FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

CISO PROGRESS
Areas of Growth & Measuring Progress

NOVEMBER 2016

WWW.KLOGIXSECURITY.COM 888.731.2314

K logix
Earning the right to be confident in Information Security

FEATS OF STRENGTH

BY K LOGIX

PROFILES IN CONFIDENCE

FEATURES

LETTER FROM

KEVIN WEST

CEO

HOW WE MEASURED PROGRESS IN 2016

When I speak with CISOs about measuring progress, they often talk about their efforts to enhance their engagement in the Boardroom along with their impact on tangible and positive business outcomes. Some CISOs speak about making operational progress, such as improving proactive defense strategies.

When CISOs complete projects they should reassess their security programs, since the playing field has likely changed. With any type of project, the risk landscape is modified and affects the organization. This in turn means the approach moving forward must align to any changes. Each time CISOs complete a project, they earn the right to stop and assess where their program is, and where it is headed.

Some CISOs are already taking this approach. For them, tracking progress is an exercise in adaptability. Our industry simply moves too quickly to set specific plans for even a year out. DocuSign CISO Vanessa Pegueros tells us she is focused on agility and growth, just like the company itself, "We are a high growth, fast moving company, so I ensure we have an agile roadmap and planning horizon. Things can change quickly, so we must be flexible since new priorities and challenges can come from every business deal. One of my biggest realizations is instead of a one year roadmap, I narrow them down to the current quarter and two quarters that follow. I don't push my team to predict the future anymore."

When CISOs look beyond their own organizations, to the progress our young industry has made there is a lot of excitement and optimism for the impact security professionals will have on business in the next few years. For example, Steve Bartolotta, CISO at CHNCT says, "The major trend I am hearing about is that more and more CISOs coming out of the IT department. I would estimate 50% of my peers are no longer [coming from] IT, which is great." For Bartolotta and his peers though, it's not just about having autonomy outside of IT, it's about making progress with the Boardroom. "At every forum I attend, boardroom reporting and visibility is always at the forefront of discussions."

Within this *Feats of Strength,* we have reconnected with Pegueros, Bartolotta, and some of the other CISOs we profiled before, to understand the milestones they have reached in the last year, and how those accomplishments have changed their landscape. Also in the magazine, we profile leading CISOs like Corey Scott of LinkedIn, who says that, he is tracking internal and external milestones, and communicating them company wide, "We report on our performance to my direct manager and CEO, but also horizontally to the head of IT, legal counsel, the internal audit committee and engineering leadership. We want a lot of people to be aware of our organization's performance."

Security professionals lived 2016 at lightning speed, just like they have every year for the past decade or more. The pace of rapid change and innovation in our industry is staggering. The progress – both tactical and strategic - is dramatic, but there is still more to be accomplished. As our industry continues to move things forward, we must remain focused on our joint objective - to improve business operations through security innovations. With that objective as their focus, CISOs in 2017 will continue to amass milestones, reassess their posture, and make further advancements.

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

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT INFORMATION SECURITY PROGRAMS

JOHN NAI
CISO, PAYPAL

HEADQUARTERS: San Jose, CA

EMPLOYEES: 16,800

ANNUAL REVENUE: $9.25 Billion (2015)

"I don't need to convince the Board to make security a priority. They get it. At the executive and board level, we work to ensure they fully understand our security risk profile."

- JOHN NAI

"Our brand is built on the trust and security we deliver for our customers and merchants," said John Nai, the CISO of PayPal. "That means security is not as much a competitive advantage as it is a table stake. It is an absolutely crucial part of our service offering." Unlike many CISOs, Nai did not spend extra effort convincing his Board and executives about the value of security. He said, "When I sit on committees about building new products or applications, security is a consideration from the onset. I have an equal voice at the table with business unit and profit owners."

SECURITY-FOCUSED CULTURE

PayPal's security-focused culture lands Nai in front of the Board on a regular basis. During these meetings, he helps them understand many aspects of security, including the key measures his team takes to protect the brand. He commented, "I don't need to convince the Board to make security a priority. They get it. At the executive and board level, we work to ensure they fully understand our security risk profile. Transparency with the board and the executive team is critical. The more information we share with our teams about our risk profile, our defenses, and how we are being attacked, the better we are all aligned and the better we can maintain brand trust."

Innovation stems into PayPal's products and services, with a key goal of doing so in the most frictionless and enabling way possible. Nai and his information security team work hard to ensure this frictionless experience

> "We have the benefit of having massive scale in payment volume. We have 188 million active customers. From a security perspective we are in over 200 global markets. The scale in which we can do things is significant."

has a secure foundation. Nai said, "We are always walking the balance to make frictionless experiences that are highly secure. It is an ongoing dialogue within the company. Even though security and trust are in the DNA of PayPal, challenges still exist. We need to be an enabler and not a progress inhibitor. Too many security organizations think their role is to say 'no'. We say, 'no' when we have to, but we know our prime role is to enable the business."

SECURITY IMPLICATIONS FOR CUSTOMERS AND MERCHANTS

"In respect to threats, PayPal is similar to most companies in Payments and Financial services; we are under constant attack from bad actors, so we need to make sure the Board knows what controls and risk mitigation we have or need. The Board's understanding opens the doors for communication to all of our other communities. We start at the top level to get the support we need."

With an influx of people's personal information and financial lives online, many security implications arise for PayPal's merchants. In regards to his relationship and approach with merchants, Nai commented, "I engage with some of our largest merchants. They want to know what we are doing to protect ourselves and their business." He continued, "One of PayPal's value propositions is that we provide secure transactions. Clearly secure processing is core for our largest partners as well, so they want to know what we do, how we do it and how we ensure our brand promise of trust and security."

Merchants and customers have come to expect innovation from PayPal, something that extends to the information security team. Nai said, "We have the benefit of having massive scale in payment volume. We have 188 million active customers. From a security perspective we are in over 200 global markets. The scale in which we can do things is significant."

SECURITY OF THE INTERNET

"We look at security internally and externally. We build security into our own platform and we also help with security of the technology ecosystem. For example, PayPal was one of the founding companies behind DMARC email protection and FIDO for authentication. We were among the first companies to offer a bounty for uncovering bugs. So of course we look at security internally, securing our own infrastructure and apps, but we also take a leadership role securing the technology ecosystem in general for our customers and merchants."

Similar to other internet companies, PayPal invests heavily in security infrastructure and purchasing security firms to build out strong teams. In 2015, PayPal purchased the Israeli predictive malware detection firm CyActive. "That acquisition gave us their product, but also their talent. Now we have a large presence of highly technical security professionals in Israel," said Nai.

Nai's team, which includes hundreds of security professionals and 16,800 employees at PayPal who make security a priority, is set up to enable innovation. "Our team is spread out across three geographies. We have a core team in our San Jose headquarters and many security engineers in our Security Operations Center in Arizona. We also have a second Security Operations Center in Israel, so we have 7x24 coverage," Nai remarked.

HIRING EXCEPTIONAL TALENT

Even in a well-tapped industry when it comes to recruiting security talent, Nai acknowledged a clear advantage at PayPal. He commented, "The security industry knows that PayPal prioritizes security, and that is a great enabler for us when hiring exceptional talent."

The Silicon Valley culture is an important factor that contributes to his team's success and their ability to innovate. "One big thing for us is we participate in information shares, peer-to-peer working sessions in Silicon Valley. People think the region is competitive, but there is a lot of cooperation here, too. At my level, I speak with my peers about things like how to talk to the Board."

What is next for the future of PayPal's innovative ecosystem? Nai said, "It is hard to predict the future and how commerce will evolve overtime, but we are looking at partnerships with commerce in new contexts and how to protect that at the scale we need to do business. That is a phenomenal opportunity and there will be more innovation in the FinTech industry in general."

OPINION: SECURITY LEADERS SHARE 2016 TRENDS

There has been some shift from fear, uncertainty, and doubt, to a focus from Boards and the C-suite on spending more time proactively talking about cybersecurity. We still have a lot of work to do, but CISOs are starting to help the business and enable their mission.

- THERESA PAYTON, FORMER CIO, WHITE HOUSE

More of my peers are gaining a higher level of visibility with decision makers. In some cases, the reporting structure is changing so that they report directly to the CEO or COO, distinct from the CIO. Information security is starting to be viewed as a strategic business imperative instead of a back-office technology problem.

- VANESSA PEGUEROS, CISO, DOCUSIGN

I have not seen an increase in healthcare CISOs moving out from under the CIO. However, in other industries, this is happening more often.

- PHIL CURRAN, CISO & CPO, COOPER UNIVERSITY HEALTH

The major trend I am hearing about is more and more CISOs moving out of the IT department. I would estimate 50% of my peers are no longer in IT, which is a great. This stronger positioning allows for rapid solutions with fewer roadblocks. Also, at every forum I attend, Boardroom reporting and visibility are always at the forefront of discussions.

- STEVE BARTOLOTTA, CISO, COMMUNITY HEALTH NETWORK OF CT

CHECKING IN: ARE WOMEN ADVANCING IN INFORMATION SECURITY?

It has been over one year since we put a focus on women in information security. In August of 2015, we learned that women make up just 11% of the IT security workforce, and fare only slightly better in IT in general – at 28%. This is the reality even as our industry battles with jobs we simply can't fill, as openings in our industry outpace security professionals by more than 3 to 1. At the same time, women are now the majority sex in colleges. These three realities should be inter-related. We should be seeing more women entering the security industry.

But, sadly, one year later that's not really the case industry-wide. Women have made small gains – up one percent in information security roles in 2016.

What are the challenges and barriers to women working in IT security? What can we do to encourage more female participation in our industry? We turned to the experts for advice.

Women Find Success on Aetna's Security Team

Jim Routh
CISO
Aetna

Jim Routh, the CISO at Aetna says that 41% of his team is female, including 60% of his direct reports.

Routh proudly reports, "My leader, Meg McCarthy, is the keynote speaker at the upcoming Executive Women's Forum (EWF). Several of my direct reports regularly participate in women in security industry events."

Routh states, "Several companies (Aetna, Facebook, Uber, etc.) have mature and sophisticated programs in place that enable them to greatly exceed industry norms in hiring and retaining women in cybersecurity. Sharing this information throughout the industry can do a lot to ultimately turn the 11% into 22%. Also preparing featured articles on profiling those women that have been successful as cyber leaders would be helpful.

Routh has suggestions for what we can do as an industry to increase the ranks of women on our teams.

Routh shares three ways to increase the ranks of women in our teams:

1. IMPROVE RESOURCES SUPPORTING STEM

Primary policy focus is to improve resources supporting STEM- the more female students are interested in math and science the higher the probability of them gravitating toward computer science and ultimately security.

2. MENTORING WOMEN

Next priority is mentoring for women once they choose a cyber security related curriculum. We need undergraduates and graduate programs to help find internship programs for them and guide them on curriculum choices.

3. INCREASE PROFESSIONAL MENTORING PROGRAMS

We need to increase professional mentoring programs (like those sponsored through EWF and Women in Security) to give women access to mentors from both genders.

More Gender Diversity in Cybersecurity Will Yield Big Payoffs for Organizations and Women

Deborah Hurley
Creator of ISO 2700
Professor at Harvard University
and Brown University

"From my point of view the situation for women in IT, including cybersecurity, is dire," said Hurley. She cites three inter-related problems that combine to disadvantage women and to reduce opportunities and payoffs for organizations.

1. WOMEN AND GIRLS SELF-SELECT OUT OF MATH AND SCIENCE

"Although the new field of computer science stimulated an initial blip of interest from women, women's participation in math and science since then has continued a precipitous decline. By middle school, girls are opting out of these important, interesting, growing areas of study and economic activity."

2. MISSING OUT ON BIGGEST ENGINES OF WEALTH CREATION

"The situation assumes disastrous proportions when you consider that, by self-selecting out of science and technology, women have closed themselves off from the biggest engines of wealth creation in our era. Compounding this already shocking state, the number of single-parent families is growing in the United States. 'Single-parent families' is a euphemism for women raising their children by themselves. So, the women AND their children are excluded from wealth creation. That is a tragedy."

3. WHILE WOMEN IN IT ENCOUNTER A CLIFF OF DISCRIMINATION

"The women who do go into science and technology fields encounter a virtually all-male environment or a cliff of discrimination. The percentage of women in Silicon Valley is miniscule, compared with the fact that women are 50% of the population. There are numerous other examples, such as Gamergate. Some women drop out. Others hang in there, but do not receive the same recognition, training or opportunities as their male colleagues."

There are counterpoints to these dismal trends, such as the relatively new field of the Chief Privacy Officer. (A 2014 International Association of Privacy Professionals survey of 1000 Chief Privacy Officers found that 48 percent were women.) Hurley said, "This is an emerging field that has attracted women. They work on privacy and data protection and engage with many technology-related issues. The CPO often must work closely with the cybersecurity team."

Hurley thinks that there are many opportunities to engage more women in information security, which is inherently interdisciplinary and multistakeholder. She would know. In 1990 Hurley wrote the first comprehensive report on information security. Prior to that, only technical manuals existed. "My report was the first time we looked at information security across disciplines, including technical, management, legal and other issues," said Hurley.

She continued, "I n order to address cybersecurity problems in a robust, sustainable manner, it is essential to confront them in an interdisciplinary way, pulling what's best and the needed tools from the entire arsenal, whether they be technical, legal, management or other, and to use them in combination to meet the security challenge. People from diverse backgrounds have to come together to solve cybersecurity problems. The ability to get along with, bring together, supervise, and get results from a broad range of people is a vital skill. Further, it is useful to be able to understand and manage human and social behavior among employees, customers and clients, and the public at large."

Hurley pointed out that many cybersecurity problems have little to no technical component. She said, "The biggest cybersecurity problems come from human beings. The effective management and training of people is essential. When we talk about human vulnerabilities, the popular imagination runs to malicious hackers and cybercriminals. They exist and are a problem. But, in fact, the biggest cybersecurity issues come from employees, not the disgruntled ones, but employees who are well-intentioned but are fatigued, negligent or insufficiently trained."

Cybersecurity is a growing field with lots of jobs and opportunities. Hurley strongly encourages women to take a look. Whatever a woman's talents – with people, administration, management, education, technology or law – there is likely an aspect of cybersecurity for which her skills and expertise are needed. In addressing cybersecurity issues and in working with colleagues from many disciplines, which will be a daily part of life, these women will grow in knowledge and experience, thereby making themselves more expert and more able to contribute to their workplace, the economy, and society.

See our recent profile of Deborah:
https://www.klogixsecurity.com/blog/mother-iso-27000

Q&A with Theresa Payton

Theresa Payton
Former CIO, White House
CEO, Fortalice Solutions LLC

Previously, we featured Theresa Payton, Former Chief Information Officer of the White House, in our Profiles in Confidence. Payton shared insight about the current state of information security, the lack of talent, and the importance of including more women, minorities, and veterans in the industry. We recently checked in with Theresa Payton again to hear what changes she has witnessed for women in security. She shares her thoughts with us:

Q: What is the current state of women in cybersecurity?

A: According to Womenscyberjutsu.org, women account for only 11% of information security profession. Overall, I think the industry can do more to help women understand the crucial role that cybersecurity professionals play that make a difference in our everyday lives. Unfortunately, ethical or unethical hackers are often pictured as men dressed in hoodies, and women cannot picture themselves in that role as a possible career choice. These kind of images tend to make women think they may have nothing in common with hackers. Studies show that women want to work in professions that help people, where they are making a difference. When you stop a hacker from stealing someone's identity, you made a difference. At the end of the day, the victims of hackers are people and women can make a tremendous difference in this field. This is something the industry needs to do a better job of showing women.

Q: How can organizations start hiring more women?

A: The industry tells us there is a talent shortage in cybersecurity. There is a perception that if a person doesn't have specific certifications after their name, a degree from a certain university, or a career path 'punch card', then they are not qualified candidates. Hiring managers that only look for the resume qualifications and are unwilling to recognize life experiences, creative problem solving, and a "go-getter" attitude as qualifications are going to miss out on the most successful cybersecurity professionals. Many times, women may be going through a career change and trying to enter the cyber industry yet they feel their certain certifications or work experiences are lacking. Yet they do possess fundamental critical thinking, problem solving and analytical skills that would enable them to be very successful in cybersecurity.

My biggest piece of advice to executives everywhere is to be creative, innovative, open, purposeful, and mindful about how a candidate looks beyond their appearance on paper. Hiring managers should look for women, minorities, and veterans who may not be the exact "type" of candidate they are looking for, but if they invest the time to be a coach and mentor, they can get them up to speed. This, in turn, creates loyal, creative, problem solvers who are more likely to stay at their organization.

Much of this starts with the executive suite making a concerted effort to take a stand and ask themselves and their organization why they don't have more women on their teams. I was recently at a global healthcare organization and the CISO said women account for almost 50% of his team. I asked him what he thought the key to success was and he said he focused on recruiting and retaining women and going outside of the health care industry and security business to get team members with different backgrounds.

Q: How can organizations attract and retain more women?

A: Organizations should run focus groups for women to give them a place to talk and grow. Providing a platform shouldn't be about men vs. women, it should give women a place to flourish and thrive by supporting one another.

If there's someone on my team that impresses me and I appreciate their work ethic, I ask them if they have any friends they would recommend. We also pay employees a referral bonus as they are our best recruiters. This is a great way to gain qualified, loyal employees.

For recruiting, women on cybersecurity teams should go to college campuses to attract other young women interested in the industry. Female college students love seeing women who are already in an exciting career field. The industry does not place enough emphasis on the importance of personal connections like this.

Organizations should make networking tools available to women, such as the Grace Hopper event or RSA Conference, to meet other female colleagues and share stories and growth.

Q: What can the industry do?

A: Last year, the RSA conference started a Security Scholars program that was open to both males and females. I noticed that they had a significantly higher percentage of females and minorities involved than I typically see at companies. I found this very impressive. When I asked about RSA's new focus, they said they were deliberate about making sure there was a good mix of not only genders, but different socioeconomic statuses as well.

As more security conferences look to create "hackathons" for middle and high school students, as well as scholar programs for college students, they must make sure they deliberately foster diversity.

Something very positive happening now at many conferences is women "get-togethers" such as social hours and dedicated tracks of networking. Again, we don't want to create a separation of men vs. women, but I highly recommend taking advantage of these events to gain valuable career growth and participate in networking.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT INFORMATION SECURITY PROGRAMS

CORY SCOTT
CISO, LINKEDIN

HEADQUARTERS: Mountain View, CA

EMPLOYEES: 9,900

ANNUAL REVENUE: $2.99 Billion (2015)

When Cory Scott joined LinkedIn more than three years ago, he took on an emerging, yet highly visible role at one of the largest social networks in the world. “LinkedIn is in a unique position in the ecosystem. We are a large social network focused on the professional aspect of peoples’ lives. The platform has influence on peoples’ careers and personal growth, and I was very attracted to the job. When I came on board there was not a significant security presence, so this was also an opportunity for me to build the information security program from the ground up,” said Scott.

