FEATS OF STRENGTH

A Business-Focused Cybersecurity Magazine

IN THIS ISSUE:

DECEMBER 2024

K logix

Data Governance

Reducing Data Complexity by Partnering Across the Business

TABLE OF CONTENTS

December 2024

FROM THE *Editor*

Dear Readers,

The theme of this issue is data governance - a seemingly complex topic that has emerged as a key focus area for CISOs for years, with the added necessity of cross departmental collaboration to ensure it is holistically addressed. We dug deeper into this topic through the five interviews we conducted, with each security leader sharing their approach, thoughts, and other bits of relevant information.

In the interviews, we highlight leaders who are making an impact not only in their organizations, but across the industry. They exemplify passionate security leaders, focused on leading strong teams, and ensuring they continue to improve maturity and reduce risk.

With the year coming to an end, we want to thank our readers for their input and viewership over the past 365 days. Wishing everyone a successful end to 2024 and strong start to 2025!

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
Marketing and Design Specialist, 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*

DONNA ROSS

CISO
RADIAN GROUP, INC.

HEADQUARTERS: Bellevue, Washington

EMPLOYEES: 500+

REVENUE: $250 Million

As early as Donna Ross can remember, she was interested in taking things apart and fixing them, and this curious mindset has helped in her extensive and successful career in cybersecurity.

Her career in security happened somewhat by chance, when she was volunteering at a food bank and met someone who worked in security, and who eventually became her mentor. Through this mentor relationship, Donna was offered her first security job. She explains, "I was in marketing, I had a degree in economics. But I met someone who worked in security and I asked him if he would be my mentor. He agreed. And we started working together and maybe three months into that mentorship, he invited me to join his team, and I said to him, 'I know nothing about security, but I'm eager to learn.' Subsequently I've gone back to school and achieved some key security certifications."

She continues, "My life lesson and my foray into security was: first asking for help, but secondly, when someone in a leadership role sees something in you, you may not see it in yourself. So take that job, take that role, and be the best you can be, because I think a lot of times women career-limit themselves when they see a job description. I know there have been studies on this, we tend to look at it as a checklist. I can do this. I can do that. I could do this. I can't do this, so I won't apply. Where men will look at that same job description and are happy if they meet 60% of the skills and they'll go ahead and apply for that job. I guess in my case, I realized my mentor believed in me. I liked him. I knew I could learn from him, so I quickly realized I should take the job. And that's how I got into security - I didn't choose it, it chose me."

Her background in marketing, economics, and a business school degree helped Donna make an easy transition from technically focused roles into more leadership driven roles. Currently the CISO at Radian Group Inc., a mortgage insurance and real estate services company, Donna is responsible for the overall information security program, protecting the data that is entrusted to them by customers, partners, employees, and counterparties. Her team is broken into three distinct groups, as she explains, "I have an information security technology team and a leader that runs that reporting to me. We also have an information security operations team, focused on operational tasks and incident response. And then I have an information security governance risk and compliance team that really is focused on assurance, compliance, awareness and training, and all those non-technical components."

WHAT CISOS ARE FOCUSING ON

Donna says cyber leaders should be focused on four things looking forward. One is reducing the attack surface and considering a zero-trust model where you trust no one by default and are continuously verifying access. Another area is focusing on ransomware readiness and cyber resiliency, including incident response readiness, backup and recovery strategies, and employee training. The third area is cloud security, specifically because regardless of what kind of cloud, it's a shared responsibility model. It is important for CISOs to better understand what their responsibilities are and what the service provider's responsibilities are in those cloud instances. Lastly, supply chain security is key, with a focus on having a rigorous vendor risk management program and process looking at single points of failure and continuous monitoring. There have been a barrage of data

"My life lesson and my foray into security was: first asking for help, but secondly, when someone in a leadership role sees something in you, you may not see it in yourself. So take that job, take that role, and be the best you can be, because I think a lot of times women career-limit themselves when they see a job description."

breaches within supply chains that could impact anybody that uses that product or service, so it is really important to ensure you are prepared and proactive in your approach.

By focusing on these four areas, Donna believes CISOs and security leaders alike can help advance their programs in a mature and risk reducing manner.

EFFECTIVE COMMUNICATION WITH EXECUTIVES

Donna believes in transparent and honest conversations. She comments, "I am highly transparent whether I'm reporting to any of our internal committees or whether I'm reporting to the Executive committee or even the Board of Directors. The key is being honest, being transparent, and talking in terms of risk. What I talk about is not necessarily information security, it is all about how we are managing risk, and then to keep it simple I avoid talking to them in technical terms. I try not to talk in zeros and ones, I try to make it more of a conversation. Anytime you're in a technical area, you know you do a much better job when you can speak in business language. It is important to speak in terms of dollars and risk to the business."

