under his belt, we asked Dunning for his advice to newer CSOs. He states, "First, establish the behavior of yourself and your team. A successful security organization is not just comprised of engineers and architects, but consultants. You will have engineers and architects on your team, but everyone should be acting in the role of a consultant. The security team has to be available to help their peers solve business problems with security solutions. Getting involved in these discussions as early as possible is always a plus!"

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

MARK OLSON

CISO, **IRON MOUNTAIN**

HEADQUARTERS: BOSTON, MA

EMPLOYEES: 17,000

ANNUAL REVENUE: $3 BILLION

ELEVATING THE **RISK CONVERSATION**

Mark Olson, CISO of Iron Mountain, took over the role from his predecessor with the initiative to transform the conversation with executives and align security to the business. With an established information security program already in place, Olson had a comfortable transition into the role. He immediately sought to direct the conversation away from one of being attacked or compromised, to instead an important discussion about risk. "The programs were well in hand here and working when I came in, so it was really how I could elevate the awareness level to the executive team," says Olson.

Olson is involved in conversations about cyber insurance policy levels, revenue levels associated with business, the impact in customer volume, and how these risks may affect business proceedings. This risk conversation has become a true driver for ongoing projects and changes to infrastructure. To accomplish this conversation, Olson's team uses an enterprise risk management system that tracks risk from a business perspective. "I always go back to this risk position and include business revenue and cost in it. I then take all of this material and add it to the application, making this system the single point of reference," says Olson.

Reporting to the CSO and working closely with the CIO, Olson meets regularly with the Risk and Safety committee of the Board to provide them with a high-level view of the most critical risks, details on the remediation of these risks, and a running commentary on long and short term projects. While most Boards hear from the CIO, Olson states that is not the case at Iron Mountain, "The CIO and I jointly present."

"I'VE BEEN EXCLUSIVELY FOCUSED ON RISK EDUCATION TO GET A SOLID POLICY IN PLACE AND ESTABLISH STRONG COMMUNICATION WITH THE EXECUTIVE TEAM SO THEY ACCURATELY UNDERSTAND WHERE WE ARE AND WHERE THE RISKS ARE."

“WHILE THERE IS NEVER ENOUGH TIME AND NEVER ENOUGH PEOPLE, THERE IS A BALANCE YOU NEED TO STRIKE, WHETHER AT A LARGE OR SMALL COMPANY, ABOUT THE CAPACITY TO MAKE CHANGE WITHOUT HAVING A DETRIMENTAL EFFECT ON BUSINESS.”

BOARDROOM **DISCUSSIONS**

“To characterize the questions I hear from the Board committee – they often ask questions to ensure we understand the problem and that we have an adequate solution to resolve or remediate risk,” says Olson. As CISO at Iron Mountain, Olson finds that these Boardroom discussions are really about executives getting comfortable with who he is, what he knows, and whether they feel he has identified the right things to help reduce cyber risk.

Olson believes the Board committee understands the value of security and sees the need for a dynamic security program to be in place. While this understanding is important, Olson knows that security is one of many issues the committee needs to consider in reviewing business operations. “The Board committee feels that security is important, but what is of overriding importance is if the company is being run effectively,” says Olson. This is why Olson has focused on enabling his security program to support business growth.

Olson ensures a productive, two-way communication with the Board committee by doing two things. First, he educates the Board in a clear, concise way by painting a business-focused picture and avoiding any tactical IT-intensive conversation. Second, Olson never speaks specifically about how he is getting a project done, he instead discusses crucial things he has identified, what programs are in place, and where he is within that program. Olson also produces a one-page metric chart comprised of projects and a coordinating color-system for their level of completion. “I always show the Board committee two basic charts which provide the status of public-facing infrastructure and key projects to provide an overall picture of the progress of the projects and their value to risk management.”

CISO **MATURITY**

As a second-time CISO, Olson has experienced the evolution of the role as it matures into a crucial tool for the business to position to customers. “Today, when we go out and talk to the customer base, we talk about the great offerings that we have and the good physical controls on warehouse space. Information security has become part of the sales cycle and a true value statement to our customers,” says Olson. He believes security has evolved into a direct relationship with business and has become part of the core operational decision set.

TECHNOLOGY VS. BUSINESS EDUCATION

“Educating my team on technology is not difficult. I make sure that everyone attends one major conference or training session per year, sometimes more, but that is our guiding principle. At these events, they receive a mix of networking with peers and education. To educate my team on the business side, it is something I continually try to reinforce. I always ask, ‘how is this going to affect the business?’ and ‘how is this affecting other projects around us?’ I keep encouraging them to think about the effect that everything they do has on the overall business. Having them compare their work to how they think about their personal home budget decisions has resonated well with them and I have found they value having an understanding of the part they have in the overall business.”

CISO LEADERSHIP SUMMIT

CISOs Focus on Leadership, Strategy, and Carving a Space in the Boardroom at K logix's first CISO Leadership Summit

Twenty-four CISOs from across New England came together at the Langham Hotel in Boston to spend the day collaborating, solving challenges, and encouraging each other to embrace their opportunity to take a higher-level, more strategic position in the Boardroom.

Leadership and Perseverance in the Face of Challenges and Doubts

James Bradley, author of the New York Times best-selling work *Flags of our Fathers*, set the tone for the event. Bradley's father was one of the soldiers pictured raising the American flag during the WWII Battle of Iwo Jima, the most reproduced image in history. Bradley decided to tell his father's story and his book was finally published after four years and being turned down 30 times. His perseverance paid off, as *Flags of our Fathers* eventually spent 46 weeks on the NY Times Best Sellers and later turned into a movie by Clint Eastwood. He believes the biggest factor in his success was his clear vision and determination. He had a story he knew should be told, and he was committed to finding a way to tell it. Security leaders can learn from his struggle and commitment as they struggle to educate the company and the Board on the value of their efforts.

Not a Sprint, Not a Marathon, a Journey

Michael Santarcangelo, a featured editorialist for *CSO Magazine* and a Security Leadership Consultant, led the leadership workshop. He reminded CISOs that security leadership is neither a sprint nor a marathon, but instead a journey. Santarcangelo stated that because security requirements are ever-evolving, the security leader cannot focus on a finish line, rather he or she must focus on the journey. Part of the journey is defining "value and vision" and communicating that to the organization. CISOs today need to understand their value to the business and be able to translate that value into a vision for how security can positively impact the company's goals. As the moderator for the event, Santarcangelo kept everyone focused on leadership and communication. Strong

"HIRE PEOPLE WITH A MISSION AND VISION THEY CAN CLEARLY ARTICULATE."

Chris Dunning (CSO, Affinion) & Kevin Pouche (COO, K logix)

CISOs and CIOs at the Langham Hotel during the Leadership Workshop

"THE BEST SECURITY AWARENESS TRAININGS THAT ENGAGE STAFF ARE THOSE THAT HAVE A MIXTURE OF PERSONAL/HOME SECURITY, ALONG WITH SECURITY IN THE WORK PLACE."

Steve Bartolotta (CISO, CHNCT), Jon Fredrickson (CISO, Southcoast Health) & Sumit Sehgal (CISO, Boston Medical Center)

"ALL TALKING POINTS TO THE BOARD MUST BE ASSOCIATED WITH BUSINESS OBJECTIVES THAT HAVE ALREADY BEEN IDENTIFIED."

Katie Haug (Marketing Director, K logix) & Anil Kapoor (ISO, Five Star Quality Care)

"IT IS IMPORTANT TO FIRST ESTABLISH TRUST WITH THE BOARD IN ORDER TO FACILITATE OPEN AND PRODUCTIVE COMMUNICATION."

Breakout Roundtables Gave CISOs the Chance to Share Challenges and Successes

CISOs Collaborating with CIOs. This roundtable spoke about trust and alignment when working with CIOs, and other business leaders in general. Trust is one of the most important factors in any successful CISO/CIO relationship because the two must work closely together on nearly every project.

Finding the Right Talent. Everyone at the roundtable was in agreement – there is a talent shortage in the security industry. CISOs emphasized hiring someone with a clear mission and vision that can be articulated during an interview. It is important to showcase how your organization is innovative in order to attract talented professionals. Also, making your plans for hiring known to the community allows for a broader talent pool.

Security Awareness Training. This roundtable spoke about how CISOs have shifted training from a corporate focus to a more personal one, as they realized the message of security awareness resonates better with employees when it impacts their personal life. CISOs invest training hours in topics like cyber bullying and how to protect your home in the age of the Internet of Things. CISOs also discussed the challenges of creating security awareness programs that are multi-cultural and will work in offices across the globe, with barriers of different languages, customers, and behaviors.

Making an Impact on the Business. This roundtable discussed understanding their role in the Boardroom and the need to clearly articulate their impact on the business. A common theme was emphasizing the importance to first establish trust with the Board to facilitate open and productive communication. CISOs need to find at least one ally to gain mindshare of the rest of the Board. Parallel to communication is strategizing to ensure security directly aligns with the organization's business objectives, which creates a solid foundation for positive interactions.

"THE HIGH CALIBER ATTENDEES PAIRED WITH RELEVANT AND THOUGHTFUL CONTENT, RESULTED IN A QUALITY EVENT THAT I WILL BE HAPPY TO ATTEND AGAIN."

If you missed our Summit & would like to attend another one, please stay tuned.

NYC & Boston Summits are coming up in 2016

Q&A WITH CHRIS QUINN

REGIONAL VP, CHECK POINT

We spoke with **Chris Quinn**, Regional Vice President of **Check Point,** to discuss future trends and innovation. Chris shares how Check Point secures the future with industry leading security products for Threat Prevention, Mobility, Firewalls, Security Management and more.

HOW DOES CHECK POINT **HELP CISOS**?

CISOs are tasked with the challenging job of going in front of the board to articulate risk levels, their process, and how their critical assets are being protected. We provide an extensible, solution-oriented approach across the entire enterprise and give them a clear vision into what is taking place today and what actionable things need to be done to augment their posture.

One of the biggest challenges I hear from CISOs is how they view incident readiness as well as the overall visibility they have into their environment. They often have lots of data, and the important question they ask is 'how do I make sense of all this data?' One of the compelling things we are doing is our ability to normalize data in a practical and highly relevant way. CISOs receive a status update and mapping of what is happening, in real-time, within their environment. This helps them understand how they can augment their security posture real time and drive results.

> "It is important to note that innovation is not just creating the next wiz bang feature! You need to integrate these solutions so they can operationalize in very efficient ways."

Recently, I met with the CISO of a large financial organization. He made it clear that they have a number of disparate technologies in play and one of the greatest challenges they see is how to operationalize across all technologies and drive measurable results. He said to me, "My sprawl in security is significant and there are so many "best of breed" technologies, but are they really "best of breed" from an operational standpoint?" We implemented a plan to coordinate his technologies better. We did this by giving clear visibility into what was happening in his environment and we made it actionable with controls that were easy to implement and manage. Think about it for a minute; if you have twenty interfaces to implement controls, are you really going to control anything? You need a lot of money; and many skilled resources that you know will be on the job for the long haul.

We can help CISOs by having a very objective dialogue; we have a lot of industry experience to offer and we have the pedigree.

WHY IS CHECK POINT CONSIDERED AN **INNOVATIVE COMPANY**?

Check Point has been an industry leader for 23 years and we have done this with an uncompromising focus on security and a commitment to our client's success.

We are in a 'get it done' business and focused on delivering extensible security solutions that are easy to implement, manage, and drive results. Our innovation today is leading the industry with revolutionary approaches; for example, we are the first to pass 'known good traffic'.

Why is this important?