In order to strengthen and elevate the security program, Scott understood he needed clear support from most senior executives. “When I was considering the role, one of the things I was concerned about was the support of senior management,” Scott continued, “I was lucky to speak with Jeff Weiner, CEO of LinkedIn, during the interview process. We talked about the priority he knew LinkedIn needed to give to security. I found he had an incredibly detailed and technical grasp of the challenges of security. He had taken the time to educate himself on its value. He was very supportive of putting security first to build up the trustworthiness of the platform.”

The trustworthiness of the platform is a central theme for Scott. Building up consumer, internal and partner trust in the security program at LinkedIn is the guiding objective for Scott’s group.

“Trust in our platform is integral to how we execute on our vision to connect professionals and make them more productive and successful. If members believe that LinkedIn is a trustworthy place to do business then they will engage with the platform more, and the more they engage, the more valuable the platform is to them, and to us as a business.”

“In my three and a half years here we have learned a lot about the value of trustworthiness. What matters is not just the impact of security actions, but the message you send about security as an inclusive, participatory initiative. It signals to the rest of the world that the organization takes security and privacy into account at every step of development and innovation. Security is moving more into the forefront of peoples’ minds. It is something they consider more now than ever before.”

Scott runs his security program to support the company’s mission of connecting professionals to make them more productive and successful. Three specific objectives drive the information security organization’s ability to make a positive impact.

1. Attract and Retain Talent Who Execute on Vision – When building an effective team, Scott knew he must

first consider the audience and culture. LinkedIn has a strong engineering and data-driven culture, so his security team consists of employees who succeed in that environment. “Even the program managers on my team have written software. When the security talent aligns with the rest of the organization, we have more successful interactions. It also makes our organization more attractive partners to the other business units.”

Scott continued, “It is no secret there is a shortage of security talent. Because we are LinkedIn, we have access to a lot of data on supply and demand for professionals. For every four people employed in information security today there are three open positions. It is hard to find talent with specific security expertise. To combat this, we try to bring people over the wall from other parts of the technology organization into our security team.”

He said, “We have a strong technical bar for almost all security employees. We also look for people with key soft skills, who understand how to problem solve and work with multiple stakeholders. Most important of all, we want our team members to be curious. They need to want to figure out how things work, and how things can be improved.”

2. Achieve Operational Excellence – Scott’s team must understand how to handle demand, standardize on approach and processes, and effectively communicate success as it relates to key metrics. When measuring success and reporting on metrics, Scott divides the functions of the security team into two sets – internal demand and external demand. “Internal demand includes securing the infrastructure, discovering new attacks, maintaining plan alignment and reducing security risks. Progress on these efforts can be tracked via traditional means, such as milestones and achievements. But the other 50% of our time is spent on external demands, which are tougher to measure. This includes servicing the organization, ensuring new projects and programs kick off with strong security, doing compliance work and reviewing contracts and plans because policy requires it. External demand boils down to supporting someone else’s big project. But we still have to measure our work. So we measure things like the number of security reviews we do, the number of bugs found before the application goes live, and we have metrics to measure incident response.”

It is important to note that Scott shares these metrics with all stakeholders, not just his team. He said, “We report on our performance to my direct manager and CEO, but also horizontally to the head of IT, legal counsel, the internal audit committee and engineering leadership. We want a lot of people to be aware of our organization’s performance.”

3. Foster an Inclusive Program – “We emphasize that security is not a team in the corner or in an ivory tower,” said Scott. “We try to be available and involved. That means we are visible, both online and offline. We hang out where engineering and operations congregate and spend time in the same internal chat rooms. Our role is as internal consultants to help teams find solutions to security problems and reduce risks. We want them to see us as advisors more than regulators.”

Scott’s team expanded upon the standard security ambassador programs that some organizations run, when they created the Security Champions program to foster inclusion and commitment outside of the security team. This program requires 25% of an employee’s time and is a six month commitment. “The program is broken into two halves. The first half requires participation in the Stanford Continuing Education program to obtain a certificate in advanced computer security. Once that is complete the Champions become advocates for security within the company. They also perform a “tour of duty”. We put them to work on security, this is where our program goes beyond traditional ambassador programs,” said Scott.

Scott noted that interest in the program is high (they have a waiting list) because security is fun and interesting, but also because it is a good career move. He said, “LinkedIn is committed to the development of our employees. Our founder and executive chairman Reid Hoffman wrote a book called The Alliance that focuses on the relationship between employee and company and the mutual agreement to support advancement, including the employee’s next play. The Security Champions program fits right into that approach.

Scott believes LinkedIn’s approach exemplifies what the future will look like for information security, as the discipline takes on a bigger role. He commented, “Security is becoming a key differentiator for products as they go to market. Large organizations talk about it now as part of their core message. There is always a need to tell a good story about security to the market.”

Q&A WITH CRICKET LIU

CHIEF DNS ARCHITECT, INFOBLOX

Cricket Liu is Infoblox's Chief DNS Architect and serves as a liaison between Infoblox and the DNS community. He previously worked for HP for nearly 10 years, where he ran hp.com, one of the largest corporate domains in the world, and helped found HP's Internet consulting business. Cricket later co-founded his own Internet consulting and training company, Acme Byte & Wire. After Network Solutions acquired Acme Byte & Wire and later merged with VeriSign, Cricket became director of DNS Product Management.

Q) WHY DID YOU JOIN INFOBLOX?

A) I joined Infoblox nearly 14 years ago when the company was located in a small office space above a Taekwondo studio, with only a few employees. It was interesting to be around and see the arc of development of the company over a long period of time. I've had the opportunity to see many smart people contribute to the success of the company, which is now over 800 employees.

One of the biggest milestones was when our former CEO joined because he really changed the character of the company, and through his leadership we were propelled towards an eventual IPO.

Q) WHAT DIFFERENTIATES INFOBLOX?

A) We have a tremendous pedigree and our engineers are some of the best. These things, paired with a rock solid product, make us stand out in the market. The niche market that we started in was DNS and DHCP and at that point it wasn't a big niche, so I believe that a lot of this industry was carved out by Infoblox.

Building on almost twenty years of industry experience with DNS, DHCP, and IPAM services, Infoblox has developed the Actionable Network Intelligence Platform. This platform goes beyond DDI to enable organizations to harness insights derived from the rivers of core services data moving through their networks to enhance all aspects of management, security, agility, and cost control.

Recently, within the last few years, Infoblox has been pushing the idea that your DNS and DHCP infrastructure can be a security asset. DNS servers can be intelligent about queries that they answer and are able to identify infections and malicious activity, which is a dramatic change in how we view the capabilities of DNS servers.

Q) WHAT DRIVES INFOBLOX?

A) The network is the connective tissue of today's IT infrastructure and is critical to the success of any organization—more essential and also more vulnerable than ever. DDI services—DNS, DHCP, and IP address management—are mission-critical. Yet managing and securing them is getting harder as networks become bigger and more complex. We are dedicated to simplifying network control and to using the invaluable data generated by core network services and threat intelligence to deliver actionable network intelligence.

Q) HOW DOES INFOBLOX HELP CISOS?

A) Many of the conversations we have with CISOs are along educational lines, since some CISOs do not fully realize DNS can be a security asset. We help them see that DNS may actually play as part of their security ecosystem. We are still evangelizing and showing CISOs how we can do things like identify infections or malicious activity, how we feed SIEMs and how we interoperate with solutions like Qualys and FireEye.

Q) WHAT PLANS FOR GROWTH DOES INFOBLOX HAVE?

A) A large part of what we are doing in addition to security is cloud-based services. Infoblox solutions for cloud provide automated core network services for virtual machines in the datacenter to improve IT agility, enable faster time to service, and reduce operating costs.

Checking In with CISOs

We spoke to CISOs we previously profiled and asked them to update us on their goals and challenges.

CISOs are battling an uphill climb while playing an increasingly important role as safety officers in the digital transition of the enterprise. The job is tough, and sometimes it can be hard to see the progress through all the work. But, in the years we have been profiling CISOs we have seen the role evolve from a transactional program within IT to increasingly a strategic element of the company, with impact on innovation.

In the PWC Cyber Security 2017 study, David Burg said, "We're seeing more and more that cybersecurity can actually become a remarkable way to help a company innovate and move faster." Compared to two years ago, this is major progress for our industry. Here we check in with the CISOs we have profiled already, to gauge their own progress on solving security challenges, aligning with the business, and carving out a strategic role with executives and in the Boardroom.

Boardroom and Roadmap

During my first year at Webster Bank, board awareness around information and cybersecurity was a hot topic. Today I have consistent "face time" with a dynamic group of directors, no less than six times yearly. Strengthening an already talented Board of Directors and realizing Webster's need to remain relevant at every level, the bank recently brought on an extremely talented and forward leaning technology Board Director.

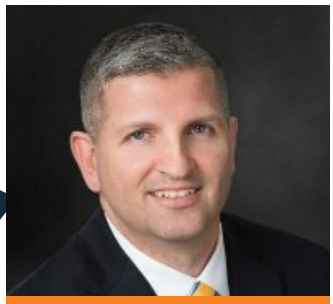
Over the past three years, one consistent topic for the Board remains cybersecurity insurance. Discussions center on limits, types of coverages, carriers, risk transfer strategies, and retainers.

Our talented and relevant Board of Directors and Executive Leadership has supported a 75% growth in staff, doubling of expense, and significant influx of capital into the Information Security Program over the past three years. Thanks to this outstanding support, my department is able to defend against current threats, plan for regulatory change, and anticipate potential future threats and mitigate them in advance while working in tandem with the lines of business.

Moving Away from MSSP

One of the most significant information and cybersecurity accomplishments over the past 12 months has been the institution of a Technology Operations Center (TOC) at Webster Banks. The TOC has two primary goals, 1st combine elements from the Security Operations, Service Desk, Infrastructure, and Applications group into a specially designed, centralized, and collaborative work area and 2nd to use this collaborative group to better respond to and resolve mundane and line of business technology needs and provide faster and more effective incident response.

As this group begins its journey to 24X7 operations, the next major milestone is the elimination of our currently underperforming and costly outsourced Managed Security Services Provider (MSSP).



Damian Laviolette
CISO
Webster Bank

Putting Plans in Place

Last time we spoke, we did not have a formalized plan for the information security management program. I have since developed a formal plan that addresses mission, goals, and overall strategy including cyber security systems, business continuity and incident response, data management, awareness and training, and policy management. After establishing a clear mission and strategy, I developed a management process designed to accomplish them. This was a major milestone that strengthened my relationship with the Compliance and Audit Committees. We also launched a comprehensive audit plan and implemented a Governance Risk and Compliance (GRC) system.

Increased Visibility

When I started here, it was my desire to create a culture of information security awareness. I was asked to be a member of the Audit Committee. This transition allowed me to successfully promote and raise awareness of our information security program. Ultimately, it served to inform the Board of Directors of the challenges facing the security team and the organization and the measures we've taken to address those challenges. I firmly believe they now have a realistic sense of the risks and are very supportive of our program.

Challenges & Wins

As a smaller company, we are challenged with not having the resources that a large company has to staff a security program, yet we have the same security requirements. Planning and doing can't occupy the same space and operations (doing) will always take the priority. Therefore, having a solid strategy and plan in place is essential to keeping staff focused on what is most important. This helps us overcome the resource issues.

We are going through the HITRUST certification process right now. Attaining certification will be a major win for us because it provides so many benefits to the organization.

Steve Bartolotta
CISO
Community Health Network of CT

Phil Curran
CISO & CPO
Cooper University Hospital

Board-Focused

I consistently meet with the Board and brief them on a regular basis. Most recently, we brought in someone from the New Jersey Cyber Security Communications Integration Cell (NCCIC) who shared what they are seeing in the healthcare industry and suggestions for information security programs. One of these suggestions was encryption at rest, which could have a significant impact on the physicians treating patients.

I now update and explain to my Board on how we have been training our staff to recognize things like phishing email scams, as well as what we've done from a patching and back-up program, so the Board understands the steps we are taking to mitigate risk.

It continues to be important that our board drives information security down throughout Cooper so we may ensure this becomes part of the culture.

Strategic Plan

I've been focused on understanding my strategic plan and continuing to keep focused on that plan.

Kevin Hamel
CISO
COCC

Growth Outside of COCC

I worked with the founders of the CISO Executive Network and started up a Hartford chapter. Through reaching out to many of my CISO peers in the area, we got the chapter up and running and now get together six times a year to have meaningful conversations about information security in today's world.

I also participated in the eight week Citizens Academy run by the FBI. This program gave me a behind the scenes, in depth look at the FBI, which has really helped to strengthen our relationship with them and the DOJ. It's really beneficial for us as an organization, because if our clients experience financial fraud or experience a cyber breach, I can reach out to federal law enforcement on their behalf and potentially get our clients some help from federal agencies.

Working with Boards

My strong relationship with our Board and CEO has opened up opportunities for me to speak to our clients' board of directors about cyber security. I've also been asked to speak at a number of other venues such as local chamber of commerce events, audit associations, and even hospitals' board of directors meetings. Board members and business leaders are trying to get their arms around the challenging issue of cyber security.

Focus on Business Risk

Our information security program continues to evolve to a more risk-based focus. We look at info sec findings and translate them into business risk. Also, our employees continue to have a healthy focus of exactly how they play a role in protecting the organization.

Sales Closer

A big part of my role has shifted relative to sales enablement. I now work with our sales organization to assist in being a "closer" from information security perspective. My involvement comes in the late stages of the sales cycle, where security becomes a key differentiator against our competition to help us win the deal. This has been particularly effective when I am utilized with larger enterprise accounts to help them close those opportunities.

Decentralized Security Model

We have really strengthened our risk management program over the last year by pushing a decentralized security model out to the business. We are actually ensuring the business understands, is aware, and takes ownership of the information security risk they truly own. This allows my team to act in more of an oversight and management role, and pushes accountability out to the business.

Agility with High Growth

We are a high growth, fast moving company, so I ensure we have an agile approach to roadmap and planning activities. Things can change quickly, so we must be flexible since new priorities and challenges can come from every business deal. One of my biggest realizations was that narrowing down the horizon for the roadmap to the current quarter and projecting two quarters out provides more responsiveness versus being locked into a one year roadmap. I no longer push my team to predict the future that far out, as priorities can change.

Vanessa Pegueros
CISO
DocuSign

Transition into Healthcare

Seven months ago I transitioned from my role as a CISO in retail to a VP, Information Security (CISO) at a large healthcare organization. Something that drew me to this industry was the opportunity to address risks across many industry verticals within a health system. There is healthcare information risk, regulatory risk (HIPAA, PHI, etc.), credit card risk (PCI), operational technology risk (OT), medical device risk and ultimately every other vertical within a growing health system. I've found having an information security background in other verticals has assisted me in lowering risk across the large ecosystem in our health system.

One of the draws to this organization was the openness of the CIO to partnering with security, along with his proactive approach to lowering cyber risk and driving security awareness at all levels. I saw this as a great opportunity to use my executive security experience to build a risk-based security program to enable secure innovation to assist in saving lives.

Boardroom Discussions

I found this organization to be more Board-driven than any other industry I have ever worked within. I have attended seven different types of Board meetings with maybe 45% of the same audience. Each Board has a different mission statement and reason why they are interested in the security risk we have across our organization, including the strategic direction information security is taking to lower risk. There is a high expectation of continual updates on how their security investments are lowering cyber risk.

Healthcare Before Information Security

Although some areas of healthcare may be slightly behind other industries when it comes to cyber protection, healthcare is more in tune and has been doing security for far longer than information security has been around. In many cases you could say information security's terminology was derived from healthcare. Our information security methods of remediation, containment, isolation, monitoring and triaging risks are how hospitals have been successfully addressing health incidents for years.

Darrell Keeling
CISO
Parkview Health

WHAT HAVE WE LEARNED?

CISOs are executing on their goals and accelerating their information security programs. Great progress has been made with Boardroom alignment and communication through business-focused conversations and strategic discussions.

Every CISO discussed specific goals they accomplished since we featured them in our magazine. They track their progress through metrics and roadmaps, and present this information to both their teams and the Boards. Many of the CISOs we spoke with have grown and improved their teams to act as business enablers.

Overall, CISOs continue to grow from their successes and failures, learn from one another, and push forward to protect their organizations while aligning to the business.

Methods for Managing Forward Progress

A look at business and academia methods

While security professionals are acquiring advanced business degrees in significant numbers now, many still bring a technology mindset, and a background in computer science, to the profession. This makes them excellent security practitioners, but less natural project leaders and strategic business executives. Security leaders have the best intentions to align security to business goals, but without a proven model or business methodology to follow, success may get lost in the tactical efforts required to keep up with the onslaught of evolving threats.

In the security organization, heads are down and focus is on putting out the next fire. Professionals are not always able to take the time to think strategically about their security programs and how best to implement them.

Here we outline key takeaways from business and academia methods that help security professionals prioritize efforts, recognize and respond to progress and maintain consistent focus on the grand end game.

Method:	The Kellogg Innovation Framework (Northwestern School of Business)	Lean Process Management	Stanford University's Design Thinking
Description of Method:	According to Dr. David Reis (SVP & CIO at Lahey Clinic), the Kellogg Innovation Framework, "helps you develop an innovation engine for reacting to today and preparing for the future."	Lean organizations are agile, adaptable, healthy and smart. Lean businesses create high value processes at the lowest overall cost. In lean organizations, value is created as the process is fine-tuned over time.	"Design-thinking" makes empathy a part of the innovation process.
Key CISO Takeaways:	o Use the framework to ensure your "security program makes forward-looking progress, while dealing with near term issues," says Reis. o Instill an innovation mind-set in your team to develop creative security solutions that enable business.	o View security programs as cyclical processes, not linear to ensure continuous evaluation and fine-tuning of security processes to provide the maximum value. o Lean process management discourages distractions and keeps the security team focused on business alignment.	o Design security solutions that deliver a positive, even transformative experience for users. o Regularly evaluate security programs in relation to how they impact users.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT INFORMATION SECURITY PROGRAMS

ANTHONY SIRAVO
CISO, LIFESPAN

HEADQUARTERS: Providence, RI

EMPLOYEES: 23,000+

ASSET SIZE: $1.9 Billion

Anthony Siravo is the Chief Information Security Officer at Lifespan, Rhode Island's first health system founded in 1994 by Rhode Island Hospital and The Miriam Hospital. Working at a healthcare organization enables Siravo to feel a sense of community contribution. He said, "My contribution is being on the front lines protecting our patients' data, and ensuring the security of their private information."

Prior to Lifespan, Siravo held a CISO role at a large technology organization with 140 global locations. Siravo said, "I chaired the Information Security Governance Committee and was a principal member of the Product Security Council. I oversaw the successful $3.5B acquisition and subsequent secure integration of Motorola Solutions' enterprise business."

While chairing his previous organization's Information Security Governance Committee, Siravo had exposure to the executive board and key stakeholders in the company. "I worked with key business unit partners to implement practices that meet defined policies and standards for information security. I also served as the process owner for all activities related to the confidentiality, integrity, and availability of customers, business partners, employees and business information, in compliance with their information security policies."

AN MBA TAKES SECURITY TO THE BOARDROOM

Siravo's extensive experience with business leaders in past roles inspired him to seek his MBA. Although he possessed an expert technical mind, he needed to improve his ability to translate security to the business community. He recognized that executives who held the purse strings, such as CEOs and CFOs, only cared about technical requirements to a certain extent. To achieve the funding he required to run a successful security program, Siravo knew it was essential he understood how to speak the language of business.

Siravo said, "There are only so many security threats you can throw at an executive and effectively convince them of the importance without tying it back to financial risks. It didn't really matter that I thought a risk was not acceptable if I could not understand what the business thinks is unacceptable. My MBA provided the knowledge necessary to dive deeply into finance, budgeting and business presentations."

Siravo believes the most important thing he learned in business school was the value of being prepared to address questions from business leaders immediately, and with an answer they

can understand. "We learned how to present to the Board. I call it 'Boardroom Mode'. You need to speak slowly, avoid fillers, and repeat your message in laymen's terms. You also have to dress the part. Lots of executives pre-determine who you are based on how you are dressed. Technical people do not always realize that how you dress matters. When I first started presenting, I wore business casual. When I switched to suits, all of a sudden they wanted to hear more from me. This is called mirroring. If you make them comfortable by dressing the part you will have better results."

Siravo attended the MBA program at Bryant University, where they also emphasized the importance of working in a team. "The program used the Meyers Briggs test to methodically create teams of diverse personalities. We had to learn to work together. Every team member hated it at first, but by the end we were all best friends. It showed that you can work with anyone if you put in the effort."

MATURE SECURITY STRATEGIES IN THE HEALTHCARE INDUSTRY

At Lifespan, Siravo came into the position after a number of shorter term predecessors, creating a challenge to piece together a somewhat disjointed information security program. He said, "While I wasn't starting the security program, I have had to act as if I was. We were nearly starting from scratch."

Another challenge Siravo faced was understanding the appropriate methods to increase budget and resources. To overcome this challenge, he put his MBA-acquired skills to use through strategic communication. He commented, "I spoke in business language while I presented and educated the Board and business leaders. I put together real business cases, not PowerPoints that do little more than point out threats and risks. I have an open-door, education-focused policy."

Through discussing risk as it relates to business goals and metrics, Siravo further aligned information security with the organization as a whole. He emphasized, "Security is not the only risk to an organization, so you really have to build your case to get the budget you need."

According to Siravo, "Lifespan's mission is to "Deliver Health with Care" and we accomplish this by prioritizing the 4P's. The 4P's are Patients, Providers, People, and Purpose, with sub goals to increase quality and safety in order to provide patients a better experience. Our security effort aligns with these corporate goals by ensuring compliance with regulatory requirements such as HIPAA, CMS, and TJC and securing the technology and patient data that help deliver health with care. My organization seeks to protect Lifespan's network, information assets, intellectual property, and PHI from internal and external cyber and information security threats."

Siravo lists education, training and awareness as one of several strategic security goals for Lifespan. Ensuring the entire workforce understands cyber threats, improves the organization's ability to protect the patients and people, and deliver on their purpose. To achieve this level of awareness, Siravo's team focuses on educating users about ransomware and phishing scams. "I launched a phishing campaign at Lifespan that notifies a user when they have been successfully phished. More than half of our executives failed our first phishing test. They were mad! Now they are our biggest reporters of phishing. They took the exercise very seriously and we have dramatically improved as a result."

His efforts are paying off as the organization continues to move to a more formalized security process. He said, "Exception approvals used to be verbal, we now have a written system. New risks are managed in our enterprise risk register (in conjunction with Corporate Audit), providing proper evaluation, and are addressed by Lifespan executives. There was no risk register when I came in."

In addition to users and executives, Siravo holds business partners more accountable for information security. He established his own security analysis program for third parties and partners, and keeps tight control over security policy adherence. He said, "The SRA (Security Risk Assessment) is a process that all new vendors must go through if they access, store, or transmit personal health information, personally identifiable information or payment card information and business confidential data. We based our SRA on the NIST framework. The questions in the assessment align with generally accepted practices for a comprehensive security program. Once we have the answers, my team presents the results of the SRA to the legal, purchasing and the business sponsor for consideration."

Another important strategic role for Siravo is his position as security consultant during intra-hospital or business partner organizational activities. He commented, "When new business partners inquire about our security capabilities, my office will, upon request, provide descriptions of our capabilities and our operational security execution." By being a vocal and willing contributor to all conversations about security process, Siravo makes it easier for the business to collaborate and engage with partners, and important business objective for the company, and an obvious example of Siravo putting his MBA to good use.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT INFORMATION SECURITY PROGRAMS

BARRY ABRAMOWITZ
CIO, LIBERTY BANK

HEADQUARTERS: Middletown, CT

EMPLOYEES: 705

ANNUAL REVENUE: $4.5 Bliion

INFORMATION SECURITY TAKES CENTER STAGE

As CIO of Liberty Bank, Barry Abramowitz's responsibilities cover the entirety of technology operations for the company, including security operations. Liberty Bank is the oldest mutual bank in Connecticut with more than $4.5 billion in assets and 56 banking offices throughout the central, eastern, and shoreline areas of the state. "My role has shifted from 80% technology innovation and 20% security, to 80% security and 20% technology innovation. It's just the nature of business now; security is front and center," said Abramowitz.

"The shift in my focus is a byproduct of our environment. In banking, internet services have really taken off in the past decade, with mobile apps and the Internet of Things leading the change. More systems are connected, more business is done over the internet, so this creates more security issues. Twenty years ago, security was about access and asset management, now security is about protecting your business from the world."

As head of the technology and operations division, Abramowitz leads a team of security engineers who implement the organization's security controls. He also partners closely with the bank's Risk Management organization which is responsible for information security policy and procedure. Abramowitz said, "In business today, security is everybody's job, but my role is to be one of the thought leaders for the bank as we address information security. I work closely with the head of the Risk Management team to implement the necessary controls."

TECHNOLOGY STRATEGY REFLECTS CORPORATE GOALS

Abramowitz and his team create a technology strategy to mirror and support the bank's overall goals. The bank clearly states their goal to maintain a positive reputation with customer service, even as they grow their digital services, expand their market position and evolve to support more non face-to-face transactions with customers. Other important aspects to the bank's success include maintaining a well-trained and engaged workforce and being responsive to risk and compliance requirements. "Those are our top corporate strategies. Relating to what I do and how our group performs, I take the corporate plan and develop

a technology strategic plan to support it," commented Abramowitz.

The bank's current technology plan is focused on customer and employee self-service and security of those systems. The technology team is also focused on managing data in an effort to make Big Data more available and easier to digest and understand, and more secure.

Abramowitz's team selected the NIST Cybersecurity framework as a way to measure and manage security efforts as well. He stated, "Once we decided to work within the NIST framework, we had an independent assessment to help us baseline our maturity level. This really helped us understand where we are as an organization and where we need to go. It helped us prioritize our efforts and gave us a way to measure success. We over-laid our risk assessment process on top of NIST and we have a good roadmap for our security program. Now we report our progress against NIST to the Board on a regular basis. "

Abramowitz reports directly into the CEO, who approves his plan and budget, along with the Board. "Our CEO and Board are very engaged in cybersecurity and they recognize the importance of it to our organization." Abramowitz foster's this interest through regular interactions with the Board. He provides monthly reports and presents to the Board in person every two-to-three months. In those presentations Abramowitz focuses on making cybersecurity relatable to his audience, through emphasizing business impact and drawing comparisons to issues they may recognize as general technology consumers. "We have also brought in third parties to give perspective on security to the Board. That format also works very well," he said.

EVOLUTION IN THE INDUSTRY OVER 20 YEARS

A key evolution Abramowitz experienced during his long tenure as CIO is the bank's approach to technology purchasing decisions. Abramowitz said the emergence of numerous technology startups with impressive and innovative solutions, particularly in IT security, has made the bank more willing to make investments in technology solutions from emerging companies. "Previously, we had a minimum requirement of a certain number of years in business in order for us to work with a technology provider, but the technology market is evolving so rapidly, we are moving away from that requirement. Especially in security, we need to be able to evaluate the most cutting edge solutions that address today's concerns best," said Abramowitz.

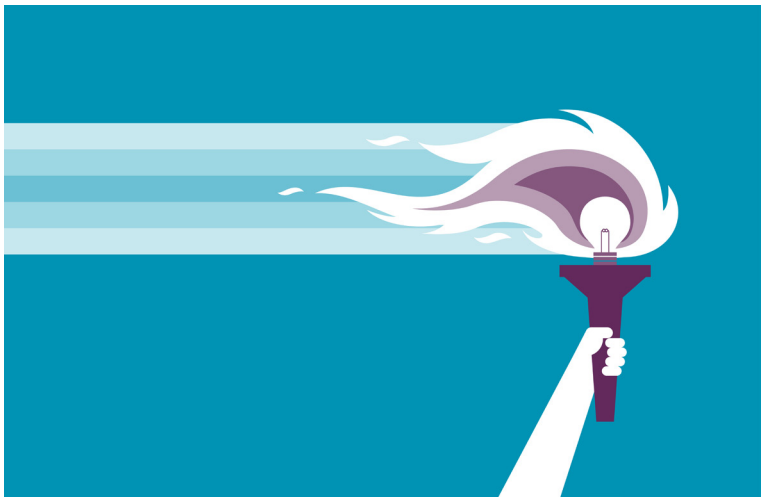
Abramowitz does caution other CIOs and CISOs to look carefully at their existing assets and infrastructure before making additional purchases. "You have to be very pragmatic and go back and revisit your tool sets from time to time. Can we improve our current processes with existing systems? Are there updates or enhancements to our existing solutions that will solve a new problem we have encountered?" said Abramowitz. He continued, "We do a good job of tracking enhancements with our core banking system, and we are working to extend this to all of our systems. When new releases come out, we track all of enhancements, even if we do not implement them. The worst thing you can do is bring in a new provider to solve a problem that an existing system could address easily and cost efficiently."

LOOKING BEYOND BANKING FOR INNOVATIVE SOLUTIONS AND EXPERTISE

"I am a committed community banker. I have been in banking my entire career and have many peers in my industry that I rely on for expertise and shared insights. What I do now is take myself out of my comfort zone. I routinely attend functions with representatives from other industries – such as healthcare, pharmaceuticals, insurance and manufacturing. Sometimes I am the only banker in the room. Because industries sometimes march in line, the group can overlook other ways to address issues and approach opportunities. Speaking with peers in other industries exposes me to new solutions," said Abramowitz.

He continued, "Likewise, there are vendors who get strong footholds in different industries. This could be because of word of mouth, and those vendors may not be working with the financial services industry because of their traction elsewhere. But their solutions can be very relevant to our problems or what we are trying to accomplish. I have met a different set of vendors this way, and when we bring them into our environment it is very refreshing and very educational." In general, Abramowitz believes it is necessary to stay educated and be open to new solutions in order to keep pace with emerging threats and issues facing businesses today.

IN YOUR OPINION



Q: FROM A STRATEGIC PERSPECTIVE, OVER THE PAST YEAR, WHAT HAS BEEN THE MOST IMPORTANT CISO TREND?

RYAN KALEMBAR
SVP Cybersecurity Strategy
Proofpoint

"Today's CISO oversees more communication channels, and new technologies, than ever before. This year CISOs prioritized improving their defenses against modern threats and modifying their security controls to address how people work today.
Small or large, nearly every cyber-attack of note starts the same way – targeting a person, whether delivered via an older technology like email or a newer one like a social network. In order to stop sophisticated cyber threats and accurately assess risk, the CISO has increasingly needed to become an expert in how their business operates and go beyond the bits and bytes of how systems work. An understanding of how to enable the business, while protecting it, has been essential throughout 2016—and will continue to be a top priority in 2017."

"CISOs are faced with the challenge of protecting their organizations from an ever- evolving threat landscape, while their visibility and context of their current environment is limited – putting them in a very difficult position. As a result, CISOs are spending more of their budget on tools that give them better visibility over their environment, as well as tools to help them identify threats that may already exist in their environment. That includes tools to help understand what cloud apps individuals may be using, as well as analytics tools that can evaluate security events, network traffic or user behavior to identify threats much more quickly, and reduce potential risk to the company. CISOs are also striving to, but struggling to understand how threat intelligence gained from services, government entities or their own products can effectively be leveraged to detect and stop advanced threats."

DOUG COPLEY
Deputy CISO; Security & Privacy Strategist
Forcepoint

FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

CISO PROGRESS

NOVEMBER 2016

K logix

WWW.KLOGIXSECURITY.COM
888.731.2314