Throughout her career, Donna has had the privilege of briefing the board, whether it was annually, quarterly, or monthly. She says the best approach is always to do your homework – research current events or things they may have read in the Wall Street Journal, and to know who the members are. She shares, "I need to know other boards they are on, so I'll do some research leading up to the board meeting. Have any of their organizations been in the paper? Has there been an event, have any regulations changed that align with their area of expertise? I spend a lot of time in the months, weeks, and days leading up to the board meeting, doing my homework to avoid surprises. My first advice is to know your board, know what they do, know what they care about, and know what's going on in the news. And the other thing is if they ask me something and I don't know, it's okay to say I'll get back to you. I'm very honest and open with them."

PROACTIVELY APPROACHING CHALLENGES

For the cybersecurity industry as a whole, Donna believes outside of budget and people, that CISOs should focus on external factors that could impact their program such as the threat landscape or geopolitical factors. She says to think about what is going to happen with the US election, what are the different scenarios should one candidate win versus the other? Donna also shares that it is important to consider evolving areas like Artificial Intelligence and how it might be used by bad actors. The compliance landscape is another challenge – to better understand how it is changing and how to be one step ahead of these changes.

THE VALUE OF MENTORSHIP

Donna considers herself a visionary leader, someone who prioritizes not just her needs, but those of the company and her team to ensure their development and well-being is considered. She learned a lot from her early mentor and strongly believes in finding a mentor to help guide you in your career journey. She

"I am highly transparent whether I'm reporting to any of our internal committees or whether I'm reporting to the Executive committee or even the Board of Directors. The key is being honest, being transparent, and talking in terms of risk."

comments, "Find that mentor, that coach, that advocate, and make sure you can articulate a really clear vision. Through mentorship you are able to create a commitment aligned around shared goals and shared growth that encourages innovation and forward thinking. I've mentored many people over the years and my goal is to help guide them in achieving the goals they have set for themselves."

She always looks at how she can motivate and influence her team to drive better results and create an even stronger culture. To continue to grow as an individual, Donna seeks feedback, is constantly learning, participates in networking, and engages in self-reflection and self-assessment.

Donna belongs to a number of professional groups including CISO and analyst communities. She also has an extensive group of CISO peers she can call up and problem-solve with. She explains, "We don't talk about anything like technology pricing, we talk more broadly about the problems we are facing. We share things like how we solved certain problems, lessons we learned, how we would have done things differently, and other relevant things. Having this amazing Philadelphia CISO network that I'm part of has been rewarding because we are all incredibly interconnected. We have known each other for a long time. Most of us have been around for years, so even if I'm going to a conference, I have a distribution list on my cell phone with everyone's number and I'll just check who's at the conference and ask, "Do you want to meet up later and talk about what we learned?" So, we're very fortunate in this community and in the Philadelphia area where the CISOs and the security folks are very tight knit and we support each other and help each other out."

PROFILES IN *Confidence*

JOHN MANDRACCHIA

CISO
Health Plans Inc.

HEADQUARTERS: Westborough, MA

EMPLOYEES: 500+

REVENUE: $74 Million

John Mandracchia was originally featured in the Feats of Strength magazine in March 2021, where we profiled his career experience, goals, challenges, and focus areas. Since then, he has significantly grown his skillset, evolved his approach to leading an information security team, and ensured he stays up to date with current threats impacting both his organization and the healthcare industry as a whole.

John began his career at Health Plans, Inc. over sixteen years ago, working his way from System Engineer to his current role of CISO, a title he has held for almost six years. Health Plans, Inc. is a national third party administrator of customized, self-funded health plans serving employers and brokers. John brings over twenty years of experience in cybersecurity and infrastructure to continually help the organization accomplish their goals and serve their customers with quality services. John's success stems from his focus on core competencies including strategic cybersecurity planning, implementing risk management policies, and leading cross-departmental process improvements.

RANSOMWARE AND SUPPLY CHAIN SECURITY

When discussing new challenges that have surfaced since we last spoke with John, he shared that ransomware and supply chain security have become incredibly relevant areas of focus. He explains, "There's been a significant uptick of ransomware attacks, especially in the industry of healthcare-related services. It is a consistent threat to environments that carry highly sensitive information and working in any healthcare related fields makes you a prime target. We focus on supply chain and ransomware attack defense because, as the saying goes, you're only as strong as your weakest link. Social engineering attacks have become very sophisticated and it is a lot easier to fool unsuspecting individuals. It only takes one employee from one vendor we supply data to, with an off day, for us to be impacted."

He continues, "I've focused on how we can evaluate the security postures of the vendors around us and how we can work with them. When we do this, we don't expect everyone to have fortune 10 security levels or have military grade defense mechanisms in place, but we are ensuring these vendor organizations are aligned with NIST, have SOC validations, or HITRUST certifications. Positions such as these are really assuring to us as an organization. We like to see that our vendors are putting these types of controls in place, it gives us peace of mind."

Having a comprehensive plan against ransomware and supply chain attacks is paramount for John and his security team. They not only need strong policies in place, but they must continually research and stay one step ahead of current threats or changes as it relates to these areas.

