FEATS OF STRENGTH

A BUSINESS-FOCUSED CYBERSECURITY MAGAZINE

SEPTEMBER 2021
KLOGIXSECURITY.COM
617.860.6485

K logix

FEATS OF STRENGTH

CISO RESPONSIBILITIES

SEPTEMBER 2021

FROM THE *Editor*

Dear Readers,

CISO Responsibilities is the theme of this issue of Feats of Strength magazine, a topic that continually comes up when speaking with customers and the security community. Customers often ask – how are my peers structuring their programs? How should I organize my team? What should my focus areas be? How do I address the risks associated with business transformation? What resources are needed for each of my program areas?

We asked these types of questions to the leaders featured in this magazine. We found that no two security programs are the same, they are each crafted based on specific corporate missions and goals, how the organization is structured, and much more. The similarities we did find include:

- Ensure security program objectives are proactively shared with business executives
- Clearly define each team member's responsibilities, even if they wear many hats
- Utilize part-time workers or outsource to fill any talent gaps
- Keeping pace with threats is key, especially with remote workforces and an uptick in ransomware
- Focus areas should be directly aligned with business goals and keep pace with transformation
- Identify specific resources to achieve goals and overly prepare for budget discussions

I want to encourage any readers to reach out to us if they struggle in any of the above areas. We have extensive data that answers many of these questions and actively help CISOs and other security leaders in effectively structuring their programs. We help ensure security is aligned with the business to reduce risk and increase maturity. Our focus is always on justification and making a positive impact.

Kevin West

CEO, K logix

Magazine Contributors:

Katie Haug

VP Marketing, K logix

Kevin West

CEO, K logix

Kevin Pouche

COO, K logix

Marcela Lima

Marketing Manager, K logix

About K logix: Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.

We craft our services to address specific customer and industry challenges. One of the ways we do this is through our thought leadership, business-focused publication *Feats of Strength*. Through hundreds of CISO interviews, we extract trends in order to provide services that align business to information security.

www.klogixsecurity.com/feats-of-strength

Marketing@klogixsecurity.com

DAN BOWDEN

CISO
SENTARA HEALTH

HEADQUARTERS: Norfolk, VA

EMPLOYEES: 30,000+

REVENUE: $10 Billion

When we last interviewed Dan Bowden, CISO at Sentara Health, he was focused on rebuilding a security program, with an emphasis on developing an effective, business-aligned department. Today, he shares that security is supported and trusted across the organization. He comments, "I'm rolling up on five years at Sentara now. It's been an enjoyable time for me. I'm honestly sometimes surprised how happy I am in my position. And I think in terms of how things have changed, for myself and my team, we're more acknowledged and recognized as enabling what the organization is trying to do."

EVOLVING TEAM AND PROGRAM RESPONSIBILITIES

Bowden believes security program responsibilities may differ based on the organization's specific requirements and structure. For his specific program, he says the three core tenet areas include enterprise cybersecurity, enterprise cyber risk, and enterprise identity services.

For Bowden's enterprise cybersecurity team, they oversee enterprise threat management, and control management throughout security operations, architecture, and red team work—maturing towards a future cyber fusion center. He explains, "Along with prevention, detection and response functions, this team will mature towards on-going purple team exercises, constantly testing security posture, validating the efficacy of controls, figuring out which threats are exploitable, and how you're going to mitigate that risk. The director will have responsibility for the stack of controls and how the people, process and technology in that function is managed."

Bowden is actively looking for a Director of Enterprise Cyber Risk, someone who manages all of Governance, Risk and Compliance (GRC). He comments, "The big responsibilities include vendor risk management, developing organizational information security policy, standards, and procedures, then mapping those into what our business requirements are and the regulatory requirements that we have. What are our contractual obligations? What are our internal policy obligations? And how do these align with applicable frameworks? And if we are audited, either from a regulatory, contractual, or an internal audit perspective, are we accounting for the frameworks that will be used in that audit? There's a lot on that person's plate in terms of managing a $10 billion health system. HIPAA is very challenging to manage from a regulatory perspective, but on our health plan side, some of the contractual obligations are equally if not sometimes more challenging for securing data than even HIPAA."

The third tenet of the program is enterprise identity services.

The director of this program manages the governance platform, how that platform interacts with HR and ERP, and how it is mapped into driving workflow into various systems. This includes where people's credentials will need to be created and entitlements added or deprecated, depending on how their roles change in the organization. Also, they may need to occasionally terminate access for people as they leave, and then workflow to manage segregation of duties and some of their more high-risk applications.

Bowden says, "That's how I'm going to organize my team strategically going through 2022 and the upcoming years is those three directors. And as we develop the amount of work, what drives work, what creates work, how do we prioritize things, that will then inform how we model the teams that report to them. I delegate a lot. I ask a lot of questions. How is work getting done? How is performance being managed? But for the most part, I don't really tell the directors specifically how to model their teams. The next couple of years will be interesting because we'll be changing our org model a little bit, and we will be increasing the total breadth of the services that we offer to the organization."

FOCUS ON IDENTITY GOVERNANCE AND DETECTION & RESPONSE

The top two areas Bowden and his team will be focusing on are identity governance and detection and response capabilities.

He says they are trying to align their investment in a new identity governance platform with the deployment of their enterprise resource planning (ERP). He explains, "We have a new leader in our digital innovation area. What we'll be doing is making sure that the investment we make for identity governance, for identity proofing, for onboarding workforce and consumers, that we have a really good partnership. Identity is a really big one in 2022."

An important consideration when investing resources in an identity governance platform is ensuring it is integrated with their ERP project and some other key projects the organization is focusing on. He says it is crucial to focus on alignment with other departments and ensure integration with their workflows and processes.

Increasing their detection and response capabilities is the other key area Bowden's team is focusing on. He explains, "We also will be investing in increasing our detection and response capabilities. We've had great support building up a very solid protective preventive control posture, and as we've assessed ourselves and had red team assessments, we've had to look at how we are going to detect and stop adversaries once they do get in—or, how we discover insider threats. It's tough to find good controls that give high fidelity and actionable event information, and we'll be spending a considerable amount of time on how we find the right tools and capabilities for detection. And we've done a lot of homework on detection and learned about some better internal preventive and protective controls. In particular, a much more granular segmentation inside our network that's even more robust than we've done before."

> *"The cybersecurity problem is ubiquitous and omnipresent, and everybody in an organization sees it all day every day. And I believe everyone in the organization wants to help the CISO prevent a major cyber incident."*

DEFINING A TEAM ACROSS THE ORGANIZATION

With intimate experience restructuring and building security programs from the ground up, Bowden believes in focusing on people, communication, and alignment as keys to success. He believes in defining who should be on your team when looking outside of the security department. There are different levels or degrees of a team starting with peer business leaders. He encourages CISOs to find out who the CTO, IT Director, Chief Counsel, Privacy Officer, Chief of Internal Audit, and the like are, in order to make sure they are part of your team and core stakeholders in security. Then, he suggests finding a strong oversight committee which might include the COO, someone from brand engagement, and people from other parts of the business.

Bowden says, "My point is, don't look too hard at the org chart under you until you've gotten to know people across the organization, especially who your peers are. And it's hard. It takes a lot of work. It takes a lot of time. It takes us out of our comfort zone. A lot of us IT people and security people are introverts. We play extroverts when we're at work. If you are restructuring, look to your peer set first. These peers are the people you need to consider as part of your team. You help them win, and they help you win. I'm tired of hearing CISOs saying nobody cares. I just don't believe that anymore. If you're hearing nobody cares, I would wager that you didn't talk to anyone. The cybersecurity problem is ubiquitous and omnipresent, and everybody in an organization sees it all day every day. And I believe everyone in the organization wants to help the CISO prevent a major cyber incident."

TIM SWOPE

CISO
CATHOLIC HEALTH

HEADQUARTERS: Rockville Centre, New York

EMPLOYEES: 17,000+

REVENUE: $3 Billion

For over three years, Tim Swope has worked as CISO for Catholic Health, an integrated health care delivery system in Rockville Centre, New York. As a security leader, Swope focuses on identifying gaps related to key IT security processes and the implementation of information security and risk management.

With over twenty years of experience, Swope understands the connection between productive, proactive security programs and business priorities. As a seasoned leader, he emphasizes the importance of strong communication with business leaders and executives in all departments of an organization. In this profile, Swope shares his thoughts on the progression of CISO responsibilities and valuable advice for other leaders.

EVOLVING CISO RESPONSIBILITIES

Swope says CISOs must constantly adapt to changing business environments, especially in healthcare organizations which have seen dramatic shifts in digital transformation, remote workforces, the internet of medical devices, and more. Swope says responsibilities that fall under CISOs are not just data security related anymore, they have grown to include patient privacy and safety.

He explains, “In the post-COVID world, people are going to start seeing that there’s a patient privacy initiative. In other words, who can tell if you’re securing these records? Did you get your vaccination? Did you have COVID? Those sorts of things are very big issues because of the patient privacy initiative. And that’s from a healthcare standpoint, part of the CISO’s initiative. But also response to threats. We have to do as much as we can do proactively, but a lot of companies have been attacked by bad actors with ransomware. You also have to prepare yourself with your response and how fast you can get your system up and running and get back to daily operations.”

Another area CISOs must adapt to is changing budgetary issues, especially as new government directives emerge, requiring organizations to implement or change existing policies, technology, or other areas of investment. While these types of government directives are beneficial to continue to increase the security of organizations, security teams must then reevaluate their budgets and organize accordingly.

Digital transformation is also impacting CISO responsibilities, and Swope says, “There’s been some studies that, especially millennials, are very into the wearable technology, so you can have proactive healthcare. Such as - what’s my heart rate today, what’s my blood pressure, am I eating healthy, getting enough exercise? These go into a medical record where a healthcare provider like us can analyze them. So the digital transformation expands our ability to give help.”

He continues, “Also, the potential attack surface has expanded

by more than a hundred-fold. So as we've moved from the confines of our productive, traditional, and safe walls, now you have more outwardly public facing websites, applications, and ways to interact, be it zoom, digital, or other ways. And that opens up an attack surface for you that you never had before. So these are some areas of concern that a CISO now works with and is defining. When you look at those initiatives, is it something that we can secure and do we have the funds outside of the project to do that?"

TOP FOCUS AREAS

Protecting endpoints is a top area of focus for Swope, because as the hospital system grows, more endpoints emerge that require protecting. With an influx of outside medical devices being dropped off to patients' homes, security must adjust and set strong protective measures. He comments, "You must make sure that our remote staff and now our remote vendor endpoints are protected. Imagine all the vendors, consultants, and service providers we have who all sent their workforce to work remote. So when we certify a vendor for a risk assessment, now they just went outside their own area that we conducted the assessment against. Those are some big concerns over the next 12 months. And they'll continue to be."

Another concern for Swope is the uptick in daily requests for data related to COVID patients. Accessing and protecting this data requires security resources, and he is working hard to find easier means to get this type of information to the right parties.

SECURITY PROGRAM STRUCTURE

Establishing a proactive and diligent program is paramount to Swope, and he has organized his team to address key cybersecurity areas. The cybersecurity governance group has direct control of future and current information security and new systems. For any new systems coming in, his team has comprehensive oversight into them. They also have a strategic planning function for not just security, but also for infrastructure and architecture, another crucial group within his program.

He explains, "Under my cybersecurity governance group, we have our infrastructure and architecture group, which includes networking. We make sure from a top-down level that anything that's put in follows certain requirements for security or privacy for architecture and how data is set up and the like. Then those we can actually manage, there's the audit functions."

He continues, "Then we have the policy and procedure lifecycle, that's big because those touch everything from security, privacy, infrastructure standards, architecture standards, and how that information is disseminated within our entire corporation. That would also include corporate risk management, IT risk management audit functions, strategic planning, and risk management for patients."

> *"Identifying what the priorities are and making sure that you're picking the right ones is an ongoing exercise. Especially with the rapid evolution of threats, something that may be low priority today might become really important tomorrow."*

INVESTMENT AREAS

Along with increasing their footprint for endpoint security, Swope and his team plan to put significant investments in Privileged Access Management. They currently have remediated all the privilege access to a point where they have a strong benchmark, but with a standard amount of employee turnover, it continues to be a challenge.

With patients being seen outside of hospital walls, Swope plans to investment in Identity and Access Management solutions to address these concerns. Patients are now accessing their information from their phones, tablets, or other devices, and security must keep pace with ensuring only the patient themselves are accessing that data.

From a proactive standpoint to address ransomware attacks, they are planning to invest in a secondary data disaster recovery. He comments, "People have offsite applications, but we are literally creating a mirror image of our site and air gapping it, so if we do have a ransomware attack, then I'll have a mirror image that's up to date and can be turned over rather than backing up what we've got from backups. I'll flip a switch and we're up and running within 15 minutes on the total shutdown. That is a significant investment. It's one that most people can't make. These are some of the methodologies I give seminars on, how you can stop ransomware attacks or help yourself afterwards."

By focusing on proactive risk management, Swope hopes to identify risks in the organization before they happen. Swope says if you can identify the danger first, you have the opportunity remediated. He will focus on looking proactively at what they can remediate and protect before something happens, while monitoring everything else. He explains, "Some people are looking for a methodology to protect them. I can't give them one that's one hundred percent, but I can give them one that puts them on that journey. That comes from first, identifying the risks that you have, and then looking at the criticality of them as attack factors, then putting in some strategy to remediate those while monitoring everything else."

CISO RESPONSIBILITIES

BREAKDOWN OF SECURITY PROGRAMS WITH EXCERPTS FROM SECURITY LEADERS

By Katie Haug (K logix)

In this issue of the magazine, we interview effective security leaders with deep expertise building and maintaining robust, proactive security programs. While their leadership styles may vary, the approach they take to a strong program is similar – they focus on building programs directly aligned to business goals to ensure they make a positive impact and reduce risk.

We found that no two programs look the same in terms of structure, responsibilities, or team. Below we share snippets from the security leader's profiles:

HEALTHCARE

Page 4 - Dan Bowden, CISO, Sentara Healthcare

Dan Bowden, CISO, Sentara Health organizes his program into three areas: **enterprise cybersecurity**, **enterprise cyber risk**, and **enterprise identity services**. He plans to have directors oversee each of these areas, with a team to execute on core goals. Bowden says, "That's how I'm going to organize my team strategically going through 2022 and the upcoming years is those three directors. And as we develop the amount of work, what drives work, what creates work, how do we prioritize things, that will then inform how we model the teams that report to them. I delegate a lot. I ask a lot of questions. How is work getting done? How is performance being managed? But for the most part, I don't really tell the directors specifically how to model their teams. The next couple of years will be interesting because we'll be changing our org model a little bit, and we will be increasing the total breadth of the services that we offer to the organization."

INSURANCE

Page 14 – Jon Fredrickson, Chief Risk Officer, Blue Cross & Blue Shield of Rhode Island

When Fredrickson first started at BCBSRI as Information Security Officer (ISO), he oversaw the **information assurance program**, comprised of a team responsible for **governance, risk and compliance**, some **incident response**, and **threat intelligence** with limited technical responsibilities. Shortly after, he added the title of HIPAA Privacy Officer because of his extensive experience working in healthcare. Then, **security operations** was brought in under him, along with **enterprise risk management** and most recently **business continuity**. He has since transitioned from CISO to CRO, now responsible for the entire risk portfolio. Today, his programs include enterprise risk management, business continuity, information assurance, security operations, and privacy.

SOFTWARE

Page 10 – Billy Spears, CISO, Alteryx

Billy Spears looks at his security department from a functional perspective, with the traditional information security side, along with the cybersecurity side of the organization.

The information security side includes **governance, risk, and compliance**. Spears explains, "We have programs like program management and underneath that, **training**, **awareness**, **policies** and similar things. We also have our **compliance** functions. This is the review function, audit function, and regular analysis to understand where you are versus where you think you need to be. And then **risk management** assesses the rank and stack of that."

On the other side, the cybersecurity organization provides services to two different areas – the enterprise side and the software or product side. Spears says, "The enterprise is your traditional core company. That's the **front-end of the house** to make the company work. It's your **network,** your **infrastructure,** your marketing, those kinds of things."

He continues, "The product side is composed of the product or the design for what we want to build. And then that goes over to the engineers. Those are the folks that actually build the technology. And then you have the customer team that works with customers and communicates and helps the process move forward. **Product security** is heavily involved in most of those areas, and then we support the customer team in their interactions with the customers."

FINANCE

Page 16 – Sean Kearney, CISO, Natixis CIB Americas

Sean Kearney says, “I lead the **second line of defense security risk management t**eam, which provides direction and oversight to all **technology and security operations,** ranging from patch and vulnerability management to antimalware coverage, from identity and access management to secure development practices. My team and I provide the oversight and monitoring of how effectively these areas, and the controls within them, are performed. My role in a nutshell is to make sure that information security, IT security and anything related to that space is performed appropriately. I do that by owning and managing the cybersecurity program which is made up of a number of different policies and risk management processes including a robust control framework to monitor and test all key technical controls.”

WHERE DO CISOs FOCUS THEIR TIME?

We compiled high-level, top of mind areas based on feedback from our CISO community.

No programs look exactly alike, but these are potential starting point areas for building a strong program.

Risk Management
- Identify and manage risks
- Vendor risk
- Regulatory requirements
- Policies, standards, procedures
- Operational risk management

Security Operations
- Data protection
- Network and application security
- Zero Trust
- Detection
- Incident response & tabletop exercises

Identity & Access Management
- Managing identities
- Authenticating users
- Authorizing access
- Alignment with HR and other departments

Privacy
- Prepare for state privacy laws
- Understand GDPR
- Customer and employee privacy
- Address digital transformation implications on data

Governance
- Policies and procedures
- Strategy and business alignment
- Awareness and training
- Metrics and reporting

Business Enablement
- Cloud migration/digital transformation
- Communication with executives
- Justification
- Alignment with business mission and goals

Legal & Regulatory
- Compliance
- Audit
- Vendor contracts
- Investigations

Architecture
- Networking
- Application protection
- Remote access
- Defense-in-depth

Graphic by Marcela Lima, K logix

BILLY SPEARS

CISO
ALTERYX

HEADQUARTERS: Irvine, CA

EMPLOYEES: 1,500+

REVENUE: $495.3 Million

Billy Spears is currently the CISO at Alteryx, a software organization that unifies analytics, data science and business process automation in an end-to-end platform to accelerate digital transformation. As the first CISO in the organization, Spears has an opportunity to work with business leaders who support and value security as a key component to help drive the organization's technology offering forward. His focus has been on improving the security protection strategy to support overall business objectives.

SECURITY PROGRAM FROM A FUNCTIONAL PERSPECTIVE

Spears looks at his security department from a functional perspective, containing information security, cybersecurity and application security components serving the needs of the organization.

The information security program includes security-related governance, risk and compliance functions. Spears explains, "The governance function manages programs like business continuity and disaster recovery, insider threat detection and response, security awareness and training and security-related policies, standards and procedures. Our risk and compliance function are focused on security sales enablement, security risk management, third-party vendor security risk management and compliance with security-related frameworks, industry standards, internal policies and laws."

The cybersecurity program focuses on ensuring the protection of devices, networks, applications and data from threats. This program has two primary focuses - enterprise and product or application security. Spears says, "Enterprise cybersecurity includes areas like security information and event monitoring, network security, identity and access management, vulnerability management and incident response."

He continues, "Our application security team focuses on ensuring a 'security-by-design' philosophy is integrated using a 360-degree approach to proactively managing security of our internally developed products."

KEY FOCUS AREAS

Spears key focus areas include mitigating risks associated with security threats and vulnerabilities, modernizing the policy portfolio, supporting digital transformation and proactively managing security hygiene.

From Spears' perspective, CISOs are transformational leaders. He enjoys serving as a change agent working with cross-functional areas of responsibility matching the speed of digital transformation initiatives with agile, forward-thinking security strategies that consistently transform with the business to

> *"Over time you'll establish credibility within the organization and gain positive momentum as people begin to integrate security from the ideation phase and support the movement."*

deliver reliable system performance with security throughout its ecosystem amid constant and changing threats.

Companies are continuing to increase reliance on remote workforces. The work from anywhere concept has established an interesting opportunity for CISOs to consider strategic approaches for managing non-traditional security risk. He is always aiming to expand the security architecture and accelerate integration of new technologies to increase visibility and subsequently boost data protection capabilities.

To up level their policy portfolio, Spears and his governance team established modern security policies that align with industry standards and outline critical controls to protect the organization from risks. They actively partner with business stakeholders, collaboratively ensuring security requirements are utilized as guiding principles setting the tone for a positive security culture. Spears says he is fortunate to have positive support from the executive leadership team demonstrating their organizational commitment to information security as a component of the overall business culture.

Lastly, managing security hygiene is a critical component for reducing risk associated with known vulnerabilities and a key focus area for Spears and his team. They concentrate on cyber resiliency and have adopted a mindset that centers around increasing attacker costs while improving remediation responsiveness. His team gets excited about improving their cyber innovation and strategizing new approaches for reducing security risks while supporting organizational priorities.

COMMUNICATION: THE KEY TO SUCCESS

Spears says when building or strengthening a security program, it is imperative to develop strong relationships to understand the core needs of the organization. He believes it is important to work with respective business leaders and create alignment on mutually beneficial opportunities for the security team to support organizational objectives while improving security posture.

He remarks, "If you integrate too much change rapidly, you may unintentionally disrupt the ecosystem of company initiatives. Security professionals see a great deal of opportunities for improvement and naturally want to remediate everything, all at once." Spears suggests developing a risk-based prioritization of what should be accomplished then working with business leadership to build support for those initiatives spread out over a defined period. He doesn't often hit the brakes when building security programs, however he says that he has learned to take his foot off the accelerator at times to ensure success.

He also believes in embedding security into the cultural DNA of the organization. According to Spears, "Security leaders should focus on education and awareness to ensure all personnel are able to recognize and appropriately react to security risks such as email phishing or other security events." He understands the importance and value of a strong security program. Spears comments, "It's important to have a little bit of resiliency as a security leader. Each time I speak with leaders I provide some insight or a tip about a specific security theme enhancing the value of proactive security measures. Over time you'll establish credibility within the organization and gain positive momentum as people begin to integrate security from the ideation phase and support the movement."

CITIZEN DATA SCIENTISTS & PREVENTING FUTURE CYBER ATTACKS

As workers everywhere become more comfortable working with data, the ability of businesses to deliver value in data processing and analysis increases exponentially. Spears believes their ever-expanding skillset increases value by delivering actionable insights from terabytes of otherwise impenetrable data to help the company forecast, mitigate risk and fraud, deliver relevant products to their customers and improve cybersecurity defensiveness.

Spears states, "Effective cybersecurity threat hunting has always been built around the constant pursuit, near capture and repeated escapes of adversaries attempting to infiltrate a corporate network. Using a powerful analytics platform that enables machine learning capabilities is crucial to detect and address cybersecurity threats more rapidly by providing security departments with the ability to examine large volumes of data to uncover trends, identify patterns and deliver actionable intelligence."

With the further democratization of data, citizen data scientists will play key roles in helping security teams enhance and simplify their cyber defense technologies by precisely detecting future attacks, proactively identifying security blind spots across the network and protecting valuable company information.

BUILDING A STRONG CYBERSECURITY CULTURE

EXCERPTS FROM K LOGIX'S CYBERSECURITY BUSINESS PODCAST INTERVIEW WITH CHRIS HOLDEN, CISO, CRUM & FORSTER

K logix's Cybersecurity Business Podcast interviews CISOs and other security leaders to hear their advice about the business of cybersecurity. This podcast gives our listeners actionable takeaways to help them increase the effectiveness of their security programs.

In episode 15 of the podcast, we interviewed Chris Holden, CISO, Crum & Forster. Chris discusses how to build a strong cybersecurity culture within an organization.

Below, we included brief excerpts from our interview with Chris. **To listen to the full podcast episode, go to www.klogixsecurity.com/podcast**

EXCERPTS FROM Q&A WITH CHRIS HOLDEN, CISO, CRUM & FORSTER

WALK US THROUGH YOUR CAREER – WHAT BROUGHT YOU TO YOUR CURRENT ROLE AT CRUM & FORSTER?

I found the field of cybersecurity while I was in college at my alma mater Utica College, they were one of the few schools to have a cybersecurity degree, and there I focused on forensics and incident response as a minor. After college, I first started working in a forensics position for Hewlett Packard. And then from there moved on to a series of consulting roles where I branched outside of forensics into incident response, penetration testing, program development, NIST gap assessments, et cetera. I came to Crum & Forster about three or four years ago as a manager, and was promoted about a year ago to the CISO role to lead the organization's security efforts.

YOU MENTIONED YOU WERE A CONSULTANT, DO YOU THINK THAT HELPED YOU PREPARE FOR THE POSITION YOU'RE IN TODAY?

Absolutely. One of my biggest recommendations for young people coming up through their career path in cybersecurity is always to spend some time in consulting. The amount that you learn in such a short period of time working for different clients, seeing different organizations, being exposed to different facets of the industry. In such a short amount of time I was able to sit by some of the best penetration testers in the country, sit next to some of the best forensics and incident response people in the country and learn from them and get exposed to those different areas. It was imperative in my growth and my career trajectory.

YOU OFTEN HEAR HOW IMPORTANT SECURITY AWARENESS IS, BUT WHEN IT COMES TO SECURITY CULTURE, HOW WOULD YOU DEFINE WHAT A STRONG CORPORATE SECURITY CULTURE IS?

The first time I think I realized that we had cultivated a strong security culture is when I started seeing cybersecurity start as adversarial and become a department where people are proactively engaging you. I was at an organization previously and cyber was introduced as a "not to be spoken to." Why does cybersecurity always have this connotation? We're here to help. From there, it's always been an initiative of mine to be the department to come to for help in how to secure the organization.

WHERE DO YOU START?

This is actually perfect timing being in September. One of the most monumental shifts I saw was a few years back. We took a big approach to cybersecurity awareness month which happens in October. We fostered some really great relationships with our employee base that we typically don't get a lot of interaction with. It starts typically with weekly blog posts and just consistent interaction via email or the company's internal website.

IS BRINGING PEOPLE LIKE AN FBI AGENT IN HOW TO ENGAGE THEM? BECAUSE THERE'S A PERCENTAGE OF PEOPLE THAT WILL BUY-IN RIGHT AWAY AND OTHER PEOPLE THAT THINK IT'S A CHORE, IS THAT HOW YOU GET THEM TO BUY-IN?

I think that's one of the most useful things. Because not only is it our standard awareness and our standard training that we're already doing on a yearly basis, but it's entertaining. These individuals come with really interesting stories of either major

incidences that have made headlines and people are already either familiar with, or one-off incidences that affect everyday people and their personal lives as well. That definitely helps.

FROM YOUR PERSPECTIVE, WHERE DO YOU THINK PEOPLE FAIL WHEN IT COMES TO BUILDING A STRONG SECURITY AWARENESS PROGRAM?

The most obvious is having an inability to communicate effectively with the business. The best cybersecurity professionals I know talk at too technically of a level that doesn't explain the situation or the issues to the business in a way that they understand it. When you have people in HR or you have people in accounting, you have various business groups right there. Their primary goal is to do the best job at that position that they can, they're not cybersecurity experts. They should never be cybersecurity experts. They need to be cyber aware and we need to help communicate how they can effectively be cyber aware in those positions.

DO YOU EMBED YOUR STRONG SECURITY CULTURE IN YOUR VALUE PROPOSITION TO TRY AND RECRUIT PEOPLE TO COME TO YOUR ORGANIZATION?

Exactly. If I'm hiring an EDR engineer, they're not going to be isolated in that box. My goal in hiring successfully is providing career development. As you mentioned, this is a very, very competitive market right now in cybersecurity so we need to bring that extra value to entice the right individuals to join our team. In cybersecurity, the really strong individuals are the ones interested in career trajectory. If in our interviews these people are asking about training that we provide and opportunities to provide change in the environment, I find those are often the people that are truly passionate about cybersecurity and often help the most.

WHEN IT COMES TO EDUCATING, DO YOU NEED A SPECIFIC PROGRAM FOR THE OTHER EXECUTIVES BECAUSE THEY'RE SUCH HIGH VALUE TARGETS?

Yes. There is a baseline awareness program that all of our employees go through. We do run additional exercises for our executives. These are more intimate trainings on very specific use cases as decision-makers for the company. Often times, we'll have another guest speaker or presentation come in. They're very, very focused and tailored to helping these executives make decisions about the company in a cybersecurity focused way. We try to focus a little bit more on helping them understand that they are a higher value target for attackers.

IS CYBERSECURITY AWARENESS AND CULTURE SOMETHING YOU SPEND A LOT OF TIME ON, OR DID YOU SPEND A LOT OF TIME UPFRONT BUILDING A SOLID SECURITY PROGRAM SO YOU CAN FOCUS ON OTHER THINGS?

I wouldn't say that we're in the category that we spend most of our time on security awareness, there was some initial setup early on that went into designing a little bit of the program. But we have it structured now in a way that it's repeatable and consistent, but we change the content frequently enough to not make it boring and expected.

WHAT ARE THE TOP METRICS THAT YOU WOULD USE TO GAUGE THE SUCCESS IN THE ADVANCEMENT OF THE PROGRAM?

The click rates and monitoring repeat offenders in the phishing campaigns is one metric we use. Another one we've been tracking recently is we've built out an identifiable system for reporting malicious emails. Your awareness should focus not just on not clicking on those emails, but also getting the users to do the right thing in reporting those emails. If one user receives a phishing email, it's more than likely there's been a few others that have received either the exact same one or a similar email as well.

HOW DO YOU THINK THE CISO ROLE WILL TRANSFORM IN THE NEXT FIVE OR 10 YEARS?

We're more than halfway through probably one of the most active cybersecurity years in history, with all the major breaches. I think awareness is becoming a bit easier, but also requires extremely consistent and pointed communications. As an example, when some of these major breaches have occurred, like the Colonial Pipeline or SolarWinds, there was a lot of misguided concerns around those. People are aware cybersecurity is an issue, but it's helpful to get out in front of those issues and provide some context as its relevant to your organization, especially starting with your executives.

To listen to the full podcast episode, go to

www.klogixsecurity.com/podcast

CHIEF RISK OFFICER
BLUE CROSS & BLUE SHIELD OF RHODE ISLAND

JON FREDRICKSON

HEADQUARTERS: Providence, Rhode Island

EMPLOYEES: 760

REVENUE: $1.7 Billion

When Jon Fredrickson was a child, he was fixated on exploring the limits of computers as soon as he had a computer with a modem. His high school was part of the Cisco Networking Academy, providing students the opportunity to take classes that counted towards achieving the Cisco Certified Network Associate (CCNA) certification. Because he participated in that program, he was hired as an intern at American Power Conversion upon graduation.

He explains, "I began my internship working the help desk, answering the support line, and helping with similar duties. I maintained this internship through college because I went to University of Rhode Island, a short walk from American Power Conversion. I was able to come and go as I needed to with classes. Halfway through my junior year, a position opened up on the networking team. That started my information security career. Back then people weren't cybersecurity analysts or engineers, they were network engineers. So that's where I received exposure to things like firewalls and web proxies."

After working in security leadership roles at CVS Health and Southcoast Health, Fredrickson moved to Blue Cross & Blue Shield of Rhode Island (BCBSRI). With two CISO roles under his belt, he recently transitioned to Chief Risk Officer (CRO).

THE BENEFITS OF RISK + SECURITY RESPONSIBILITIES

When Fredrickson first started at BCBSRI as Information Security Officer (ISO), he oversaw the information assurance program, comprised of a team responsible for governance, risk and compliance, some incident response, and threat intelligence with limited technical responsibilities. Shortly after, he added the title of HIPAA Privacy Officer because of his extensive experience working in healthcare. Then, security operations was brought in under him, along with enterprise risk management and most recently business continuity. He has since transitioned from CISO to CRO, now responsible for the entire risk portfolio. Today, his programs include enterprise risk management, business continuity, information assurance, security operations, and privacy.

While adding the responsibility of privacy poses unique challenges, Fredrickson welcomed the opportunity to strengthen his knowledge in that area. He explains, "HIPAA guides a lot of our privacy program. The privacy rule is complex and fact specific, which can be challenging at times. There are a lot of nuances in the HIPAA privacy rule and sometimes I need help. I report to the General Counsel, so I have a team of lawyers, not at my disposal, but who I can quickly interface with for some of those tougher HIPAA legal questions. It is definitely a challenging area, but there are always opportunities to learn."

Fredrickson hopes more security leaders assume extended risk roles in the future. He comments, "You look at all of the more recent attacks and the old school, CIA triad: confidentiality, integrity, and availability. With the way ransomware's going with

extortion, it's really all about confidentiality and availability right now. And I think that if you have that higher lens or report through something that's not just IT then you'd hopefully have a better view of the organization and the impacts if a cyber event were to affect operational capacity."

The enterprise risk management department is comprised of not only cyber or IT risk, but it also extends to the entire organization. The team manages any risks that have the potential to impact the strategy, operations, finances or compliance of the organization. Fredrickson explains, "Cybersecurity is one of a myriad of risks that we monitor, and we provide the business with a framework and report all the way up to the board on what our top risks are, how we're managing them, and what our inherent vs. residual risk portfolio is. So it's not just cyber-focused by any means."

BUILDING OUT PROGRAMS AND SUPPORTING CLOUD TRANSITION

For the enterprise risk management program, Fredrickson says the next twelve months include a build out capacity for operational risk management. He says, "Today at the enterprise risk management level, you're looking at things that have not happened yet that could affect our ability to execute on our strategy. Folks will come to me and say, hey, I've got this project that's going awry, and I need help with risk management. And I respond, well, have these things already happened? Because then it's not managing a risk, it's managing an issue. So I think that the organization is now needing an operational risk management program and we're going to help do that in the next twelve months."

On the privacy side, the program is moving at an incredibly fast pace. With states beginning to adopt their own privacy laws, it is always a challenge to keep up. Fredrickson states, "Our business is moving quite quickly with digital transformation, an omni-channel experience for our members. So a lot of that is around member privacy. At the end of the day, the member owns the data, we don't own the data and we need to make sure that we stay one step ahead of that, but also enable the business with member privacy in mind."

Both the information assurance and security operations programs are undergoing a fast push to the cloud, so Fredrickson and his team are working diligently to establish the necessary guard rails to take advantage of the speed the cloud offers. They also need to ensure they keep the organization as secure as transparently possible, with business continuity being a large part of that, especially as they continue to rely on third party vendors.

FOCUSING ON THE BUSINESS

"One of my security leaders earlier in my career, had a picture frame in his office and it said something like "it's not your job to say no, it's your job to say yes, but here's how," and I've really driven my team to follow that mantra. I think that's helped us with the business. You are a partner and you're here to enable the business to do what they want to do, but we have a responsibility to do it safely and with member privacy in mind. And reminding the team to consistently do that, has driven us to have successful relationships with the business," explains Fredrickson.

For security leaders looking to build programs, Fredrickson says, "I would start with, what does my company do? What is their mission and purpose, what are their current priorities? And then make sure the framework that you've adopted makes sense for the organization, both culturally and strategically. We've adopted the NIST Cybersecurity Framework. I think it's the right size and it maps well and easily into HIPAA. But if you're a government contractor, you need to align with their regulations. So make sure it's the right fit. And then I would do a third-party maturity assessment up against that framework. Some boards prefer an independent opinion. Folks can get more funding that way and then see where the holes are. For example, you may think you are strong at protecting the organization, but your "Identify" foundation in NIST CSF might be lacking. You then need to either make people or technology investments to be more robust in that area. I would work backwards again from the business, adopt a framework, and see where the gaps are."

PRESENTING TO EXECUTIVES

For Fredrickson, relevancy is key when presenting to business executives. He says business leaders are not typically interested in hyper-specific technical metrics; security leaders must understand their audience, what their goals are, and in what capacity the security program applies to them.

Topics at board meetings typically include questions around any newsworthy cybersecurity events, so Fredrickson always includes a slide that discusses the global threat landscape. This keeps board members up to date on any threats the organization could potentially face.

Fredrickson says, "Another question from board members which I really appreciate is if I have enough resources to achieve my mission. And that's a nice question to receive, I've had a lot of educated and pointed questions about ransomware and business resilience. Even to the point where we conducted a dedicated cybersecurity session for particular board members that wanted to go a bit deeper. It was a productive candid conversation with a subset of the board that I think was pretty successful."

SEAN KEARNEY

CISO
NATIXIS CIB AMERICAS

HEADQUARTERS: New York, New York

EMPLOYEES: 700+

REVENUE: $750 Million

Sean Kearney is a people-focused leader passionate about protecting organizations by leveraging a strategic, business-aligned approach. He began his career in cybersecurity recruitment, exposing him to the industry and sparking his interest in pursuing a more technically-focused career. He then moved to a business security consultant role, working on projects such as identity and access management, risk management and compliance. As he evolved his career, he worked in the financial services industry across many security functions, from security management to architecture, risk management and more. After moving from his home in the United Kingdom to New York, he took on an Information Security Manager role at Natixis and was made CISO after six months.

Natixis is a French multinational financial services firm specializing in asset & wealth management, corporate & investment banking, insurance, and payments. As CISO for the Americas, Kearney helps enable the organization to support corporations, investors, financial institutions, and institutional clients worldwide.

OWNING AND MANAGING THE CYBERSECURITY PROGRAM

Kearney provides oversight for the first line of defense at Natixis. He explains, “First-line of defense is the hands-on security engineers, networking, and IT teams. I lead the second line of defense security risk management team, which provides direction and oversight to all technology and security operations, ranging from patch and vulnerability management to antimalware coverage, from identity and access management to secure development practices. My team and I provide the oversight and monitoring of how effectively these areas, and the controls within them, are performed. My role in a nutshell is to make sure that information security, IT security and anything related to that space is performed appropriately. I do that by owning and managing the cybersecurity program which is made up of a number of different policies and risk management processes including a robust control framework to monitor and test all key technical controls.”

Kearney’s team assesses the effectiveness of the first line of defense by identifying risks and distinguishing plans for remediation. If there is a missing patch or a recent vulnerability, his team figures out how to address it, and if necessary, determines how to report it up the chain. They also help with

> *“We must align with where the risk appetite is for the firm, what are the objectives that they want to achieve, and really get behind them and try to reduce risk as much as possible.”*

framing new and existing security risks to ensure appropriate decisioning regarding budget allocation.

Security awareness also falls under Kearney, a program that involves phishing campaigns, training workshops, seminars, posters, leaflets, and any other pertinent channels.

He continues, "My team also owns data loss prevention across email, web, physical devices, and so on. As the CISO, regulatory compliance, as it pertains to information security, is a key part of my role. I work with our regulators to ensure continued compliance with local, national, and international laws and regulations. I also have consulting responsibilities where I'll sit with the business and IT when they have new projects and new initiatives. Obviously, we need to get security involved as soon as possible to ensure security is baked into the product, by consulting on how best to meet the policy objectives that we're enforcing."

INCREASING SECURITY AWARENESS AND REDUCING TECHNOLOGY RISK

Building out the security awareness program is a top goal for Kearney to solidify a mature security culture, something that requires a large amount of time and resources. Not only does it involve effort from the security team, but the ability to change attitudes and perceptions is not a quick win. He comments, "You can see significant improvements in your risk posture, in the threats that you're facing, your capability to deal with those threats if you've adequately trained your staff. I mean, you look at any of the major breaches in the last couple of months. I'd say at least 50% of them involved the human aspect. More specifically, if we look at the latest Verizon report, 85% of breaches involve the human element. That's why it's at the top of my list."

Another top goal is a heavy focus on technology risk by ensuring their technology keeps pace with the changing threat landscape. With upticks in ransomware, targeted phishing, and social engineering, their risk management processes must be capable of moving with these shifts.

Kearney says, "Then you have compliance too. With regulators right now, cybersecurity is a hot topic as is privacy. So, for both of these, we need to react to stay on top and to stay ahead of that. Keeping a finger on that pulse and making sure that we respond appropriately to the new and expanding regulations is key."

DELIVERING WHAT THE BUSINESS WANTS TO DELIVER

For Kearney, one of his guiding principles is never losing sight of business goals. He believes security is there to support the business. He explains, "At the end of the day we are there to deliver what the business wants to deliver. We must align with where the risk appetite is for the firm, what are the objectives that they want to achieve, and really get behind them and try to reduce risk as much as possible. Doing this while being conscious that sometimes that can be a detriment for delivering those business objectives."

Kearney says to not do security for the sake of it; focus on the business and align with organizational objectives. He also says not to minimize risk just for the sake of it, it could be expensive and unnecessary, you must work with senior management and establish a risk tolerance or risk appetite they are comfortable with and then build around that.

Policies are a strong starting point, because by understanding the business, you may build your support structure to support the business in as secure a way as possible. He comments, "The old adage of "security says no" is not something that we want to reinforce. We want to make sure that security is seen as supportive. For me, I start at the top - what are the business goals? And then build policies and the program underneath that. Aligning the program to what the organization needs to achieve and making sure those control statements within the policies are the way you want them to be. As you're doing that, really start building those relationships across teams. There's no point in writing policy statements that pertain to network security controls without having spoken to anyone in networks about feasibility."

DOING YOUR PART TO INCREASE THE TALENT POOL

"We all see challenges with hiring. Yes, the talent isn't always there, but what are we doing about it on a personal basis? Are we involved in reaching out to the communities? Are we helping pro bono? Are we doing things that can increase the talent pool and encouraging diversity into our industry?

There are so many different mindsets, backgrounds, and perspectives. As a recent parent myself, I know my outlook on a lot of things have changed dramatically. People of different parental status, career experience levels, ethnic backgrounds, genders, sexual preferences and orientations, have all sorts of different outlooks which present an opportunity to solve diverse challenges. For example, who could be better to develop an inclusive and relevant awareness program than a diverse team of people who represent the mindsets, viewpoints, and diversity of the broader organization?"

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485

K logix

FEATS OF STRENGTH
SEPTEMBER 2021

CISO RESPONSIBILITIES