Think of this example; most companies have a high volume of CVs coming in on a daily basis. Let's say for example, you are hiring a security expert for your organization. The job posting outlines all of the requirements for the job and also gives a hacker the ability to know what technologies you have in your environment based on the job description. The hacker can embed malicious content into the Word document and then begin to canvass the environment. What Check Point does in this instance is we sanitize the document with threats extracted and known good passed.

Another example of innovation is in the zero day arena; many are suggesting that sandboxing is being obsoleted by hackers and their advanced techniques. At Check Point, we are taking an aggressive approach that is centered on breach prevention. We are doing this with the threat extraction capabilities I mentioned and also our CPU level capabilities which disable the most advanced malware prior to it being weaponized in your environment.

'Get it done' innovation is what you get in our SandBlast solution and it can be leveraged via the cloud or on premise. The cloud is a very simple way for organizations to take advantage of these capabilities and transition from the world of detect to breach prevention.

> “ONE OF THE BIGGEST CHALLENGES I HEAR FROM CISOS IS HOW THEY VIEW INCIDENT READINESS AS WELL AS THE OVERALL VISIBILITY THEY HAVE INTO THEIR ENVIRONMENT. ONE OF THE COMPELLING THINGS WE ARE DOING IS OUR ABILITY TO NORMALIZE DATA IN A PRACTICAL AND HIGHLY RELEVANT WAY.

When I came to Check Point thirteen years ago, attacks were more nuisance-oriented, but today attackers are targeted in terms of approach, with varying degrees of motivation. Whether state-sponsored or organized crime, we have seen a tremendous uptick in the complexity of threats that are unique and targeted. Zero-day is the buzz, and this problem continues to be amplified by a much broader attack surface.

Take for example mobile devices; hackers are licking their chops at the opportunity to compromise these devices and find yet another way to harvest your data. Mitigating the risk in this area is another key area of innovation for Check Point and we do this with our Mobile Threat Prevention solution.

How real has this attack surface become? Look no further than the recent XCode Ghost attack. Apple has a very stringent certification and security process, yet many legitimate applications were compromised by this attack. Our innovation is focused on neutralizing these vulnerabilities and we are able to do this at the device, application, and OS level.

It is important to note that innovation is not just creating the next wiz bang feature! You need to integrate these solutions so they can operationalize in very efficient ways. Our innovation is also focused on delivering a solution platform that is portable, simple to implement, and drives results.

HOW WILL CHECK POINT CONTINUE TO STAY **A STEP AHEAD**?

One of the compelling areas we are staying a step ahead in, is looking at the ‘cat and mouse’ game going on in terms of malicious traffic taking place. I have talked about the importance of passing ‘known good’ traffic which comes via our SandBlast innovation. However, innovation also needs to be defined by the ability to implement solutions in an effective way. This is where Check Point continues to stay a step ahead; having software in our DNA gives us a great advantage as organizations leverage the cloud more and more. We can port our solutions quickly and effectively to address dynamic infrastructure requirements for elastic computing requirements in the public cloud via Amazon or Azure for example. Or we can provide the flexibility for organizations to automate security in their own private cloud scenarios. The bottom line is that we can create and will continue to create solutions that scale to meet the demands of the enterprise with security that is extensible, consistent, and easy to manage.

Want to learn more about Check Point?

Visit them at www.checkpoint.com

FUTURE OF SECURITY

It was recently Back to the Future day, so when I jump into my DeLorean, I look at my three kids and see the types of technologies they are gravitating towards. My daughter knew how to swipe through and play rudimentary games on my iPhone before she learned how to talk. This shows a huge catapult in terms of embracing technology, and over the next ten years, the Internet of Things is really going to take hold.

I love skiing and have a GoPro I like to use when I hit the slopes. There are now innovations like drones you can throw in the air that will film you as you go down a mountain. This embracement of technology is quite dynamic, whether it’s your ski drone, elliptical machine, mobile device, or something else, it is clear there is an exponential expansion on the attack surface. Overall, we can be certain that the definition of critical infrastructure is going to continue to expand.

Critical data will reside on these devices and from a personal point of view I have embraced the software approach because it is highly extensible. I know Check Point provides solutions to mitigate these changing risks because we have the ability to port solutions to the Internet of Things and when you think of Check Point now and in the future know this; WE SECURE IT!

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DARREN DEATH

CISO, **ASRC FEDERAL**

HEADQUARTERS: BELTSVILLE, MD

EMPLOYEES: 10,000 +

ANNUAL REVENUE: $4 BILLION

THE POWER OF **MENTORSHIPS AND COLLABORATION**

"One of the biggest challenges I've experienced is being given jobs that, at the start, were beyond my ability to do," says Darren Death, the Chief Information Security Officer at ASRC Federal. Previously the CISO for Governance, Risk, and Compliance at FEMA, Death recently transitioned to the CISO at ASRC Federal, where he is responsible for the Enterprise Cyber Security Program across a $4 Billion portfolio. Getting to where he is today required overcoming many challenges, something Death believes he accomplished through mentorship and collaboration. "Throughout my entire career I have been mentored, but many times when I was younger, I did not realize that this was occurring. Nowadays, I recognize the need and actively seek out mentors and the leadership of people who have done it before," says Death.

Death is no stranger to mentoring others either, and he actively participates in advisory councils, speaking engagements, and has taught a number of courses. He dedicated one year to the American Council for Technology – Industry Advisory Council's "Voyagers Program", a leadership development program for 'rising stars' in both government and industry who have a high potential for future advancement, and he currently holds a seat in their Mobility Working Group. Death has provided his mentorship skills for the SANS Cyber Foundations/Aces Online Program and has spent time speaking at highly regarded SANS Institute events. He has also spoken at the AFCEA, Digital Governance Institute, OWASP, and 1105 Media. For Death, any type of collaboration, whether it is amongst his team or with others in Information Security, is an intrinsic action for personal and professional growth.

Death is regularly expanding his network of peers and leaders, something he strongly values. He comments, “I do not believe in just networking within one’s own sector because there is the idea that a person in a different sector can be doing something that could help you and get you outside of your bubble.” He argues that reaching out across the United States and across sectors correlates to the evolving world that we live in today and specifically to his current position, where he works with many sectors including finance, healthcare, retail, energy, construction, and government.

MAKING **BUSINESS CASES**

The plentitude of Death’s mentoring and collaboration has allowed him to hold positions where he elevated security through making business cases. Making the case for specific security solutions is often times meaningless to the average person in the organization. Death comments that as a leader in the IT security field you need to be able to show how the security program adds value by protecting the organizations assets and continuing to keep the business operating.

Death has also learned that in order to function in the Boardroom, it is essential to meet with the business leaders and to market oneself. “I believe that the number one thing to do is marketing by hitting the streets, talking to all departments, and even speaking with customers. This is where you are going to find your advocates.” Death acknowledges that you are not trying to sell cyber security to these people, you are helping them see the value in how security affects business and you are aiding them in making intelligent business decisions.

> “I THINK THAT ONE OF THE BEST THINGS YOU CAN DO IS SURROUND YOURSELF WITH SMART PEOPLE, HOPEFULLY PEOPLE SMARTER THAN YOURSELF.”

THE ROAD AHEAD FOR CISOS

Death believes that the CISO position will be moving towards a heavier emphasis on business responsibilities. In most cases, he says that it will be the duty of the CISO to elevate themselves to this heightened leadership role. Although some CISOs may reap the results during the time they are at an organization, some may never see the results of the work they are doing, and it might only affect future CISOs in their role. “For many organizations, this is going to be a lot of hard work, it may not happen organically and some organizations may not see the importance. However, once they do see the importance, a switch will turn on and the CISO will easily make this transition,” says Death.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

FEATS OF STRENGTH

THE FUTURE OF
INFORMATION SECURITY

DECEMBER 2015

K logix
WWW.KLOGIXSECURITY.COM
888.731.2314