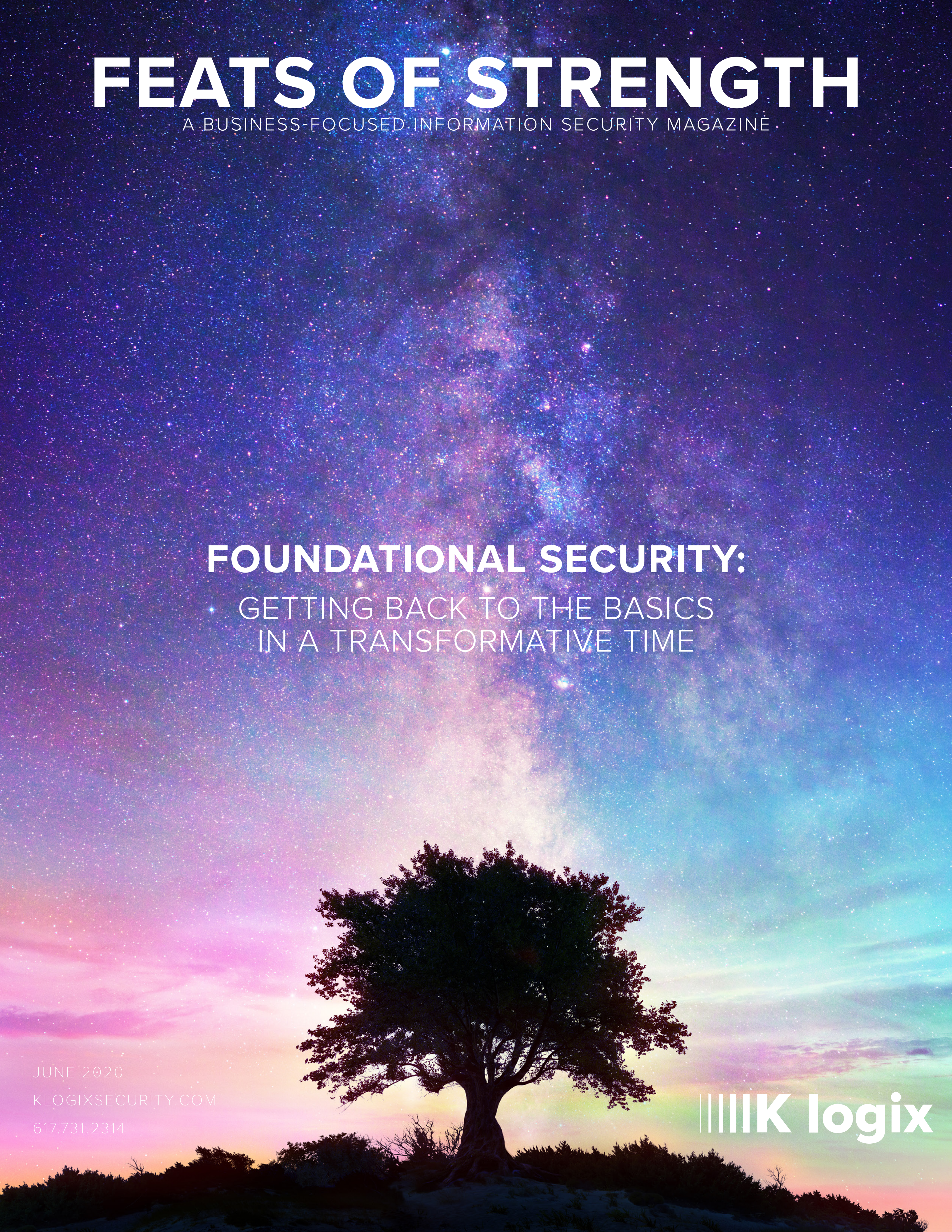


FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

FOUNDATIONAL SECURITY:

GETTING BACK TO THE BASICS
IN A TRANSFORMATIVE TIME

JUNE 2020
KLOGIXSECURITY.COM
617.731.2314

K logix

FEATS OF STRENGTH

FOUNDATIONAL SECURITY:

GETTING BACK TO THE BASICS IN A TRANSFORMATIVE TIME

JUNE 2020

FROM THE Editor

We focused on foundational security for this magazine issue because in the current COVID climate, security programs with strong foundations have an opportunity to make an impact and move at the same speed as the business. Regardless of the industry or size, businesses are accelerating to the cloud or undergoing rapid transformations, and if basic security principles are not in place, security may fall behind and not be included in strategic planning and execution. Security must ensure they move alongside the business as partners, working together towards a goal. Here are some highlights from this issue of *Feats of Strength*:

- We spoke with Mike Towers (CISO, Takeda Pharmaceuticals International) who shared that many of the highest impact breaches come in through basic ways, so we must focus on foundational security hygiene to understand where you are vulnerable and how to prioritize. You can read more about his experience on pages 4-5.
- On pages 6-7, Anne Coulombe (Data Protection Officer, MassMutual) shares how her role is like being 'glue' by piecing together similar and conflicting data protection needs.
- In our article about foundational security on page 8, we share how different leaders approach getting back to the basics. This begins with adhering to a framework, then implementing controls, processes and methodologies around identity, data security, and application security, among others.
- Bradley Schaufenbuel (CISO, Paychex) discusses the exciting challenges ahead of him in his new role on page 10. With less than a year under his belt, and significant shifts of employees working from home, he talks about plans for growth and how he remains focused on strategic business alignment.
- Another leader at MassMutual, Ariel Weintraub (Head of Security Operations and Engineering), talks about how she helps build teams and programs. You can read her profile on pages 12-13.
- We share an article on page 14 about Shifting Left and what that means for DevSecOps. I recommend reading this if you are new to the concept or thinking about using this approach in your organization.
- Joe Minieri (CISO, Orvis) talks about why back to the basics is the theme for his security program this year. He discusses his leadership style and much more on pages 16-17.
- On pages 18-19, Sue Bergamo (CISO and CIO, Episerver) goes into detail about how she approaches her dual role, as well as why it's more important than ever to focus on foundational security in today's changing climate.

I hope you enjoy reading this issue of the magazine.

Kevin West

CEO, K logix

Magazine Contributors:

Katie Haug

Director of Marketing, K logix

Kevin West

CEO, K logix

Kevin Pouche

COO, K logix

Marcela Lima

Marketing Coordinator, K logix

About K logix:

We provide information security strategic offerings, threat and incident capabilities, education/awareness, and technology services. 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 150+ 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

617.731.2314

MIKE TOWERS

CISO
TAKEDA PHARMACEUTICALS INTERNATIONAL

U.S. HEADQUARTERS: Cambridge, MA
GLOBAL HEADQUARTERS: Tokyo, Japan

EMPLOYEES: 52,000+

REVENUE: $32.2 Billion

"I've worked in bio-pharmaceuticals and life sciences for about 25 years and done a lot of work in various IT, digital and technology roles. Working in information security, I've never felt closer to the business. A lot of people across technology functions may sometimes feel isolated. They're not sure where their role may fit within the vision or mission of the company. I don't feel that way at all. I feel deeply embedded with the business and deeply embedded in what we're trying to do as a company. I'm inherently enamored with information security and don't see myself doing anything different," says Mike Towers, the current CISO at Takeda Pharmaceuticals International.

In his previous CISO roles, Towers was the first security hire, building information security programs from the ground up. At Takeda, Towers embraced the challenge of inheriting a preestablished, yet relatively young program. When joining the organization, he saw this as an interesting and exciting opportunity to take a different approach than he had in previous roles. Furthermore, Takeda was about to engage in a large-scale acquisition that would solidify them as a top 10 global pharmaceutical company and Towers was able to leverage his unique experience working in large scale business transactions of integrations, acquisitions and divestitures.

SETTING A STRONG FOUNDATION

Coming into his new role at Takeda, Tower's approach, first and foremost, focused on governance. He explains, "What type of organizational dynamics are in making decisions? What's the overall risk posture of the company? What type of reputation and/or advocacy does the security mindset or function have, whether it's an individual perspective or a collective group perspective? What importance does the company place on security? I spent a lot of time getting to know stakeholders, focused on governance, and obviously spent a lot of time on getting to know the team. Because I was inheriting a team, I wanted to get to know each and every person in the group, not only my direct reports but also the organization as a whole. That was the focus for the initial 30 days."

Towers then began integration planning that involved resourcing and operating model discussions. These discussions included evaluations of staffing, technology partners, service models, budgeting, licensing models, and much more.

After procuring a foundation of understanding, Towers laid out an 18-month strategy. Key to his strategy was benchmarking against peers in the industry. He comments, "I did some benchmarking, and then proposed areas of focus that we needed to concentrate the most on for the next 18 months. It was more of a roadmap construction, then making sure the budget and level of investment that was needed to execute some of those key roadmap items was available. I asked a lot of questions and interjected myself quickly and deeply into the day-to-day operations, so I learned by doing, if you will."

FIVE PILLARS OF FOCUS

Towers has five pillars of focus that he communicates to other business stakeholders as key strategic investment and focus areas for the information security program. These areas ensure the security program continues to make a positive impact on the organization and helps drive successful business outcomes. These pillars include:

Identity management. Towers is shifting focus from internal workforce identity to external ecosystem identity, to include others such as physicians, patients or healthcare providers. By doing so, he ensures these people have a robust identity and access experience similar to that of employees.

Analytics. Focusing on more mathematical and less traditional correlation-based analytics is a top priority for Towers and his team.

Data. For the information security team, focusing on data means understanding patterns of usage and movement, making data a real corporate asset and protecting it properly. Towers is focused on how they make data something that drives decisions, regardless of where it lives.

Product security. Understanding the manufacturing and OT environment is critically important to the security program in order to identify where ongoing protection is required. Towers notes a heavy concentration on OT environments is an industry-wide priority.

Trusted digital experiences. This includes how security partners with the business for enhancements to the digital experience, to ensure the digital landscape is built with the appropriate level of trust and security.

Towers comments, "Those are our five major strategic pillars. They have ongoing focus. I would augment them with a couple of obviously tactical focus areas. The biggest that I'm sure everybody's dealing with is what COVID is doing and how the technology solutions that COVID and the post-COVID recovery are driving to make people more safe and comfortable returning to the workplace. How do you do contact tracing? How do you screen visitors coming into your plants? Among other concerns."

BACK TO THE BASICS

Towers says his five pillars are supported by foundational security hygiene, a critically important element to his program.

He explains, "I think the focus, discipline and behavior I try to instill with my team is never taking your eyes off the ball of basic foundational security. Many well-known and reputable security studies show that a lot of the most egregious and highest impact breaches come in through basic ways. Focusing on foundational hygiene, understanding where you're vulnerable and understanding priorities, is absolutely critical. I'm a big believer in knowing before you control. So rather than diving into things like how you ramp up controls, how you protect and how you apply certain controls, you must know what you have first. Observation, discovery and gathering are important. One of the first fundamental principles of any security professional should be knowing what you're protecting. Your ability to answer that question is very, very important. And I think there's also a very fundamental and strong delineation and requirement to make sure that all this is built into the culture, that these basics aren't unimportant just because they might be older."

Providing Leadership During Acquisition

Before joining Takeda, Towers was made aware of an upcoming large-scale acquisition of another pharmaceutical organization, something he would play a role in during his first few months as CISO. Because he was new to the organization, Towers felt he brought an unbiased perspective during the process of merging the acquired organization's security program with the security program he oversees.

He says, "I got to look at both security programs independently. We did what we call a CARS exercise: continue, accelerate, reduce or stop. We had to make room for some of the areas that were being done that frankly weren't going to add any value moving forward. We took a really good objective look at the program and I appointed my new leadership team within eight weeks of day one. We were able to have some stability in place quite quickly, and then we were able to appoint the rest of the organization within the next month or so after that. I had an opportunity to pull the team together into a cohesive unit very early on."

ANNE L. COULOMBE

DATA PROTECTION OFFICER, MASSMUTUAL

HEADQUARTERS: Springfield, MA

EMPLOYEES: 7,500+

REVENUE: $32.5 Billion

Information security has been woven into Anne L Coulombe's extensive career for over twenty years. Coulombe currently works at MassMutual, where she started as a Business Information Security Officer (BISO) which then grew into her current role as Data Protection Officer (DPO). As BISO, Coulombe took elements of typical CISO responsibilities and applied them to a particular line of business. As DPO, her scope is broadened to the enterprise but narrowed in focus to protecting data.

She explains, "My responsibilities from BISO to DPO changed in part with the relationship between myself and the lines of business. From a BISO perspective, you are considering security elements, attack surface and controls linked directly to where the business is headed. As the DPO, I focus on protecting the data itself. Data is a broad definition from classification to inventory, to tagging and exfiltration tools for data loss prevention. In some ways I've narrowed my focus. On the other hand, there is opportunity for broad influence across the entire enterprise."

FORGING A DATA PROTECTION ROLE

Coming into the DPO role, Coulombe had an opportunity to forge a new program spanning many departments and program areas. In her day-to-day, Coulombe focuses on securing customer and company data while minimizing the proliferation of restricted data throughout the environment, reducing business risk, decreasing the cyber-attack surface and securing core business processes. Working at a large company, Coulombe's role is to unite data protection in cybersecurity and work with partners in compliance, privacy, law, enterprise risk and data governance. She also spends time educating employees and providing awareness regarding the data protection program and how every employee has a role in protecting data.

She comments, "A Data Protection Officer focuses on cybersecurity, yet crosses into privacy regulations and laws that exist in different geographies. Part of the role is understanding how all of those pieces and parts come together. It's like a puzzle that you have to put together over a period of time. Not an easy role for somebody to walk into on day one. The best is to gather experience in different areas of business, cyber security and privacy and then bring it together to be the DPO."

The role relies on being business-minded in order to service enterprise needs while reducing risk and must align the business desires with what data is most relevant and important to secure and protect. Being a strong communicator is vital, and influence management skills are used daily while working with other groups within the organization.

Coulombe continues, “The role could be for someone who came out of privacy and added cybersecurity or somebody out of cybersecurity who has added privacy or even worked directly with a set of regulations. In my case, I prepped for GDPR as it came into force with the European area of a previous employer. Someone coming into this role must be business-minded and a good communicator. In this role you are constantly evaluating what data type and quantity need to be secured and ensure consistency. It’s important to understand influence management because it is a role that includes extensive awareness and working with multiple groups.”

UNDERSTANDING THE ROLE OF DATA PROTECTION

Data protection functions have often been wrapped into a Chief Information Officer or Chief Data Officer. Coulombe explains, “Both of those roles in my opinion are slightly different. A Chief Data Protection Officer is somebody who has CISO-type skills yet is focused on data and protecting it in a variety of ways. Not just to focus on understanding what data and its classification, but now its use, how the data is replicated or transformed, the geographies in which the data lives, data flows between systems and access controls, and assessment of how it’s protected. Who and how access is granted and controlled is also a portion of the role.”

She continues, “My role is similar to being ‘glue’ as much of what I do is piece together both similar and conflicting data protection needs and ensure communication between different functions within the enterprise. Data is incredibly critical. If you wish to go back to the very basics, one for me is to make sure that there is a clear and well- communicated data classification. Everyone understands the classification, focus on the most critical data such as SSNs; everyone knows what they need to protect these SSNs at all times and in all uses.”

One key aspect of data protection programs is the strong alignment to corporate business goals in order to establish clearly defined deliverables and work towards improving and positively impacting the organization as a whole. Coulombe explains, “What I do ties directly into the company mission and vision, which includes securing customer data. It’s security, it’s protection, it’s enabling, it’s helping. It’s educating. As a mutual insurance company, we protect customers and company data in a similar manner, as it is foundational to the to the way that the company operates.”

LEADERSHIP

Constant learning and career evolution are Coulombe’s top priorities for her team. She says the methodology for achieving that differs person to person, depending on the individual and their learning style. For some people, being immersed at a conference for days provides them the appropriate training and growth, whereas others may need more technical hands-on trainings, or to spend time with an online course. Coulombe leverages a diverse set of mechanisms from an educational standpoint to accommodate how each individual on her team learns differently.

Providing leadership to her team is not a one-size-fits-all approach. Coulombe explains, “My leadership style varies. I say that because I’m a pattern watcher. I see trends and anomalies very quickly, and that’s a net advantage. It also means that from a leadership style, I must plant many seeds so people around me are able to come to some conclusions themselves and understand the path forward. Part of that is being able to open people’s eyes to what they may not have seen at first or second glance. There’s some tough love as well, by making sure that people around me, including my direct reports and other people I work with, stretch themselves. It’s being able to help them through those different endeavors. I activate interest and hidden skills in other people as there is no way to succeed in cybersecurity without a team working together.”

To ensure Coulombe herself continues to grow and learn she absorbs information from others, reads relevant publications, or listens to audiobooks. Along with focusing on key corporate goals to expand and innovate the data protection program, she is also focused on the CCISO certification, an industry-leading program that recognizes the real-world experience, something she is hoping to achieve by the end of 2021.

BACK TO THE BASICS

Coulombe says the definition of back to the basics does not mean go back to your tried and true software. Since threat actors are savvy and adaptable, we must adopt a new view to create edges where edges may not have been before or soften some things that may have been hard.

She comments, “There is some reality of having to secure the basics, absolutely. However the method in which you do so must include non-conventional controls. Threat actors already understand the basics, and they target a company for monetary gain or disruption purposes. They know what your typical large company is utilizing in terms of services and different software, therefore a layered approach reduces access to both easy and critical asset targets. Think like a threat actor targeting your infrastructure or your data, it helps us come up with methods to trick and catch the bad actors, be creative and be a step ahead as often as possible.”

FOUNDATIONAL SECURITY

GETTING BACK TO THE BASICS

By Katie Haug

We spoke with many CISOs and security leaders who told us one of their top strategic priorities this year was a heavy focus on foundational security, or getting back to the security basics.

There is an increased focus mainly due to the business implications stemming from the current COVID climate. Businesses are rapidly transforming to address remote workforces and shifting priorities, something security has an opportunity to be part of, from initial planning to execution and implementation.

The focus on foundational security areas allows security programs to ensure they are covering core components of a strong, business-driven and mature security program.

This is vital particularly in regards to the heavy clutter of security technologies available in the marketspace, labeled 'next gen' or flush with marketing buzzwords. Attentions may shift and priorities change with leaders becoming sidetracked from securing their core areas of security. There is such thing as buying too much technology too fast, which may solve one problem, but as risks increase and priorities shift, the technology may not keep up, or may require extensive and ongoing operationalization. This results in a drag on resources and a lack of clearly defined outcomes for many technology investments.

Furthermore, as cloud adoption continues as a top priority and businesses transform at rapid paces, security programs must ensure they have strong, solid foundations in order to transform at the same rate as the businesses they support.

Many CISOs' approach foundational security differently based on their specific business goals and technical requirements. For example, in her profile on pages 6-7, Anne Coulombe, Data Protection Officer, MassMutual says the definition of back to the basics does not mean go back to your tried and true software. Since threat actors are savvy and adaptable, we must adopt a new view to create edges where edges may not have been before or soften some things that may have been hard.

Anne comments, "There is some reality of having to secure the basics, absolutely. However the method in which you do so must include non-conventional controls. Threat actors already understand the basics, and they target a company for monetary gain or disruption purposes. They know what your typical large company is utilizing in terms of services and different software, therefore a layered approach reduces access to both easy and critical asset targets. Think like a threat actor targeting your infrastructure or your data, it helps us come up with methods to trick and catch the bad actors, be creative and be a step ahead as often as possible."

Frameworks

84% of organizations utilize one or more of the three main information security frameworks. Possessing a strong approach to solidifying alignment to a framework ensures a clear plan and provides a method of tracking maturity.

On page 16, Joe Minieri, CISO, Orvis says, "First, I am ensuring that my security program covers the basic requirements sufficiently. There's a number of good standards and guidelines available. I start by trying to demonstrate how I measure up to the chosen standards. Often, processes that were implemented years ago may become laxly implemented now. Sometimes we think we're doing something completely, but not testing for thoroughness. When we test, we find out we've been missing things. This is how to identify gaps that need to be filled – either by reinvigorating a process that's become slack or by finding a new piece of technology that does something we're missing."

The most followed security frameworks include:

NIST: The National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity is used by 29% of organizations. NIST is a voluntary framework intended primarily for critical infrastructure organizations to manage and mitigate cybersecurity risk based on existing standards, guidelines and practices.

CIS Controls: The Center for Internet Security Critical Security Controls is used by 32% of organizations and includes a set of 20 actions designed to mitigate the threat of common cyber-attacks.

ISO: Used by 35% of organizations, ISO 27001 is the international standard that describes best practice for implementing an ISMS (information security management system). Achieving accredited certification to ISO 27001 shows that your company is following information security best practices and delivers an agnostic expert assessment of whether your data is adequately protected.

Program Areas of Focus

While foundational security may mean different things to many CISOs, here are some of the key areas CISOs shared with us as areas of focus:

Identity and Access Management (IAM):

IAM is the process of defining and managing the roles and access privileges of individual users, and the circumstances in which users are granted (or denied) those privileges. To ensure you have a strong IAM program, you must be able to understand what assets you have and who has access. By managing IAM policies, programs and technologies, you may reduce identity-related access risks within your business.

CISOs should holistically look at their IAM program to identify gaps and make holistic plans to close the gaps and increase maturity.

Data Security

Data Security is a process of protecting files, databases and accounts on a network by adopting a set of controls, applications and techniques that identify the relative importance of different datasets, their sensitivity, regulatory compliance requirements and then applying appropriate protections to secure those resources.

By protecting data from unauthorized access and data corruption, CISOs evaluate and reduce any risk that comes with storing different types of data.

Application Security

CISOs are focusing on security measures at the application level aiming to protect critical data from external threats by ensuring the security of all software running within the business. This area of security helps identify, fix and prevent security vulnerabilities in any kind of software application.

According to many CISOs we spoke with, checking for security flaws in their applications is essential as threats continue to increase. With rising complexity and sophistication in threats, especially in changing socioeconomic climates, application security becomes more important than ever.

Strong Security Culture

On page 18, Sue Bergamo, CIO and CISO, Episerver, comments, “I think that getting back to the basics right now is around making sure that you don’t have any holes in your environment. We must ensure we are not taking our foot off the pedal with educating our consumers, employees, and spheres of influence on the importance of staying vigilant and focused on protecting ourselves because unfortunately cybercriminals are not on holiday.”

She continues, “I think these devices, laptops, desktops, whatever you have in front of you, are the most vulnerable right now, especially from a work at home standpoint. As a CIO and CISO, I make sure that our endpoints are protected. I have employees all around the globe, I can’t support all routers in everyone’s home. No one can. So you have to make sure that your employees are educated on how to configure a router as best as possible to make sure that it’s encrypted, to make sure that it’s not open and noticed from criminals that are hanging around, and that it’s locked down and protected through a key. That’s just step one. It’s the device, the most vulnerable piece of the puzzle, that’s where things get in.”

By holding employees responsible, they become pivotal components of a secure enterprise. As workforces shift to working remotely, having an embedded security culture means each member of the organization is accountable for meeting specific security protocols and standards.

BRADLEY SCHAUFENBUEL

VICE PRESIDENT & CISO
PAYCHEX, INC.

HEADQUARTERS: Rochester, NY

EMPLOYEES: 14,000+

REVENUE: $3.38 Billion

Bradley Schaufenbuel has over two decades of experience working in information security. He earned his Master of Laws and Juris Doctor degrees from the University of Illinois at Chicago's John Marshall Law School and is a licensed attorney and a member of the United States Supreme Court Bar. Not only does this provide him with a unique perspective when working through information security challenges, but he is able to leverage law-related skills in his everyday work.

As an avid proponent of continued education, Schaufenbuel also has a Master of Business Administration degree from DePaul University. By combining his undergraduate, masters and law degrees, Schaufenbuel brings a well-rounded business-focused mindset to any role, allowing him to approach his responsibilities from a strategic viewpoint.

Schaufenbuel's career spans information security roles at banks, insurance companies and professional services firms. He quickly gained a robust set of responsibilities early on in his career, which helped him move into leadership roles with growing responsibilities. Most notably, Schaufenbuel has assembled and led information security teams, built programs from the ground up, aligned security with corporate objectives, and solidified himself as a business-focused, innovative leader.

EXCITING CHALLENGES IN A NEW ROLE

Currently, Schaufenbuel works as Vice President and Chief Information Security Officer at Paychex, a role he began in September of 2019. Founded in 1971, Paychex is a recognized leader in the payroll, human resource, and benefits outsourcing industry, supported by over 14,000 employees. As an industry leader, Paychex serves businesses in the United States, Germany, Denmark, Norway, and Sweden. According to their website, Paychex supports approximately 670,000 payroll clients across more than 100 U.S. locations, and pays one out of every 12 American private-sector employees.

The opportunity to take on the CISO role at Paychex was brought to Schaufenbuel while he was working at a smaller payroll organization in Chicago. While he enjoyed his time at his previous organization, Schaufenbuel felt he was in a comfortable place after building and maintaining a resilient security program and team. He was ready to take on a new challenge at a larger organization.

He felt joining as CISO at Paychex, he would be in a position to execute on his strategic plans in a supported manner from the business entities and organization as a whole.

STRATEGIC GOALS FOCUSED ON BUSINESS ALIGNMENT

Schaufenbuel has four main strategic goals to continue to protect the organization and its customers while aligning with the overall corporate strategy. These include:

Improving the overall maturity of the information security program. Schaufenbuel explains, “We are focused on benchmarking against NIST and measuring the maturity of each of the 108 controls as implemented at Paychex using the CMMI model. Our goal is to get all controls operating at a high-level of effectiveness to eventually achieve the AICPA Cyber Risk Management attestation.”

By focusing on NIST alignment and maturity, Schaufenbuel and his team will continue to improve their management of cybersecurity risk, not only internally within their program, but externally within other business units of the organization. Tangible maturity ratings and methodologies allow Schaufenbuel to communicate risk in a business-oriented manner, strengthening security and the organization.

Enabling the organization to innovate rapidly and safely. In order to address digital transformation in a secure manner that does not impact productivity, Schaufenbuel is focused on a “shift left” mentality.

To help maintain a leadership position in the industry, Schaufenbuel says they are adopting agile development methodologies and DevSecOps practices. Through shifting left, processes are automated and performed earlier in product development lifecycle, something that helps drive innovation faster and more securely.

He comments, “Our goal is to get security involved earlier in the development of new processes, products and strategy. I want to make sure we embed security into that thinking from the very beginning rather than bolting it on at the end. For example, typically, software developers develop code which is placed into production, then security comes in and tests for any issues. When security does find issues, they may be expensive to fix and take time away from pushing out new code. With shifting left, security is baked in at the beginning, which helps avoid costly adjustments.”

Embedding a security mindset into the organization’s culture. According to Schaufenbuel, people can often be the weakest link. He believes an organization is only as strong as their employees, and without investing time and resources into a strong security awareness program, the organization may increase their risk.

Schaufenbuel says, “I am equipping every employee with knowledge to safeguard themselves and the organization from cyber threats. By requiring all employees to go through information security training, they can continue to implement these practices every day.”

Making information security an area of competitive differentiation. Since security is a pivotal area of focus for the organization, in some capacities Schaufenbuel interacts with customers and works with other departments to create customer-facing security messaging.

He explains, “I don’t want to just enable the business. I want us to have such a strong security program that cyber resilience is one of the reasons prospects choose to do business with us. It requires continuous work and I’m focused on making a positive impact in this manner.”

LEADERSHIP AND PERSONAL GROWTH

Schaufenbuel says he is a servant leader with a serve-first mindset, focusing on empowering and uplifting his team. He continually focuses on ways in which he can help enhance the development of his team members to unlock or grow their potential and creativity. He pursues ways to develop and align each team member’s sense of purpose with the company mission.

He comments, “I like to surround myself with people smarter than myself. I focus on hiring people who are problem solvers and critical thinkers. Learning from my team is incredibly valuable.”

For his own personal growth, Schaufenbuel believes in continuous learning and holds over 25 certifications, ranging from information security, ethical hacking, computer forensics, fraud prevention and project management. He also leverages his professional network to help him overcome challenges. He says, “I can send a message to my professional network and get thirty responses. These come from CISOs and security leaders across the U.S. facing the same challenges as myself.”

He is also prolific author and speaker and serves on the advisory boards of multiple venture funds and startups.

ARIEL SALDIN WEINTRAUB

HEAD OF SECURITY OPERATIONS AND ENGINEERING
MASSMUTUAL

HEADQUARTERS: Springfield, MA

EMPLOYEES: 7,500+

REVENUE: $32.5 Billion

Although Ariel Saldin Weintraub did not set out to have a career in information security, her interest in the field grew while working as a consultant in a technology advisory practice. After acquiring her bachelor's degree in business, she started at one of the big four consulting firms. During this time, while working with a specific client, she had a one-off opportunity to join their security team to help with a penetration test.

She says, "I'm definitely a 'fake it till you make it' kind of person. I decided to take that penetration testing opportunity and use some of the things I remembered from a security class I took in college. However, I figured out how to do the majority of the penetration testing by purely hands-on work. The engagement was one week, and after it was done I decided I didn't want to go back to the other part of the practice I was in; I wanted to switch to the security practice. Since then, I've always worked in the cybersecurity space, and most of what I've learned has always been hands-on. I did end up going back to school and getting my masters to fill in some of the more focused computer science concepts that I had missed with having a business degree."

Weintraub worked in a number of organizations, moving her way up to information security leadership roles while gaining a robust breadth of experience. In her current role as Head of Security Operations and Engineering at MassMutual, Weintraub mainly focuses on security operations and talent development.

FOCUSING ON BUILDING TEAMS AND PROGRAMS

Weintraub says, "I'm really drawn to opportunities that give me the chance to leverage the more creative side of problem solving. The role I'm in now gave me an opportunity to focus on the deep technical aspect of what I've always loved within security operations, but also on ways to improve some of our talent development and retention challenges. I don't love running an existing function that's already operationalized and very mature. I really like to get involved in the details and help solve problems, getting involved in the day-to-day with the team. Then, I like to move on to something else when the new functions and teams are established. This role was a healthy combination of those two things: part of the team was already functioning at a pretty high level of maturity, while other aspects of the team needed more rebuilding. I liked the idea of being able to do a little bit of both."

Weintraub brings together different functions of team integration that might not historically interact and aligns these areas with new capabilities. She enjoys responsibilities that enable her to work within various groups and develop her

> *"I'm really drawn to opportunities that give me the chance to leverage the more creative side of problem solving."*

skillset in a holistic manner. The teams she manages didn't previously report into the same leader. Since she was the first individual in her specific role within the organization, she has been able to develop foundational principles and educate other departments on what the role means to the organization and security function.

Weintraub is focused on building a diverse talent pipeline. She explains, "We're building a global security operations center or SOC that we're looking to use as our source of talent for the rest of the cybersecurity organization. We bring people into the SOC and then after a certain period, move them into another role that is mutually beneficial. They learn a broad knowledge of different domains that they can bring into the new program that they move into. As part of staffing some of our new SOC locations, we're partnering with external organizations that focus on recruiting and training diverse talent; in particular, women, veterans and minorities that come from underprivileged backgrounds, or people that may have not had the opportunity to obtain a four-year degree."

She is also focused on integrating data science and implementing automation into their programs. By leveraging a combination of the in-house data science team as well as vendors that focus on machine learning and other data science capabilities, she hopes to evolve the organization while reducing risk.

LEADERSHIP STYLE AND COMMUNICATION

Weintraub follows the transformational leadership model. She comments, "In particular, we're introducing a lot of new programs and capabilities that require a lot of change. This impacts our organization and a lot of other areas of the company. The more you empower the team to self-motivate and make their own decisions, the more likely they are to come along in that journey. Our strategy is transforming from compliance-based to risk-based, which can be a significant amount of work and shift in how you think. I try to empower my leaders to motivate and encourage their teams."

Throughout her career, Weintraub gained different skillsets by diversifying the types of responsibilities she performs. She enjoys challenging herself to gain broader exposure to different aspects of information security, including cyber risk. She leads by example and focuses on always being able to see the bigger picture in order to deliver positive results and impact change.

WOMEN AND SECURITY

"As I mentioned, one of my mottoes is 'fake it till you make it', but it's also about empowering those around you to do the same. That's why I'm passionate about encouraging more women to join the industry - sometimes the number of men can be intimidating, as is the technical nature of the domain. It's about encouraging people to take a chance. In general, I'm very passionate about women in cybersecurity. And that's why I continued to look for opportunities outside of my day-to-day. This month I'm officially joining as a board of director for the ISACA One in Tech Foundation, which has a few different missions; one is empowering women in technology. Another focuses on enabling technology for underprivileged areas. Those are the kinds of things that I am excited about. I look for ways to give back to the community and be involved in things outside of my day-to-day," says Weintraub.

She continues, "In terms of how my career evolved, I've been really fortunate to have participated in organizations dedicated to advancing and promoting women in cybersecurity. I'm on the board of advisors for an organization called the Executive Women's Forum. Since I first joined that group as an attendee, I've seen a really big change in the number of women in the field. I think there's still more we can do to continue to empower and encourage more women to join."

SHIFT LEFT
THE RISE OF DEVSECOPS

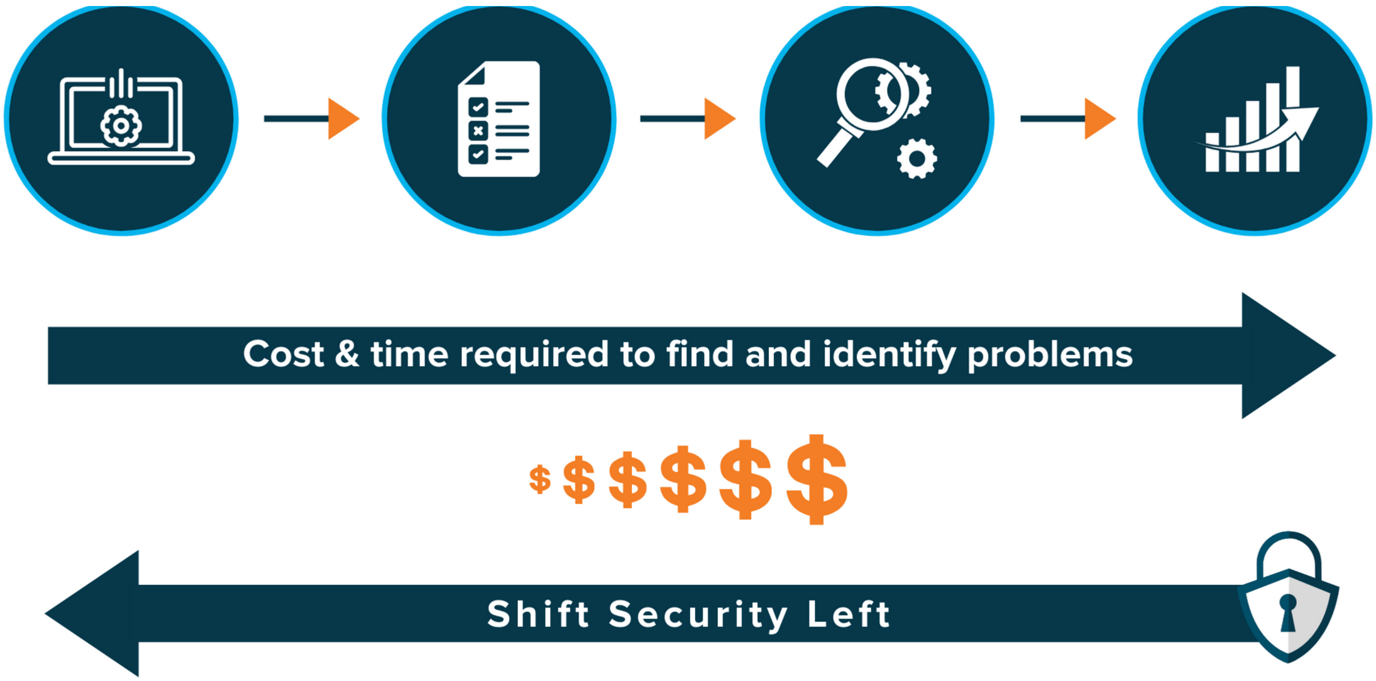
By Katie Haug

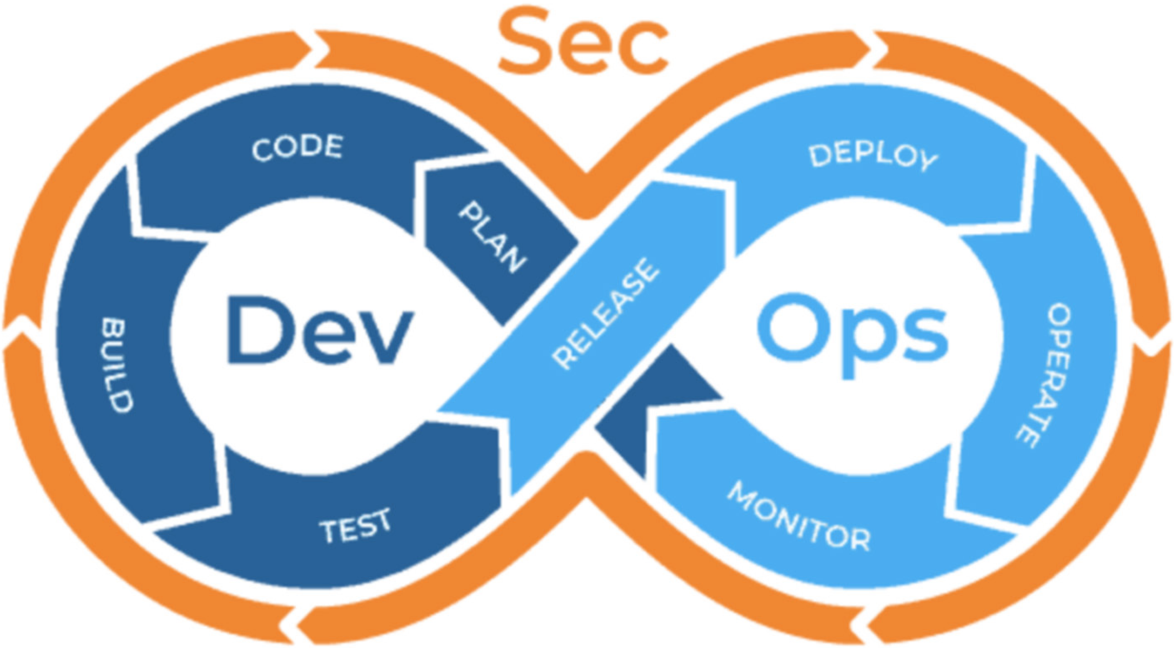
Many CISOs we speak with talk about their focus on a Shift Left approach, a popular term in the DevOps community. Shifting Left means information security is built into the application process from the beginning of the development lifecycle. When processes are performed earlier in the development lifecycle, including security checks and audits, it becomes easier to find flaws and potential issues, and resources are used more efficiently. By doing so, CISOs and their teams are able to mitigate the risk potential security concerns pose to both the delivery schedule and end users.

In order for security teams to enable the DevOps process, strong collaboration is required to transform into what is known as DevSecOps. DevSecOps means security teams working closely with the DevOps teams to address security concerns as early in the development lifecycle as possible.

But what does shift left mean? Shifting left refers to the effort by a DevOps team to implement measures to ensure application quality at an early point in the software development lifecycle. In the case of application security, this means implementing measures to ensure security concerns are taken into consideration while the application is being developed, rather than at the end of the process.

On page 10 Bradley Schaufenbuel, CISO, Paychex says, “Our goal is to get security involved earlier in the development of new processes, products and strategy. I want to make sure we embed security into that thinking from the very beginning rather than bolting it on at the end. For example, typically, software developers develop code which is placed into production, then security comes in and tests for any issues. When security does find issues, they may be expensive to fix





and take time away from pushing out new code. With shifting left, security is baked in at the beginning, which helps avoid costly adjustments."

Benefits of Shifting Left

Accelerating Speed-to-Market

With an end goal of increasing quality and reducing the amount of time required for testing, Shifting Left solidifies both of these are met. By waiting to evaluate later in the development lifecycle, the cost of fixing any security concerns significantly increases.

Improving Security Protections

Historically, development teams may have been reluctant to implement or engage in a Shift Left approach because they believed involving security too early in the process may delay or complicate a project. However, DevOps has changed in recent years, and Shifting Left has become increasingly practical, and a best practice in the worlds of both DevOps and security.

Implementing Shifting Left

Shifting Left begins with establishing collaboration between the entire security and DevOps teams. Integrating the importance of security into the workforce culture purports responsibly among all individuals within an organization. Ensuring this buy-in is vital for success. For example, developers must be bought into the Shift Left approach when they code with security top of mind.

CISO and security leaders should encourage their teams to engage in regular conversations about application security via the development process. Security must continue to speak with their developer counterparts so Shifting Left becomes embedded in their process.

Testing is also key in ensuring shifting left takes place. Testing automation and continuous integration are vital components and things to be mindful of, especially as developers are becoming comfortable with Shifting Left.

JOE MINIERI

CISO, ORVIS

HEADQUARTERS: Sunderland, Vermont

EMPLOYEES: 1,700+

REVENUE: $220 Million

> *"FIRST, I AM ENSURING THAT MY SECURITY PROGRAM COVERS THE BASIC REQUIREMENTS SUFFICIENTLY. THERE'S A NUMBER OF GOOD STANDARDS AND GUIDELINES AVAILABLE. I START BY TRYING TO DEMONSTRATE HOW I MEASURE UP TO THE CHOSEN STANDARDS..."*
>
> *- JOE MINIERI*

Joe Minieri's first involvement with information security was while building and maintaining an internet e-commerce infrastructure in the mid-1990s, where he secured the network and monitored for suspicious behavior. From there, his career in information security blossomed as he progressed into leadership roles with growing responsibilities and strategic direction.

In 2006, Minieri became the Information Security Officer at General Dynamics, a global aerospace and defense company, where he had strong support to mature the information security program. The organization's leadership believed in making investments to ensure they became a center of excellence for information security. Since only a limited security function existed, Minieri was tasked with coordinating security across the organization to push out standards, develop a robust program, and ensure the entire workforce recognized the importance of being secure.

After leaving General Dynamics, Minieri worked at L.L.Bean to help re-build their security program, address regulatory issues, invest in security program components from the ground up, hire a productive team, and establish a strong forward-looking plan for growth and innovation.

In 2019, Minieri became the CISO at Orvis, a Vermont-based fly fishing and outdoor product and services retailer. At Orvis, Minieri is responsible for the entire security strategy, the execution of security and regulatory compliance, incident response, as well as overseeing fraud prevention capabilities.

FOCUS ON BACK TO THE BASIC SECURITY

Minieri's theme for the security program this year is 'Back to the Basics'. He says, "First, I am ensuring that my security program covers the basic requirements sufficiently. There's a number of good standards and guidelines available. I start by trying to demonstrate how I measure up to the chosen standards. Often, processes that were implemented years ago may become laxly implemented now. Sometimes we think we're doing something completely, but not testing for thoroughness. When we test, we find out we've been missing things. This is how to identify gaps that need to be filled – either by reinvigorating a process that's become slack or by finding a new piece of technology that does something we're missing."

In order to determine the organization's security maturity, Minieri's first step was assessing specific facets of the security program including processes and policies in place. He was able to identify where gaps existed and devise a strategic plan to take actionable steps towards increasing maturity.

He is also focusing on maximizing the investments in their environment. Similar to many CISOs, Minieri inherited technology and processes that were purchased and implemented by other people. He explains, "I'm inheriting the results of the implementation of someone else's vision, or, worse, an implementation without a vision. Some of the investments may have been forgotten about by current employees or purchased by people who are no longer at the organization. In a new environment, you may need to sit down with finance to see what you're paying for and taking a bottom-up approach to the budgeting process."

To ensure he is maximizing their investments, Minieri first looks at everything from hardware to software and tries to whittle down the portfolio to only essential products. This may require a balancing act of removing several products in order to replace them by just one investment. By approaching it in this manner, Minieri is armed with strong justification for his decision.

INVESTING IN NEW TECHNOLOGY WHILE FOCUSING ON THE BASICS

Minieri recommends surveying all investments you already have before purchasing anything new. By doing so, you are able to see if there's potential to leverage an existing investment by operationalizing certain functions instead of having to purchase a brand-new technology.

Minieri comments, "I have found that we often already have the products we need in place; they may not be completely deployed or efficiently operating. Here, I'd invest time to tune an existing platform. I may already have a solution that will get me most of the way toward meeting my objectives. If the survey reveals the products are obsolete and need to be replaced, then I can show savings by decommissioning old gear and unused software. In a tight budget cycle, I've often been able to get funding on new projects by showing an overall savings in my budget through sunsetting old technology."

An important investment to evaluate is a Managed Security Service Provider to determine if the service they provide is still necessary and functioning appropriately. Minieri explains, "I've been able to in-source some functions at a lower cost while providing an equal or better service; this is a no-brainer. For services that we're not ready to in-source, rebidding the service and finding a better provider at the same or less cost has also been very successful for us. Once your product portfolio has been optimized, you're in a much better place to start thinking about what new technology you really require. By showing that you've maximized investments previously given to you, you'll have an easier time justifying new acquisitions."

SECURITY IS BUSINESS AS USUAL

Minieri likes to use the phrase 'security is business as usual', where the security program is streamlined and able to keep pace with the business transformation in a seamless manner. This occurs when processes and policies are in place and the team is efficiently operating to a point where it becomes muscle memory for them to execute.

Minieri says, "When I've been able to help mature a security organization to this level, we then have the bandwidth to work with the business to understand what they need and, usually, have it ready when they need it."

LEADERSHIP STYLE

As a volunteer Firefighter/EMT, Minieri must making fast-thinking critical decisions, something he leverages in his work as a CISO.

He explains, "As a volunteer Firefighter/EMT I'm often part of a team making critical decisions that affect people and their property. We rarely have time to 'meet to prepare for the meeting' but instead, are quickly assessing a situation, sizing up our resources and tackling the problem right away. This translates to cyber incident response activities easily, but also more mundane work like prioritizing and executing tactical tasks."

SUE BERGAMO

GLOBAL CIO & CISO
EPISERVER

HEADQUARTERS: Nashua, NH

EMPLOYEES: 800+

REVENUE: Undisclosed

Sue Bergamo is currently the Global CIO & CISO at Episerver, a computer software organization offering a content management and commerce platform powered by AI-backed data and personalization tools. Bergamo works alongside executive management and a worldwide team of business resources, developers and infrastructure engineers, to deliver secure and innovative solutions within Episerver's data centers and cloud services. She is responsible for creating and executing on a global IT and Security strategy, as well as operating as a hands-on business and systems architect to develop mission critical solutions. Notably, Bergamo led industry compliance initiatives in ISO 27001 and GDPR.

EVOLVING INTO A CIO AND CISO

Bergamo says September 11th put cybersecurity in more of a pivotal position, when many people began to realize not everyone sitting behind a computer had good intentions. She saw an escalation of cyber-attacks, with a growing uptick not seen prior to 2011. This sparked many organizations to begin to see the need for a CISO and a heavier focus on protecting their organizations from a cyber perspective.

She says, "The CIO continued to have to provide security services for their companies. They started going in front of boards to make sure that companies were secure and that the board members understood how secure the company was. We put ourselves on the line. We had to ask for investments where there may not have been some or not enough in the past."

Bergamo says as the world continued to turn from a security standpoint, the different cyber hacks and attacks started getting more malicious and frequent. At the same time, additional software and vendors were coming into the marketplace with different toolsets, and it did not matter what role you had in security or IT, you could not help but realize security needed to be a component of your job.

To address this heavy shift of focus onto cybersecurity, Bergamo challenged herself to get a Master's degree in Cyber with a minor in International Terrorism to formally educate herself on the growing industry. She explains, "That has lended me very well, not just having the credentials, but combining the education with the on-the-job experience. This has led me to branch out and get a role as a CIO and a CISO and combine both pieces of that into one really terrific global company."

FOCUS ON SECURITY BASICS

"Getting attacked is a constant stream, but it's the defending around those attacks that makes us good CISOs, and again, protecting our company and protecting our employees. When this pandemic hit, I was talking to my peers about three types of companies out there. There were those that were prepared, those that were semi-prepared and those that weren't prepared at all. Those in the latter category are really in a world of hurt right now," comments Sue.

With cyber-attacks on the rise in the current environment, Sue says going back to the basics is around making sure we are protecting ourselves and spending time to make sure there are no holes in the environment that a cyber criminal can crack through. She believes it goes beyond network and infrastructure, that it is also about employees.

Many employees are currently working from home, with additional pressures outside of work, making them more vulnerable or distracted to engage in risky behavior such as clicking on a phishing attempt. She explains, "I think that getting back to the basics right now is around making sure that you don't have any holes in your environment. We must ensure we are not taking our foot off the pedal with educating our consumers, employees, and spheres of influence on the importance of staying vigilant and focused on protecting ourselves because unfortunately cybercriminals are not on holiday."

She continues, "I think these devices, laptops, desktops, whatever you have in front of you, are the most vulnerable right now, especially from a work at home standpoint. As a CIO and CISO, I make sure that our endpoints are protected. I have employees all around the globe, I can't support all routers in everyone's home. No one can. So you have to make sure that your employees are educated on how to configure a router as best as possible to make sure that it's encrypted, to make sure that it's not open and noticed from criminals that are hanging around, and that it's locked down and protected through a key. That's just step one. It's the device, the most vulnerable piece of the puzzle, that's where things get in."

Bergamo says the next part is making sure your network is protected and you have a strong handle on your security posture. She says it is important to ask yourself – does the data center have its own disaster recovery plan? What does that do for your business if they are hacked? Is there enough software in place to make sure that firewalls are protected? If you're a company that's sitting on the cloud, are your applications protected? She believes if you identify anything missing from these types of questions, then you must shore up and close gaps as best as possible.

EDUCATING EMPLOYEES

Bergamo is focused on educating her workforce and community on proper safety. She explains, "From a physical standpoint there are some nations out there that you're not supposed to leave your house. That's not necessarily a cyber issue, but it is a security issue. If you're at home and you have multiple people using the device, maybe your company didn't let you bring a laptop home, maybe you're VPN'ing in or you're using your Wi-Fi. There's many different types of scenarios. How to protect yourself in a connection first and foremost, how to make sure that your device, no matter what you're using, is protected."

> *"Getting attacked is a constant stream, but it's the defending around those attacks that makes us good CISOs, and again, protecting our company and protecting our employees."*

Bergamo says there are many different nuances in this situation along with a variety of risk factors. Since the most vulnerable component of working from home is the laptop, you must ensure you are upgrading and using a password, among other considerations.

She comments, "With many vendors and tools that are out there, as soon as a new signature file is identified, they'll push it down to you. There are environments that don't have those pushes and you have to keep up with them on your own, that means you have to constantly remind people to do so."

INVESTING IN NEW TECHNOLOGY

Bergamo believes before investing in a new technology, you must engage in strategic requirements gathering to ensure it meets key standards. She explains, "What are your security standards? What kind of information are you looking for? It's about understanding what the standards are and how you satisfy those standards to meet the needs. And then from a requirement standpoint, you fulfill those needs and then figure out what's the next step of picking the technology. You must have to have a clear set of criteria involved in order to pick technology."

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

FEATS OF STRENGTH
JUNE 2020

K logix

WWW.KLOGIXSECURITY.COM
888.731.2314