PROACTIVE SECURITY AROUND AI

Artificial Intelligence is a large area of focus for not only John and his team, but for the organization as a whole. He shares, "We are looking at ways that we can use AI to help us without reinventing the wheel. In the short term, AI can act as an assistant to improve efficiencies, and in the long term, it can help us improve functionality across the organization. From a security perspective, it is our role to better

"From a security perspective, it is our role to better understand how AI might be used to damage the organization. Deep fakes and the capabilities of voice cloning are something of great concern."

understand how AI might be used to damage the organization. Deep fakes and the capabilities of voice cloning are something of great concern. It is scary to think about how these realities might be used against us. So, it is important for us to fully understand how AI can be used, and how we can create awareness and education around it so we can defend against it."

It is also important for John to help his organization securely implement their AI objectives and align AI best practices with their priorities. The goal is for security to help streamline proactively and ensure they are educating along the way.

STRONG DATA GOVERNANCE

According to John, the fundamental pillar of a strong data governance program is implementing the correct controls and tools to identify data types. He comments, "Data governance starts with the proper identification of data attributes such as data type and how old the data is. This process allows for lean data retention. There are some great tools that help detect the type of information in certain data, so you can identify where PHI or financial data resides and monitor it according to policies you have set. These policies should outline data retention, data destruction, and usage to ensure the right actions are taking place based on the type of data present."

Automating the identification of data is a key component of this process. Through this automation, the organization can save time and ensure data is properly identified.

John believes AI will expand and continue to significantly impact data governance. He explains, "It simply makes sense that there will be a heavier AI integration process when it comes to governing data. In the past I would spell check an email by hitting F7 prior to hitting send, but now we have AI that's reading our text in real time and telling us how to improve our sentence structure. So, for data governance, if we can invoke AI to assist the user and automatically classify data, then less manual work must be done. I see a lot of growth potential in this area."

GROWING AND LEARNING

Surrounding yourself with great people that want to learn is John's motto when it comes to leading a mature and proactive security program. To consistently build a strong team, he ensures he provides a platform for success tailored to each member's personality. For example, if he has an employee that prefers to speak in depth strategically, he gives them the time and space to do so.

John continues to engage in networking with his security peers on a regular basis. He comments, "Through attending conferences and networking events, I meet people that are in similar situations to me, and it's really reassuring to know they are facing some of the same challenges. To know I'm not the only one dealing with these things is nice, but also helpful to learn from them on how they overcome it. I gain a lot of value in conversations that talk about the frameworks people are following, even from a nuts-and-bolts perspective when talking about granular controls they have implemented."

"Through attending conferences and networking events, I meet people that are in similar situations to me, and it's really reassuring to know they are facing some of the same challenges."

To grow his skillset, not only does John read industry publications and journals as time permits, but he finds a lot of value in listening to cyber podcasts that provide short, tangible information on an almost daily basis. He recommends other CISOs to glean industry information in whatever format works best for their schedules.

AI, Data Security and Data Governance

By Ryan Spelman, Managing Director of Cyber Risk, K logix

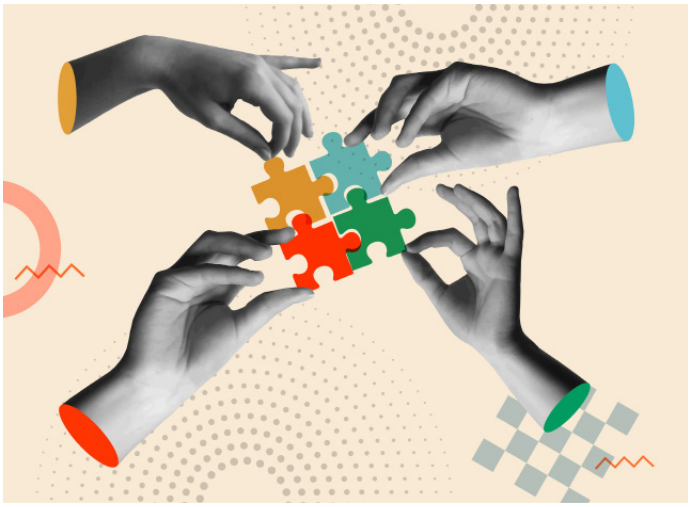
As organizations continue to invest in AI and AI-powered software, "Data Security" is also entering the conversation. Data security, as defined by NIST, is "the process of maintaining the confidentiality, integrity, and availability of an organization's data," which most organizations' cybersecurity programs strive to do. What makes this conversation around AI different than standard cybersecurity-related programs, is that risks and challenges around data security are different because of the nature of AI itself.

AI, for all its current magical capabilities, is still in its early stages. When organizations add AI to their systems, they effectively add a new user with access, but not reason. AI has the ability to consume data but has limited context to understand how to use it and handle it. A poor example, but accurate, is viewing AI the same as an intern. They have a lot of knowledge and enthusiasm but none of the wisdom, discretion, and strategic thinking of more seasoned employees.

How does a data security mindset approach this? At its core, data security is focused on whether the appropriate access controls are in place. Data that can only be accessed by those with appropriate access is "secure." Ensuring that AI, or the intern, can only access the correct data is a good first step.

There is more to this, however, as, unlike an intern, AI is part of a multiple-terabyte software program that doesn't sleep and can be in thousands of accounts and devices at the same time, consuming and processing data. Further, AI currently cannot limit their knowledge so far as if they know something, they know it forever and across all thought streams. The only limitation is their connection with other large language model programs. For example, if you use an enterprise version of Open AI, knowledge shared with it is limited to your instance. However, anyone with access to that instance is able to access that data. Thus, limiting the exposure of AI to only the data it should have access to is required.

> Data governance is the structure that identifies, manages, and ultimately "governs" the data, and is required to implement AI properly.



But how do you truly understand what data to limit access to and why? Security teams cannot revert to being the department of "NO" when it comes to AI, no matter how tempting it may be.

Enter data security's parent: data governance. Data governance is the structure that identifies, manages, and ultimately "governs" the data, and is required to implement AI properly. Data governance helps organizations understand where their data resides, its purpose, and what protections are needed, to name a

few focuses. Data security can then look to the guidance of the data governance to identify who to give access to, how it can be accessed, and what can be done with that access.

Why is this the best path?

We have a similar example to reference in the previous move to the cloud, when network management failed to listen to its parent, IT governance. When the cloud was first introduced,

> Organizations putting AI into their systems without good data governance run the same risk as those that joined the cloud with poor network design.

the “Lift and Shift” model led to dozens of exposed organizations. This strategy was network management acting without considering the finer points of IT governance (and security). Networks that were secure on-prem, behind dedicated firewalls, and limited by physical architecture were no longer secure when put on the cloud with open ports and misconfigurations. These configuration gaps and strategic misalignments would have been avoided if IT governance had been adequately implemented - the same with AI. Organizations putting AI into their systems without good data governance run the same risk as those that joined the cloud with poor network design.

The future of data security is not in choosing the right controls but in choosing the right data governance. Master the data, who owns it, how it should be protected, etc., and you will master your security risks, AI-powered or otherwise.

PROFILES IN *Confidence*

MATT CERNY

DIRECTOR OF CYBER SECURITY
INTEGRA LIFESCIENCES

HEADQUARTERS: Princeton, NJ

EMPLOYEES: 1,200+

REVENUE: Private Company

Matt Cerny began his career in security over 20 years ago, with a vast amount of cybersecurity expertise along with 10 years of experience in infrastructure. As an avid contributor to the industry, Matt participates in a number of security communities that champion peer networking and growth. He currently works as the Director of Cyber Security at Integra LifeSciences, a medical technology organization.

When talking about his first introduction to security, Matt shares, "The reason I got into cyber security was that the company I was applying at was looking for someone who could perform security for Windows, Linux and AS 400. They were looking for somebody with a skillset that wasn't just isolated into one particular platform, but who had knowledge of multiple platforms to be able perform the integration between those three entities. So, I took the knowledge I had gained through my career to look at those three different operating systems, understand the integration and apply security foundations to them. That is how I came into security, and back then security was not as big of an area of focus, it was a lot of access control and identity work that ultimately morphed into the broader scope of what security is today. I've been able to see the growth that has taken place over the last 20 years."

Working at Integra LifeSciences has been incredibly rewarding for Matt, because he has an opportunity to not only fine tune and flex his skills every day, but the work he does impacts the company's overall goal of improving lives. Integra's vision is to expand access to promising technology that enables the body to regenerate damaged or diseased tissue. Grounded on this vision, the company revolutionized the field of regenerative medicine and has since grown to be a leading global provider of neurosurgical solutions, regenerative technologies, and surgical instrumentation (www.Integralife.com).

In his role as Director of Cyber Security, Matt's responsibilities span globally as they have offices and manufacturing facilities around the world. His team is responsible for security operations as it relates to cyber risk reduction and cyber risk management, and also includes identity and access management and operational technology cyber security. Matt comments, "The way I perceive cybersecurity is by relating it to a submarine. If a submarine were hit by a missile, in a figurative manner, we, the security team, would be able to shut down that particular hole that was hit and the ship would still function while we made the necessary repairs. You're protecting certain areas of the submarine, in order to cordon an impacted part of the ship, but to also make sure you are still able to operate and continue on."

FOCUS ON AUTOMATION AND THREATS

Looking towards the next year, Matt is focused on several core areas to improve the overall security program and continue to reduce risk. Automation is top of mind, and their goal is to establish a methodology to reinforce or test one control that could ultimately comply to multiple regulations. For example, if testing multifactor authentication, they would be able to look at how many frameworks or regulations would that adhere to, so they can holistically apply it to the relevant areas across frameworks. The outputs might show that they are 80% in compliance with one framework, and only 60% compliant with another. The concept of a unified

"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."

compliance framework is a top priority, something that will help his team save valuable time and resources. To accomplish they are engaged with outside help to implement changes and integrate this methodology to match the needs of their security program.

Managing and understanding threats is another focus area for the Matt, specifically as it relates to the human element of security. He says, "Threat actors have evolved, take for example push notification fatigue, where one individual keeps receiving push notifications for multifactor authentication and ends up saying yes just to make them stop. It is security's job to ensure people across the organization understand that security is consistently evolving and just because we deployed one particular technology, that the problem may not always be completely fixed. SMS texting for multifactor authentication was common, but it is becoming less secure and the recommendation is to remove it. Now you might need to ask people to re-enroll in a new version of multifactor authentication and they might not understand why. It is our duty to ensure people understand that threat actors are changing, and our controls have to evolve alongside them to make sure we are protected. I think when it really comes down to it, people still play a very important factor in the adoption of cyber security as well as in the resiliency and the ability to recover."

STAYING EDUCATED AND LEADING BY EXAMPLE

Matt believes in continuous education in order to stay ahead of trends and changes in the industry, but also to ensure they remain uptodate on threat actors. He always tells his team to carve out some time in their day or week to focus on areas such as emerging technology in the industry, or other areas they are personally interested. He encourages his teammates to be constant learners, to always think about their career trajectories and work on skills to elevate their industry knowledge, whether it's broad areas or something more specialized.

Not only does Matt encourage his team to educate themselves, but he does so himself in a number of purposeful ways. He likes to spend at least 45 minutes reading during the morning. Whether it is intelligence briefings or gaining insight into the industry through various types of publications, he finds dedicating time to improving his leadership, technical or soft skills incredibly valuable. Networking with his peers is also very important to Matt, he sees tremendous value in discussing challenges or use cases with them, to not only share his successes but learn from others. Whether it is technologies they are evaluating, frameworks they are trying to align to, or any other relevant area, there is always something to be gained from hearing what your peers are going through.

DATA GOVERNANCE

"Data governance is really a partnership. There's a strategic aspect between legal, compliance and security on the leadership side of things. And then there's the tactical aspect of us learning from the data stores or the data owners. We're not experts in data, and I don't think we should ever pretend to be. I think this goes back to the people aspect of learning from the folks that are utilizing the data and it's really a partnership in that realm, right? As the strategic implementers or governors of the data, we have to approach the data owners and understand what their responsibilities are and what they are doing with the data. It's really this give and take of what the expectations are because at the end of the day, they're going to know what's best for what the data is utilized for. At the same time, compliance data privacy, data protection, and data security are setting barriers and foundations for the data. Also, we often overlook the role of artificial intelligence. I think a lot of people are playing catch up to go back and create these two-way relationships, yet companies that created them from the beginning are probably doing better on the artificial intelligence side of things. The fear is that once you introduce artificial intelligence, it's going to look across the boundaries of your data and maybe pull back things that you didn't necessarily want it to. Good data governance is going to set the tone for how well you're doing from an AI perspective as you continue to grow."

PROFILES IN *Confidence*

MIKE GROSS

SENIOR DIRECTOR OF INFORMATION SECURITY

Globalization Partners

HEADQUARTERS: Boston, MA

Mike Gross has over 15 years of experience in IT and cybersecurity, and throughout his career has been focused on building strong, proactive security programs, ensuring he aligns with the business, and continues to grow healthy security cultures. Mike holds a master's degree in computer science concentrated in security and has a multitude of industry certifications.

Mike began his career working in systems and IT manager roles before moving into analyst, manager, and now senior leadership positions. As he advanced in his career, Mike had more exposure to security functions and how to successfully build teams and programs across different industries.

BUILDING A STRONG SECURITY PROGRAM

Currently, Mike works at Globalization Partners (G-P), which provides services for global employment HR, legal and compliance support. He began working at G-P over four years ago, starting as an Information Security Manager before moving into a Director, and now a Senior Director of Information Security role. He oversees the entire security program, leads a team of security practitioners, and collaborates across the business.

As the first security hire at G-P, Mike was responsible for building a program from the ground up. Having previous experience was immensely helpful and Mike leveraged that to implement strong security policies and set a clear roadmap for proactive growth.

Mike's success is built on his passion for security, he explains, "I've always been a very security minded person and helping secure companies is what I enjoy doing with my time. I am really passionate about it. It always makes the job easier, when you really like what you do."

Mike has grown his skillset and capabilities as the company has grown organically over time. When he started, he began working on foundational security components. And as the company grew, Mike ensured the security program grew alongside it and continued to align to the business goals. He ensures they receive appropriate resources to continue to grow the team, their technology stack, and to build out policies. He comments, "In the four years that I've been here, besides getting promotions, I've gotten more and more budget to work with. I've gotten more budget specifically on people to grow the team because there's been times that I've said this job for one person has grown into the job for two or three people. And to manage a work life balance, I'm going to need to hire someone else."

THE IMPACT OF ARTIFICIAL INTELLIGENCE AND AUTOMATION

One of the organization's current initiatives is around integrating AI into their products, specifically helping people hire in any of the 180 plus countries around the world. Mike shares, "The great thing is that it doesn't matter what country you are in, hiring in, or looking into hiring in. What this enables us to have is a large group of professionals who have the collective knowledge of all the HR and legal requirements of working in 180 plus countries around the world. What is difficult at times, especially for sales functions or other things where we're trying to answer questions for people, is when people have specific use case questions that are niche to their region. For example, say you need

"I've always been a very security minded person and helping secure companies is what I enjoy doing with my time. I am really passionate about it. It always makes the job easier, when you really like what you do."

to hire someone in Vietnam, instead of an HR manager having to go do their own research and look into specifics, we can use generative AI instead. You could be having a live conversation and instantly know all of the key federal holidays in Vietnam."

He continues, "It's a specific type of data set that we're trying to protect. It is a very advantageous data set to have for any company that's looking to expand globally. And protecting that and making sure that we're being good custodians over that data is a very important."

From a security perspective, Mike must ensure he is involved in strategic planning, so he understands the current and future business goals. Specific to AI, Mike must ensure he is protecting the data, the controls, and anything else involved in this type of AI technology being utilized.

Another area of focus for Mike and his team is automation. For example, he says the mean time to remediation or MTTR can increase significantly with large gaps and could cause a compromise. He says automation is the fastest way to get as small a MTTR as possible, and they've shifted their mentality of how that should work. He comments, "Automation has allowed us to speed up certain processes. For example, mean time to remediation or MTTR is really important for us to reduce the amount of time it takes, because the longer it takes, the easier it is for some type of compromise to occur. Through automation, we have sped up our MTTR which in turn shifted our team's mentality of how the process should work. Typically, we had AppSec team members looking at scanning results then sending some false positives off to engineering for them to review. Now, that process is automated, and engineering receives that data as quickly as it comes out of the scanner."

COACHING A SUCCESSFUL TEAM

Mike leads his team with compassion and a coaching mindset. The organization is global, and Mike has team members across the world helping with security related functions, to ensure they have 24/7/365 coverage.

He explains, "I have a global team because we are a global company. We have someone in Europe, India, Singapore, and other areas all helping with security related functions. As the company has grown, our team has grown as well."

Not only has Mike's team grown in size, but he ensures their skillsets are continuously honed, and that he has instilled a strong security culture that emphasizes a work life balance. He comments, "I find work life balance to be very important. I've told everyone that I've hired that work life balance is valued here. And I always want to make sure that we are keeping in mind that when people are hired and also after we have hired them, so they now we are still keeping it as a focus. It has been great to afford that to my team. We are also about 50/50 female to male and have great maternity or paternity leave. All of these things demonstrate that we care about our employees and value them."

Having a global team means Mike has opportunities to learn about people across the globe – their cultures, beliefs and values. And ensure he meets them where they are and works with them in the best way possible based on their specific skillset and approach to work.

"I've told everyone that I've hired that work life balance is valued here. And I always want to make sure that we are keeping in mind that when people are hired and also after we have hired them, so they now we are still keeping it as a focus."

DATA GOVERNANCE

"Data governance is making sure you have all the policy documentation and structure set up to properly govern data at your organization. Building sophisticated programs around that has always been part of the MO in general of any company that I've worked at. For instance, it's a big part of the GRC team that I've built here. Making sure that we're focusing on products and certifications that can help provide value to our customers is very important. As time has gone on, though, it's kind of seen that those are great programs to have, but how are you able to demonstrate them other than just having an ISO 27001 or SOC 2 Type 2 report? And how are you demonstrating to your customers on a regular basis that you are maintaining these things? We focused on technologies that can help us align to demonstrating that type of continuous compliance. It's how you can demonstrate that you're doing a good job instead of just telling people that you're doing a good job."

PROFILES IN *Confidence*

ROBERT KEEFER

CISO
PEW CHARITABLE TRUSTS

HEADQUARTERS: Philadelphia, PA

EMPLOYEES: 900+

ENDOWMENT: $6.7 Billion / Budget: $374 Million

Robert Keefer's career in IT and security spans over 20 years, with a keen focus on helping organizations achieve success by continually increasing trust and comprehensively improving security programs. Not only has Robert held many notable jobs across security functions, but he was a Cybersecurity Adjunct Instructor at the University of Michigan, has co-authored a book, and advised the Michigan Department of Health and Human Services on policy and procedure to secure the privacy of behavioral health patients.

Robert's previous experience includes Senior Security Analyst at Eastern Michigan University, Lead Security Architect at Health Alliance Plan, Information Security Program Manager at Harman International, then moving into CISO roles at Tweddle Group and his current organization as Associate Director, Security Operations at The Pew Charitable Trusts.

Robert has worked at The Pew Charitable Trusts for over four years, and shares, "Pew is a data focused nonprofit that focuses on research and programs that bring measurable results, which I really like. I'm very excited by the work that we do, and I currently lead a team of absolute experts in the field that are a delight to work with. They make me proud every single day of the work that we do. We work across the gamut, we take inputs from the SOC, we respond to incidents, we do preventative work, and we do consultative work both with IT and with the organization as a whole to ensure that they're being secure. We work with just about everything that might relate to information security and my team is absolutely fantastic at it."

EFFECTIVELY COMMUNICATING THE VALUE OF SECURITY

Robert views his role as one that requires strong communication. He explains, "My role as a leader is to communicate the value of security across the organization to various teams and to communicate the work that my team is doing to keep them safe and our data safe. Because it's not just about the people who work at Pew, it's also all of the people who trust us with their data. There's a lot of what the business will call reputational risk, but it's really trust in a very human way. And my job is to communicate the value of the work that we do to ensure that that happens."

He says he accomplishes this level of communication in a few different ways, with a heavy focus on face-to-face work, meeting with his executive peers across the organization, as well as participating or working with multiple committees. Not only is it important to meet with many executive peers, but ensuring the conversations are beneficial bidirectionally, both walking away with a clear understanding of the other's priorities. Having a strong relationship with the CIO is also important to Robert, and he believes all CISOs should work closely to ensure the CIO becomes a champion for the security program.

CLEARING ROADBLOCKS AND ENSURING SUCCESS

Robert's responsibilities include cyber security, IT risk and IT vendor risk with additional ties to collaboration with the legal team on data privacy. His role is to establish a vision for the program, hire people who can help him accomplish that vision, and then put trust in them to help him build and roadmap out the program. Overall, he says his job in a nutshell is to ensure his teams success.

He continues, "I clear away roadblocks for my team, I meet with them to ensure that they're making progress, help provide direction if they're stuck, answer questions if they have them, if there's a challenge that they're having with a team or a person or a technology, I'm there to help them with that. If other people are having a challenge with

"I don't avoid hard conversations, but I do avoid seeking blame. I prefer to look for solutions when a problem comes up rather than blaming people."

them, I'm here to help with that as well. I don't avoid hard conversations, but I do avoid seeking blame. I prefer to look for solutions when a problem comes up rather than blaming people."

FOCUS ON MATURING THE SECURITY PROGRAM

Robert and his team are currently focused on maturing their automation capabilities by automating their security response and potentially streamlining routine analytic work. The goal is to speed up the response time and reduce the time between detection and resolution. Much of this work involves scripting what they can script, but also taking areas of work such as vulnerability management or data management, and finding ways to automate so his team has the bandwidth necessary to react and respond in a proper fashion.

Evaluating their current tools is another area of focus, to ensure they still align with where they are headed as a team in terms of roadmap goals. Robert says, "We are working to make sure that the technologies we have invested in still align well with our current team and program goals and where Pew is headed as an organization."

Another program focus is around data identification and protection. Robert explains, "Our privacy program is relatively new from a formal standpoint. We've always looked at privacy, but the kind of concentration on a formal framework and a formal approach is fairly new for us. And one of the things that we're learning is that there's a lot of it out there. There's a lot of data out there." He says they want to be able to help the organization become more agile, with security helping to free up the employees to safely and appropriately share data with external partners. They are currently looking at tools to help identity where their data is and what it is sensitive to, so they can automatically apply rules to it. That way, if an employee wants to share data with a partner, they don't have to think about contacting security first.

Continuing on the topic of data governance, Robert says the goal is that if an employee is doing something of high risk, they have tools in place automatically stop them from doing so. It will not only help them out from a speed perspective, but it will do so without sacrificing security. He comments, "The question then becomes how can we become better partners to the organization rather than merely being Internet cops? And, I think one of the ways that we do that is by focusing on data governance as a business enabler rather than a limiter. How do we make it easier for our people to do their jobs without having to worry about whether or not they're doing the right thing?"

GROWING AS A LEADER

To ensure he continues to grow and learn, Robert says he is an avid reader, and enjoys staying up to date on leadership books, whether it's referencing something he has already read or reading a newly released book. He is also part of many organizations and professional groups such as ISC2 and ISSA. He gains a lot of value interacting with peers because of the frank nature of the conversations that take place, with genuine collaboration and discussion around challenges. He explains, "Sometimes sharing what I've been doing, is as valuable as learning what other people have been doing. Because it can help solidify in my mind the reasoning behind an approach, help me draw out some conclusions that maybe I hadn't thought of before because I'm talking them out with somebody else or just because I'm having the opportunity to think about them again in a different way. So that's always very useful and being able to come away from those full of different ideas that I can now sit and process. I find that incredibly valuable."

The Intersection of CISOs & Data Governance

By Katie Haug, VP Marketing, K logix

UNDERSTANDING THE INTERSECTION OF CYBERSECURITY AND DATA GOVERNANCE

Cybersecurity and data governance, while distinct disciplines, are deeply interconnected. Cybersecurity focuses on protecting data from unauthorized access and breaches, whereas data governance involves the management, usage, and protection of data to ensure its quality and integrity. Together, they create a robust framework for safeguarding an organization's most critical asset—its data.

In this interconnected landscape, data governance sets the policies and procedures for data handling, which cybersecurity measures enforce. Effective data governance ensures that data is classified correctly, access controls are defined, and data lineage is tracked. These elements are pivotal for cybersecurity to function effectively, as they provide the necessary context and controls to protect data.

THE ROLE OF CISOs IN DATA GOVERNANCE

In today's digital age, the volume of data generated is enormous, and its proper management is crucial for regulatory compliance, decision-making, and maintaining the trust of stakeholders. Effective data governance ensures that data is accurate, consistent, and secure, thereby supporting organizational objectives and mitigating risks.

Chief Information Security Officers (CISOs) are increasingly becoming central figures in the data governance landscape. Traditionally focused on cybersecurity, CISOs are now also tasked with ensuring that data governance policies are aligned with security protocols.

Their role has evolved to include not just protecting data from breaches, but also ensuring that data is handled ethically and in compliance with regulatory requirements. This includes collaborating with other departments to establish a cohesive data governance strategy that supports the organization's overall goals. This collaboration requires CISOs to deeply understand data governance and the impact from a cyber perspective.

Thus, CISOs play a critical role in safeguarding an organization's data. Their key responsibilities include developing and implementing data security policies, conducting risk assessments, and ensuring compliance with data protection regulations such as GDPR and CCPA.

Additionally, CISOs are responsible for incident response planning, which involves preparing for potential data breaches and establishing procedures for mitigating their impact. They also oversee the implementation of encryption, access controls, and other security measures to protect sensitive information. It is key these responsibilities are understood with any departments they are collaborating with in regards to data governance.

CHALLENGES FACED BY CISOS IN DATA GOVERNANCE

One of the primary challenges CISOs face is the ever-evolving threat landscape. Cyber threats are becoming more sophisticated, and CISOs must continuously update their strategies and technologies to stay ahead of potential breaches.

Another significant challenge is ensuring compliance with a myriad of data protection regulations across different jurisdictions. This requires a thorough understanding of legal requirements and the ability to implement policies that meet these standards without hindering

business operations. Additionally, CISOs often face budget constraints and must prioritize initiatives that provide the best return on investment in terms of data security.

BEST PRACTICES FOR CISOs TO ENHANCE DATA GOVERNANCE

To enhance data governance, CISOs should adopt a holistic approach that integrates security with data management. This includes establishing clear data governance policies, conducting regular audits, and promoting a culture of security awareness within the organization.

CISOs should also leverage advanced technologies such as artificial intelligence and machine learning to identify and mitigate potential threats proactively. Collaboration with other departments is crucial to ensure that data governance strategies are comprehensive and aligned with business objectives. Finally, continuous education and training for both the CISO and their team are essential to stay updated on the latest trends and threats in data security.

KEY DATA GOVERNANCE PRACTICES TO ENHANCE CYBERSECURITY

To enhance cybersecurity, certain data governance practices are essential:

1. Data Classification
Establishing a robust data classification scheme helps in understanding the sensitivity of different data types and applying appropriate security controls.

2. Access Management
Implementing strict access controls ensures that only authorized personnel have access to sensitive data, minimizing the risk of insider threats.

3. Data Quality Management
Ensuring data accuracy and consistency helps in identifying anomalies that could indicate a security breach.

4. Audit Trails and Monitoring
Maintaining comprehensive logs of data access and modifications aids in forensic investigations and real-time threat detection.

By integrating these practices, organizations can create a fortified data environment that supports both governance and security objectives.

As digital threats become more sophisticated, understanding the intricate connection between cybersecurity and data governance is crucial for CISOs.

CHALLENGES AND RISKS IN INTEGRATING CYBERSECURITY AND DATA GOVERNANCE

Integrating cybersecurity with data governance is not without its challenges. One major challenge is the potential for conflicting priorities. While data governance aims to make data accessible and usable, cybersecurity

focuses on restricting access to protect data. Balancing these objectives requires careful planning and collaboration.

Another significant risk is the complexity of managing data in a multi-cloud environment. Ensuring consistent data governance and security policies across different cloud platforms can be daunting. Additionally, the rapid pace of technological change means that governance and security frameworks must be continually updated to address new threats and compliance requirements.

FUTURE TRENDS: HOW CISOS CAN PREPARE FOR EVOLVING THREATS

As the digital landscape evolves, so too do the threats and challenges facing cybersecurity and data governance. Future trends indicate an increased reliance on artificial intelligence (AI) and machine learning (ML) to enhance data security and governance practices. These technologies can help in automating data classification, threat detection, and incident response.

CISOs should also prepare for the growing importance of data privacy regulations. Compliance with laws such as GDPR and CCPA requires robust data governance frameworks that prioritize user consent and data protection. By staying abreast of these trends and continuously adapting their strategies, CISOs can ensure that their organizations are well-equipped to handle emerging threats.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM