FEATS OF STRENGTH

A Business-Focused Cybersecurity Magazine

THE EVOLVING ROLE OF THE CISO

IN THIS ISSUE:

MARCH 2024

K logix

TABLE OF CONTENTS

CISO Evolution *March 2024*

FROM THE *Editor*

Dear Readers,

The theme of this issue is the evolving role of the CISO – an interesting topic that we were excited to put together. We started this magazine in 2015, almost 10 years ago when CISOs were in quite a different position than they are today. Not all, but certainly the majority weren't presenting to boards, and many felt they did not have a seat at the executive table. They had limited budget (which has consistently ebbed and flowed over the years), but they also had limited mindshare and communication across the business.

Reflecting back on how the interview answers from CISOs have evolved, it's clear that today, more CISOs are considered business-aligned executives. More are having productive boardroom conversations, and many feel they are heard and understood. Communication has improved and security is often closer to the forefront of business discussions.

The world of cybersecurity is not perfect, there are still budget, resource, and hiring challenges. And not all organizations value the importance of security. However, we can't say things have not improved, and we can't ignore the fact that cybersecurity has earned its place within the business.

This issue brings together three CISOs across healthcare, insurance, and edtech. Each with their own approach to running a successful security program, and with that their own set of challenges.

We also include a Q&A with Kevin West, CEO, K logix, who shares his thoughts on where the CISO role is today. Kevin brings a unique experience, having owned a cybersecurity business for over twenty years. He provides insight based on his personal experience working with customers.

Another article in this issue is key highlight areas regarding the evolution of CISOs – how far they've come and where they are focusing their time. It covers new priorities like privacy and risk, and talks through the role of innovative areas such as AI.

I hope you enjoy reading!

Feats of Strength Editor
VP, Marketing, K logix

Magazine Contributors

Katie Haug - Editor
VP Marketing, K logix

Kevin West - Editor
CEO, K logix

Emily Graumann - Graphics
Graphic Designer, K logix

About K logix

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.

PROFILES IN *Confidence*

TINA MITCHELL

CISO
COVERED CALIFORNIA

HEADQUARTERS: Sacramento, CA

EMPLOYEES: 1,400

REVENUE: Federally Funded

Tina Mitchell is the current CISO at Covered California, the state's health insurance marketplace that provides free services to connect Californians with brand-name health insurance, and financial assistance to help pay for it under the Patient Protection and Affordable Care Act. The organization's goal is to ensure residents can get access to quality, affordable health insurance.

Tina was excited to join the organization and help support this valuable mission. Now one year into her role, she has learned a lot about how the organization operates, and how she can best mature and grow the security program.

Prior to joining Covered California, Tina spent twenty-nine years working at American Specialty Health, an organization offering technology-enabled services for benefits management. Tina started with the organization as a systems administrator, worked her way up to Vice President of IT Operations, and spent the last few years of her tenure as SVP of Enterprise Security/Information Security Officer.

Today, Tina leads the security team at Covered California with a core focus on maintaining strong security controls. She organizes her team into two areas – an information security engineering team focused on technical security, and an information security compliance team focused on internal audit, identity, and compliance.

FOCUSING ON AI AND BEING PREPARED FOR THREATS

As a healthcare technology organization, Tina says AI is an important topic for Covered California. She explains, "AI is a hot topic, and the technology behind it is consistently evolving. Like many healthcare organizations we are actively looking at ways to leverage AI to improve our processes and how we serve our consumers, and our security team must stay ahead of the conversation."

Another area of focus is around emerging threats and staying ahead of bad actors. Tina states that threat actors are always using new tactics and techniques, and that a strong security program should both respond to known threats and defend against the unknown. To her, always being a step ahead and prepared is of the utmost importance.

To maintain a state of preparedness, Tina says it is important for her team to keep up-to-date with the latest trends and developments in security. She comments, "We start our morning by reading the security news feeds. We are fortunate nowadays to have such great resources at our fingertips. The intelligence distributed by research firms and government agencies like CISA and the FBI are invaluable. Their advisories, reports, and bulletins are crucial for security professionals tasked with protecting networks and sensitive information from evolving cyber threats."

INVESTING IN THE RIGHT TOOLS

To make sure Tina spends her budget wisely when investing in security technology, she looks at it from a holistic and strategic perspective. She explains, "I am a big proponent of not chasing the shiny new object and losing sight of what we're trying to achieve. My approach is to explore what we already own. We look at our existing contracts and see what we have already invested in, and how we can better optimize and potentially use additional functionality. Less is more. More tools mean more maintenance and possibly more complexity to the environment. It is all about trying to keep the inventory of technologies to as few, yet as effective as possible."

She also believes in reporting to senior leadership on the tools we have invested in and says, "I'm a believer being transparent and reporting on the status of security investments. Are the tools meeting the objective, have

“I would say that I’m a transformational leader and I’m here to inspire, motivate, and influence as we work to achieve objectives. But at the same time, I’m also a servant leader - I strive to understand what each individual needs from me to be successful.”

they helped us improve our security posture as expected? CISOs, like other business leaders, need to hold ourselves accountable for how we allocate our budgets.”

Although reporting on technology is imperative, Tina believes reporting on how security is helping progress the organization’s enterprise strategic goals is even more important. Senior executives have a vested interest in the security program, and by reporting on progress against the organization’s strategic plan, she can demonstrate the positive impact of security, and the initiatives being aligned with the business goals.

LEADERSHIP

Tina considers herself both a transformational and servant leader. She explains, “I would say that I’m a transformational leader and I’m here to inspire, motivate, and influence as we work to achieve objectives. But at the same time, I’m also a servant leader - I strive to understand what each individual needs from me to be successful.”

Tina is a lifelong learner and continues to grow as a leader. She obtained her Master of Science in Executive Leadership and continues to draw from the coursework to hone her leadership skills. She is also an avid reader on leadership.

When she needs help to overcome specific challenges, she connects with her security peers to understand their experiences. Seeking guidance from peers about their own experiences, use cases and understanding why they implemented specific technologies to solve problems has been helpful. Networking with local CISO groups allows Tina to meet with peers facing similar challenges and grow her community.

Q&A WITH KEVIN WEST

CEO, K LOGIX

We asked Kevin his thoughts on how CISOs have evovled across their responsibilties, communication, interactions with boards and more.

Q: Over last 5 years, CISOs are asking K logix for trends around how they compare to their peers in terms of reporting structure, why is this important?

A: That's a great question, because I've thought a lot about why we are getting asked that. What we do know is that less CISOs are reporting into CIOs than ever before, more are reporting into CEOs and other areas of business outside of IT. We poll CISOs on a yearly basis, and recently we found that 33% report into CIOs (down from 62% in 2017), 27% report into Chief Risk Officers, 11% into Chief Technology Officers, 11% into CEOs, and the rest a mix of Chief Financial Officers and General Counsels, among other C-level titles.

So, why are CISOs asking us about this? Why do they care about reporting structures? Since the most significant change we've seen in recent years is the decrease of CISOs reporting into CIOs, I believe they care about getting out from under IT. That gives them a more direct line into the business, so they are able to communicate on their program's behalf.

I'm curious if this trend will continue and what the long term benefits will be, and look forward to continuing to watch how it unfolds in the coming years.

Q: What additional responsibilities have CISOs taken on in recent years?

A: My thoughts on this come directly from real world experience with the CISOs I communicate with among our customer base. These CISOs are taking on more risk-related duties, working through areas like GRC, third party, and transformation requirements. I imagine this is similar to CISOs across most industries, as they are persistently working to ensure the security program is keeping pace with the direction the business wants to go. Not only are they working to continually align, but they talk about ensuring strong communication is in place so security is included in projects from the beginning, as many would say the "shift left" mentality that security is baked in from the start and not an afterthought.

When I speak with CISOs, I wonder how they continue to evolve in these circumstances. Being pulled in many directions while still maintaining a low risk profile and high maturity may be challenging.

Q: How are CISOs juggling everything?

Many of our customers are dealing with budget restraints, while at the same time having more responsibilities added to their plates. Often times, they might not have budget to add headcount, so they have to think strategically about investing in either tools that have potential to help them streamline across responsibilities, or platforms to consolidate individual investments, alleviating pressure on headcount. Alternatively, they are using outside help, like a third party to come in and partner with them to ease the burden on their teams' time.

I am curious about the long-term impact of this rinse and repeat cycle, and will continue to speak with our CISO community about this topic.

Q: How have CISOs relationships with their boards and executives changed?

A: In my experience over the last 20 plus years working with security teams, I've seen a lot of growth between CISOs and boards. Today, many CISOs have seats at the table and are actively presenting to board, in contrast to 5-10 years ago when they might not have had an opportunity to speak in front of them. I'm not saying it is a perfect relationship, some CISOs get 10-15 minutes twice a year to present, while others get significantly more time. It really varies, and in many of the CISO interviews we conduct for this magazine, we hear the same thing – there is no standard, and still a wide variety of board interactions.

The people sitting on boards seem to be more knowledgeable about cybersecurity. I've heard from CISOs that their board members might sit on multiple boards and can come into meetings with context of how other companies are running cyber strategies. Many CISOs talk about there being a greater awareness around cyber, something they find to be a big benefit, because they are doing less educating and able to engage in more thoughtful conversations.

Many of the CISOs we've interviewed say that no matter what, the most important thing to do in boardroom presentations is to simplify and cut down what they plan to present and make sure it hits home with a business person. Then go back and simplify again! CISOs make a more meaningful impact during meetings and might be better positioned to gain more budget or resources. At the very least, gain more mindshare and get their priorities across in a more streamlined way.

Q: What types of questions are board members asking CISOs?

I'm not an expert on boardroom discussions, but I do learn from our customers and those we interview for this magazine about their interactions. In these conversations, I've learned that boards have elevated their level of questioning. While CISOs still receive questions like "will the cyber incident I saw on the news happen to us", they are also being asked more poignant questions specific to their organization and its goals. They are hearing things similar to - "what is the business impact of your current priorities", they are curious about things like revenue impact, privacy regulations, risk tolerance, and long-term goals for maturity.

BOB STASIO

CISO/CIO
RENAISSANCE

HEADQUARTERS: Wisconsin Rapids, WI

EMPLOYEES: 1,200+

REVENUE: Private Company

PROFILES IN *Confidence*

Bob Stasio began his career in the U.S. Army as an Intelligence Officer, then spent ten years working in the government sector, holding positions at NSA's Cyber Center, U.S. Cyber Command, and the U.S. Army's Signals Intelligence Corps. After moving into the private sector, Bob held positions at large organizations such as IBM, where he utilized his experience in cyber operations and threat hunting. He also held positions leading threat intelligence programs at organizations like Bloomberg and global financial firms. His most recent positions include Deputy CISO at DuPont where oversaw the security team while building the security operations and SOC programs, before joining Renaissance as their CISO/CIO.

Bob joined Renaissance, a global educational technology SaaS organization, over two years ago as their first CISO with the prerogative to holistically build a strong cybersecurity program. This was an opportunity for him to leverage his deep leadership expertise paired with his strong background building cyber programs. He comments, "I moved over to Renaissance because it looked like a great experience for me, leadership was switched on to the benefits of security, I was able to work in the education industry and it was clear security had support from the board. Overall, it felt like a very supportive relationship."

Bob experienced success from an early start at Renaissance, and he credits that to his broad background and proactive approach to communication. When joining a new organization, Bob recommends that CISOs ensure they understand the full scope of the budget available to them, the goals of the leadership and if they align with the security program, and areas of compliance they need to follow. He continues, "It is important to know if customers require a higher level of security and how you are going to be tied to the business. You need to know that you won't just be a cost center, that you will actually be contributing to revenue and a vital part of the business. In the end, CISOs need to also show value."

RUNNING A SECURITY PROGRAM

As the first CISO at Renaissance, Bob was tasked with building a security program and laying the groundwork for cyber maturity and protection. His first step was prioritizing critical areas such as stopping immediate threats that could be harmful to the business. Given his strong background in intelligence, he ensured the detection and response program was clearly outlined, and up and running. He also planned out milestones like achieving a SOC2 audit. It was important to Bob that security fundamentals were laid out, so they had a distinct plan and roadmap to follow that closely aligned with what the business was trying to accomplish.

It was also important to Bob that he selected a cybersecurity framework to follow that would help guide the program to maturity and provide milestones to achieve along the way. He comments, "We use the CIS top 18 framework to self-evaluate our current maturity and determine any areas we need to focus on. It helps with tracking progress. Also, when deciding on investing in a new tool, its helpful for us to leverage the framework so we can decide how to filter through the options."

CUSTOMER FACING CISOS

Today, many CISOs have begun interfacing with customers,

"I moved over to Renaissance because it looked like a great experience for me, leadership was switched on to the benefits of security, I was able to work in the education industry and it was clear security had support from the board."

sharing the value of their organization's security program, and becoming true advocates in demonstrating how security is a competitive advantage. Bob fits into this category of CISOs and explains, "We have some bigger deals that might require my presence. I come in and talk strategically with a customer to answer any questions they might have around things like our security architecture. CISOs should be able to demonstrate how they are better than the competition, so customers can clearly understand why they should work with them. It all comes down to how serious your organization takes security and being able to talk to business leaders about this."

Not only is Bob an advocate for security with customers, but he is the liaison between the business and security. He has a regular set of meetings with the executive leadership team where he presents and talks to them about his roadmap and any progress updates. He also shares details around maturity in relation to competition, something many executives are very interested to hear about. One tactic to ensure he communicates in a succinct and business focused manner is to use anecdotes when describing updates. For example, he might share a story about security's role in helping sign on a new customer faster or get through a vetting process sooner.

Overall, Bob approaches his role with the intention to educate and advocate for the security program. He recognizes the need for CISOs to focus on business language when speaking to anyone outside of security, in order to gain mindshare.

LEADERSHIP STYLE

Bob's military background helped him gain strong communication and leadership skills that he has continued to use throughout his career. He approaches leading his team with an open mind and always focuses on being a team player. He says, "Your mindset always has to go from being a janitor to a general in the organization. You're not above any particular task and you should be able to jump in and help at any point when needed. You could be the janitor one day and the general the next day. That's' the general philosophy I've adhered to for my career."

He continues, "In the military, when you get in the trenches you gain an understanding of what those guys are doing, and they appreciate that you have an interest in what they do. You may not be good at it, but at least you're showing interest and you're not above anything. This gives you a lot of credibility and helps you understand what they do. It's always been a core tenet of my philosophy."

To continue to grow as a leader, Bob ensures he is always learning from a variety of sources. He enjoys taking different courses or certifications to gain valuable expertise in specific areas that will bolster his skillset. He also attends conferences that focus on leadership for CISOs and CIOs. Learning from others is important in order to develop skills, and the tight knit security community is a great resource to leverage. Overall, he is a constant learner who connects with the cyber community in order to deepen his network as well as give back.

"CISOs should be able to demonstrate how they are better than the competition, so customers can clearly understand why they should work with them. It all comes down to how serious your organization takes security and being able to talk to business leaders about this."

CHALLENGES

"One of the top challenges is the rapid growth of new technology that's coming out, like AI. Everyone is including AI in their software and their products, and we have to properly vet it out, which might slow down the process of bringing any new technology in. We have engineers on the other side of the business that want to move fast while doing things well. And sometimes those two things can conflict against each other. So, working with the business at the speed they want to go, while being safe and secure at the same time is definitely one of our bigger challenges," explains Bob.

PROFILES IN *Confidence*

WILLIAM LIDSTER

CISO
AAA WASHINGTON

HEADQUARTERS: Bellevue, Washington

EMPLOYEES: 500+

REVENUE: $250 Million

William Lidster attended the United States Military Academy at West Point, and joined the armed forces after graduation. After his tenure in the military, he moved into a technology sales role, selling computer and networking equipment across Europe and the Middle East to government organizations like the DoD, Department of State, and United Nations. He acquired some networking skills during that experience and decided to move into more leadership-focused roles, taking him back to his home state of Alaska. William's first exposure to administering informatoin security needs came with an IT leadership role with a local electric utility company. It was during this time he recognized how interested he was in the information security side of the business, and his career took off from there. After a successful career building security programs across banking and healthcare organizations, William began working as the first CISO at AAA Washington.

What attracted him to AAA Washington was the culture and importance placed on the success of the security program. He explains, "I've been here almost seven years now. We have a great culture, great people, and I'm afforded lots of latitude. They take security seriously and it has been wonderful to develop and grow the program here."

BEING A STRONG COMMUNICATOR

In order to set himself and the security program up for success, William spent the first few months at AAA Washington connecting with business leaders, understanding their pain points, and determining how security could make a positive impact. He comments, "One of the very first things I was trying to do is get a lot of easy wins. I wanted to get to a place where security was viewed as helpful. And that we can help them quickly and efficiently, and not be a roadblock to anything other business units are trying to do. Achieving this was probably one of the best things I was able to do."

Being a strong communicator derives from William's formal training at West Point. As an officer, he was constantly communicating with senior-ranking officers, something that matured his ability to think and talk strategically. He realized most leaders want to know the what, not the how, and when you can confidently discuss this with them, you instantly gain their trust.

RESPONSIBILITIES AND FOCUS AREAS

"I'm responsible for everything that is information security. When we think about information security, we also think about physical controls, not just technical or administrative, and that's a working partnership we have internally. We have a lot of initiatives and a lot of transformation taking place in different areas, and my responsibility is that we're doing it within our risk appetite and risk tolerance. I have to make sure we are putting the right things in place to ensure our systems and data remain secure. I have overarching responsibility with governance, and making sure things are being done correctly, even if it's not in my particular department, because we do distribute things people have to be able to do, not just my team," explains William.

One of their current larger initiatives is around cloud migration, moving systems off prem and transforming their capabilities moving into the cloud. For the next twelve

"I've been here almost seven years now. We have a great culture, great people, and I'm afforded lots of latitude. They take security seriously and it has been wonderful to develop and grow the program here."

months, William is upping the security posture in response to the new perimeter. He says, "The perimeter is really going away. I'm doing basically a lift and shift, and that puts our endpoint into a different category of criticality that we didn't have to worry about before. So that's what I'm working on right now. We're replacing our EDR with something that's far more powerful, far more comprehensive. We're implementing a SASE as soon as we're done with EDR, to provide security before we go to our cloud resources. When I found out these business transformations were coming, I knew that we needed to lift and shift our controls in a different way."

FRAMEWORKS FOCUS

William and his team follow the NIST CSF framework, an approachable way to ensure they are meeting standard security requirements. His goal is to continue to mature how they align to the framework, and ensure they focus on key areas that are most applicable and impactful to their business and how it operates. For example, they might look at the CSF and map it to their GRC tool to ensure efficiency.

To effectively communicate with executives about progress on framework alignment, among other areas, William ensures he uses clear business language. He comments, "I go into executive meetings with the intention to get across, at a high level, what we are doing and why. I use my judgement to determine what milestones to share with them, and my goal is to make sure they have a good grasp on what we are doing. I don't go into details like percentage of NIST controls complete, it is not necessary for them to know this level of detail as long as they understand what we are trying to accomplish and why. They really want to know how our work relates to the business. The board and executives should walk away from the meeting with an understanding that we are doing the right things and headed in the right direction. We get asked smart questions by them, and it shows we are on the right track."

LEADERSHIP

Having a common vision and ensuring his team understands the value of their mission is important to William, and it is how he approaches leading towards a positive impact. He explains, "My team is engaged, they understand that they've got a mission and purpose, and they're behind it. And that they're free to grow and be engaged in our program. It is great that they stop and question what we are doing as well. We might be headed in a certain direction, and they have free will to question if it is the right decision or suggest alternatives. Everyone speaks up and shares their thoughts on what we are doing. I am always open to reassessing the direction we are going based on feedback from my team."

He continues, "I really value making sure that everybody's on board and knows what's going on. I formulated a Risk Governance Committee, that didn't exist before, so I can bring the business in formally every quarter, and say this is what we're doing, this is why, and this is what's next. We ask questions to make sure they understand what we are doing, and ensure we have buy-in from them. Approaching it this way is part of my leadership style."

"I go into executive meetings with the intention to get across, at a high level, what we are doing and why. I use my judgement to determine what milestones to share with them, and my goal is to make sure they have a good grasp on what we are doing."

To continue to grow his skillset and hone his leadership skills, William strongly believes in networking, whether it is at conferences or amongst his personal relationships with peers. He values learning from others in his position about their approach to communicating with executives, and how they effectively align to the business. He also discusses how his peers approach investing in solutions – better understanding their requirements and outcomes. Another way William gives back and continues to learn is by regularly teaching cybersecurity courses at universities. It provides him opportunities to stay current on trends and encourage the next generation of security professionals to be passionate about a career in the industry.

The Evolving Role of the CISO

By Emily Graumann, Marketing, K logix

The Chief Information Security Officer, or CISO, is the senior-level executive responsible for the protection of an organization's information and data security. This role has seen exceptional growth in the scope and scale of its duties since its inception in the late 1990s. Once narrowly defined as the head of IT security, the CISO role has grown into a business leader, engaging with executives, and demonstrating a positive impact on organizations.

Security programs under today's CISOs include, but are certainly not limited to: risk management, security operations, identity and access management, privacy, governance, business enablement, legal, and architecture. That is to say, the importance of this role cannot be overlooked or overstated. Attacks are only getting more sophisticated, and the global annual cost of cybercrime is expected to reach US $9.5 trillion in 2024, according to Esentire's 2023 Official Cybercrime Report. Additionally, CISOs are taking initiative to ensure cybersecurity is baked into wider business operations, and this requires a deep understanding of an organization's business objectives.

REPORTING STRUCTURE AND EXECUTIVE IMPACT

As the CISO role has grown, their position, authority, and impact within an organization has significantly evolved. Most CISOs have removed the stigma of being a cost center by demonstrating how their programs are driving innovation, protecting valuable company assets, and influencing business transformation.

It is becoming increasingly common for CISOs to interact more frequently with the CEO, CFO, and other C-suite executives, and there is also movement of CISOs reporting directly to CEOs. CISOs also communicate and present to the Board of Directors on a regular basis. Participation in the business side of the organization grows the influence of the CISO in ways this position has never seen before, and this gives this role a platform to ensure security posture is given the attention it requires.

MANAGING VULNERABILITIES DUE TO REMOTE WORK

Following the COVID-19 pandemic, remote work is a trend that is here to stay for many organizations. According to Forbes, 12.7% of full-time employees currently work from home, and this percentage will grow to 22% by 2025. CISOs are now responsible for assets and employees spread across the country or across the globe, and this also includes duties such as acquiring and deploying laptops, upgrading VPN infrastructure, being proactive against exploitative cybercriminals who want to exploit this trend, and introducing new security measures to keep employees safe while working remotely.

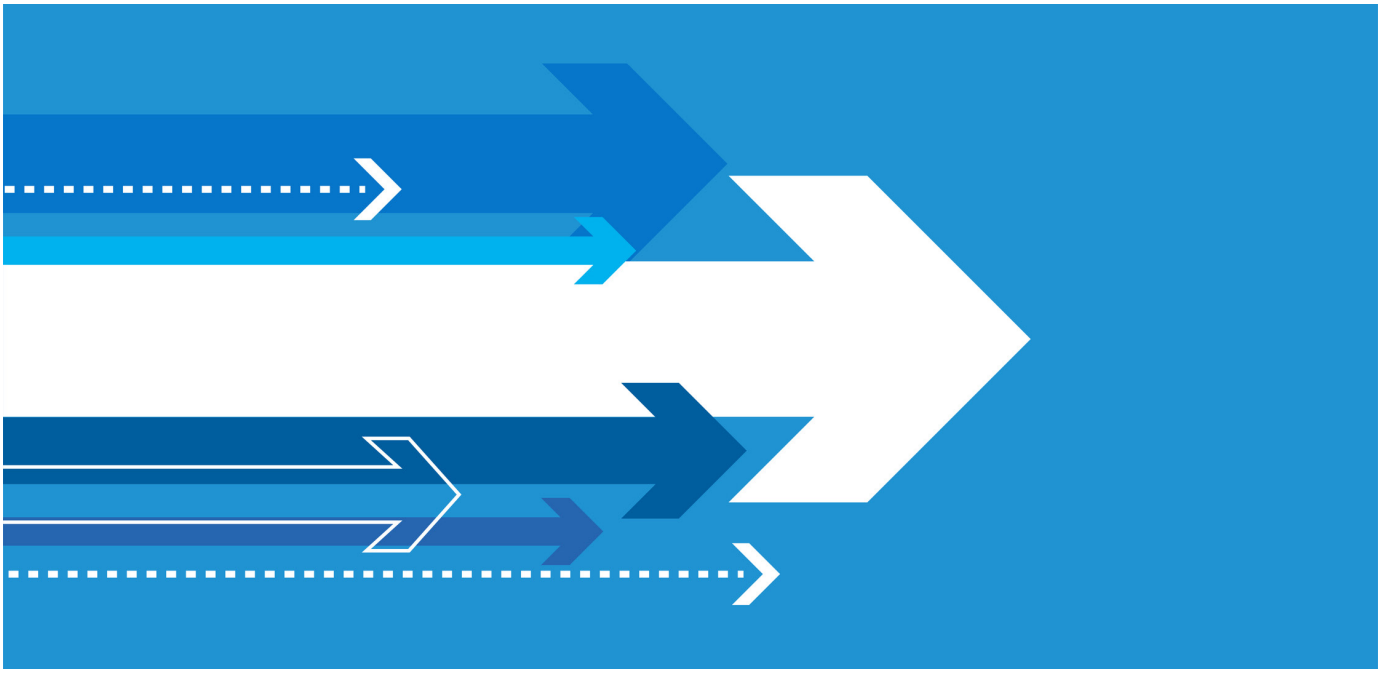
This trend places more responsibilities on the shoulders of CISOs and drives more interaction across all business departments. In order to efficiently and effectively implement necessary changes, CISOs must create strong lines of communication with executives to provide updates on progress and establish that all parties understand the importance of new measures taken.

THE RISE OF AI

To be a CISO is to be mindful of rapidly changing technologies within the industry and beyond. This includes AI, or artificial intelligence, and the extensive number of risks and benefits that come with it. The risks come at the hands of bad actors who use this technology to bolster their cyber attacks. Social engineering attacks like phishing scams have become harder to spot, because AI remedies grammatical mistakes or awkward phrasing that used to be a major identifying factor for these malicious messages, and the impact of these attacks is palpable. Direct financial loss from successful phishing attacks increased by 76% in 2022 according to Proofpoint's 2023 State of the Phish Report. And that is only one example of the way AI can be exploited, among many.

In order to level the playing field, there are advantages of AI that CISOs are harnessing. This technology is unparalleled in its ability to flag suspicious activity and detect attacks accurately. According to Splunk's CISO Report, 35% of CISOs report using AI, either extensively or somewhat, for positive cybersecurity functions, another 61% express that they either have plans to use it in the next 12 months, or are interested in doing so.

Not only does AI impact attacks, but across the business, leaders are looking into ways to leverage AI, which may pose increased risk for the organization. CISOs are tasked with reporting and communicating with each department to understand their



departmental goals, to provide a clear plan of where they are looking to invest in technological advancements around AI, and most importantly, to determine where security plays in role in reducing risk without slowing down these efforts. This means CISOs must look to AI internally without their own programs, but also communicate externally across the business.

PRIVACY

Regulations such as GDPR and CCPA have made significant impacts on how CISOs operate their security programs, bringing to light the need for strong communication with their privacy and legal counterparts.

Not only are country and state regulations changing, but in light of the rising prevalence of AI, CISOs can anticipate a wave of new regulations, especially concerning data privacy protection.

In order to combat evolving privacy risks and the concerns of vendors, partners, and consumers, CISOs must be proactive in reaching solutions that prioritize data privacy, restore consumer confidence, and guarantee compliance with regulations. These responsibilities include being able to respond clearly and reassuringly to requests and inquiries about data transparency and being able to focus efforts on monitoring regulatory landscapes.

And as CISOs face growing responsibility and regulatory load, many organizations are adding a new role—Chief Privacy Officer—to their C-Suites. Non-compliance with regulatory measures carries substantial legal risks, particularly around personal data notices and uses. A CPO is responsible for working alongside the CISO to verify and maintain compliance with complex policies, privacy laws, and regulations. With a CISO's already expansive list of duties, special attention to these areas by a CPO is hugely beneficial to avoid noncompliance with these evolving regulatory measures.

THE FUTURE OF THE CISO

The CISO role has seen significant changes in its responsibilities, and all data indicates that this position will continue to gain authority and influence. The future of this position is deeply entwined with technological shifts, trends, regulations, and advances, and because of this, proactivity is key. CISOs must be able to adapt to these changes, communicate their cause, and even embrace these emerging trends where they can. The future of the CISO is extremely dynamic, just as dynamic as the cybersecurity landscape, but so long as these priorities are actualized, CISOs have the best chance to effectively safeguard their organizations and keep their assets secure.

Sources:

Splunk, "The CISO Report"

Cisco, "What is a CISO?"

Esentire, "2023 Official Cybercrime Report"

Tripwire, "The Changing Role of the CISO"

Information Age, "The Changing Role of the CISO"

Forbes, "Remote Work Statistics And Trends In 2024"

Proofpoint, "2023 State of the Phish Report"

CSO Online, "How the CISO Role is Evolving"

KBI Media, "The Future of CISOs: Navigating Trends and Evolving Roles"

Cyber Defense Magazine, "3 New Risks that CISOs will Face in 2024"

Avertium, "Why Enterprises are adding Chief Privacy Officer to C-Level Leadership"

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM