FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

EXPLORING THE CISO MIND

Trends, challenges, and insight

June 2018

WWW.KLOGIXSECURITY.COM

888.731.2314

K logix
Confident information security

TABLE OF CONTENTS

FEATS OF STRENGTH
A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE
CLEARING THE SECURITY PRODUCT CLUTTER
When everything looks the same, how do you invest in new technology?
March 2018
WWW.KLOGIXSECURITY.COM
888.731.2314
K logix
Confident information security

To view past issues, visit:
www.klogixsecurity.com/feats-of-strength

Magazine Created By:

K logix

Magazine Contributors Include:

Kevin West
CEO, K logix

Katie Haug
Director of Marketing, K logix

Kevin Pouche
COO, K logix

Marcela Lima
Marketing Coordinator, K logix

Contact Us:
marketing@klogixsecurity.com
617.731.2314

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 100+ CISO interviews, we extract trends in order to provide services that align business to information security.

LETTER FROM

KEVIN WEST

CEO

CISO TRENDS: SHARING WHAT WE HEARD AT THE RSA CONFERENCE

In this issue of *Feats of Strength*, we tackle top CISO trends and challenges. These come directly from interviews and conversations with CISOs during the most recent RSA conference.

In previous years at the conference, we spent our time meeting on the fly with customers and some of our CISO advisors. This year, we approached it with a different mindset. I attended with my colleagues Kevin Pouche (COO) and Katie Haug (Director of Marketing), and we set out to make an impact and have meaningful CISO conversations.

Our goal was to meet with as many thought leader CISOs as possible and conduct quickfire interviews to collect trends. Not only were we able to pull together strong trends for *Feats of Strength* articles, but we are taking action on much of what we heard to improve K logix's market approach and service offerings.

Here are some of the CISOs we interviewed:

- Chris Porter, CISO, Fannie Mae
- Cory Scott, CISO, LinkedIn
- David Levine, CISO, RICOH
- Meg Anderson, CISO, Principal Financial
- Mike Raeder, CISO, OrbitalATK
- Patricia Titus, CISO, Markel
- Richard Rushing, CISO, Motorola Mobility
- Rich Licato, CISO, ARC

We also interviewed CISOs who chose to remain anonymous, yet still provided quality, transparent answers to our questions.

As each CISO sat down in our suite over the course of a few days at the RSA conference, we began asking a set of ten questions starting with what trends are most prevalent at the conference. Some of the top trends and hot topics during our CISO interviews included AI/Machine Learning, Digital Transformation, GDPR, 3rd Party Assessments, and more. Here are a few snippets of thought around some of these topics:

AI and Machine Learning. Over 40% of the CISOs we spoke with said AI and Machine Learning were top trends, mainly the influx of messaging and hype around these topics. With so many companies competing for precious budget dollars from security teams, many used marketing hype tactics to attract new customers.

After speaking with many CISOs, we found they approach any company who touts the AI/Machine Learning message with caution. On page 15 in our CISO Q&A article, you can read more about what CISOs are saying about this hot trend from the conference, and currently facing the industry as a whole.

Digital Transformation. 100% of the CISOs we spoke with say their programs and organizations are impacted by digital transformation. We discuss their top challenges when it comes to digital transformation, including security being included from the start and trying to keep up with innovation, on page 14.

GDPR. 60% of the CISOs said their programs were impacted by GDPR. What I found interesting was many CISOs discussed the clear partnership that evolved from working with Privacy Officers during the GDPR readiness period.

Along with many other interesting and insightful trends, I hope you enjoy reading this issue of *Feats of Strength* magazine.

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

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JOHN MASSERINI
CISO, MILLICOM

HEADQUARTERS: Luxembourg City, Luxembourg
EMPLOYEES: 18,000+
ANNUAL REVENUE: $6 Billion

Three-time CISO John Masserini brings in-depth experience through extensive work in all facets of information security for over twenty-four years. Throughout his career, Masserini experienced the rapid transition and impactful evolution of the role of security leadership within organizations.

He comments, “Historically, security was considered a technology problem. In some enterprises, it is still that way today. In my view, it’s about managing the risks and making sure there are strategies in place that find the spot between balancing technology risk, protecting our sensitive information, and continuing to help the business drive revenue. While my background is very technology-centric, most of my days are spent evangelizing and ensuring both business and technical risks are mitigated in the best possible way to protect our subscribers’ information and support the company’s strategic revenue objectives. At Millicom, we’ve taken the unique approach of moving the security and risk function into the Compliance and Ethics group, rather than have a direct line into the technology group. This provides a separation of duties that is often lost when CISOs report to CIOs.”

DEVISING A GLOBAL STRATEGY

The desire to come into an organization and implement a strong global strategy sparked Masserini’s interest in joining Millicom, a leading provider of cable and mobile services dedicated to emerging markets with more than 51 million customers across the globe. While each individual country has Information Security Officers in place, the organization recognized the lack of a cohesive, globally-driven security strategy. Masserini explains, “The ability to come into a place and pull together all the experts throughout the company and build a cohesive strategy was incredibly intriguing, and ultimately why I decided to join.”

He continues, “We have country operations throughout Latin America and Africa as well as back office operations in Luxembourg, London, and Miami. Each operation has different risks which they have to deal with, both from a technology perspective and from a business continuity perspective. To pull all those together and come up with a standard strategy is something that is certainly challenging, but exciting at the same time.”

Not only is establishing a strategy important, but strong intra-communication is a vital component of linking the global operations. Masserini acknowledged the importance of instilling this in his 18-month plan. He comments, “It is really about leveraging the collective experience. It is about building a communication infrastructure where we can all share ideas, experiences, and what works and what doesn’t. By being able to share awareness materials, attack and compromise signatures, third-party risk assessments, or even job descriptions, we can better utilize the existing teams to manage the evolving risk. This same approach applies just as well to the technology side– whether it's a shared Identity Access solution or a global Security Operations Center. The goal is to leverage the best of what we already have rather than reinventing each time. That's really driving the next 18-36 months from now."

BOARDROOM BALANCING ACT

"Our executives truly feel that security is critical to the future of our success; it's something we need to not just focus on, but it needs to be part of our culture," says Masserini. Having strong support behind continuing to improve and grow information security enables Masserini and his team to set clear goals and report back on progress.

When presenting to the board, Masserini believes presentations and conversations must revolve around business risk in terms of risk management and mitigation. He typically avoids talk about specific technology products or technical alerts. He explains, "It's all about understanding risk and being able to articulate that risk to the board and to the audit committee. It's not a discussion about the technology, it's about translating the risk into what your audience cares about and the perspective they have. They want to understand the risk to our customers, a revenue stream, or the corporate reputation, regardless of the source. It doesn't matter if it's a vulnerable application, a DDoS risk, or the potential of a fire in the data center. If there is a potential of a revenue impacting event, they need to understand the potential loss and the probability of that loss occurring. They don't care how we found it, they want to understand what they can do to fix it."

Masserini advises other CISOs to approach board meetings like a balancing act. You must understand the board's perspective and keep that in mind when you are presenting or answering questions. CISOs must hit on the big items without going into technical detail to ensure a successful and productive meeting, regardless of the length of time they have to present.

TRANSFORMATION WITH THE CLOUD

A personal goal of Masserini was to work at an organization that recognized the value and importance of the cloud. It was clear to him that Millicom readily adopted the cloud, and is undergoing a transformative period that Masserini plays a key role in.

He says, "With the cloud, we can provide a common platform to all of the country operations without provisioning hardware and data center space in each location. Obviously, there are some inherent risks, but those risks are what we're working on right now. We are slowly plowing through and addressing them and making sure that we're protected contractually, protected on an insurance basis, and then protected from a technology perspective. I love how cutting edge this company is, they have very focused approaches or ideas on how we can mitigate risks without the typical, 'I would just make this password stronger' or 'throw some sort of device in'."

HOLISTIC APPROACH TO REGULATIONS

The main business lines for Millicom are in Latin America and Africa, with each country requiring specific regulations, like those of General Data Protection Regulation (GDPR). Masserini and his team are part of a corporate-wide effort, working with the Legal and External Affairs teams, to satisfy GDPR and other global requirements to adhere to the vast majority of regulations in all of their operating countries.

He explains, "Fulfilling GDPR is coming from a global perspective and not just from a local view, but there are also other things to consider. It's about building the strategy that satisfies all the different global requirements that we have. It's not just GDPR, it's a privacy and data protection program that in some ways goes further than GDPR and in some ways, is a bit more specific than GDPR requires. The idea was to build the holistic strategy, not one that's just interested in one regulation."

PERSONAL GROWTH

> "One of the most beneficial things I do from a career perspective is find ways to "peer review" projects, approaches, or initiatives. Before moving to Miami, there was a regular group of New York City CISOs who would get together for dinner where someone would present a topic or project "Chatham House Rule" style. Frank, open dialog with an understanding of total confidentiality. It's wonderfully courteous and completely professional, but make no mistake, you get grilled. It's a baptism by fire at its finest. That said, the experience leads you to understand that your perception is different than others, and what may be clear to you is something someone else may not understand. It is extremely humbling, and incredibly valuable to personal growth, especially if you're new to the CISO role or when you're dealing with a new Board."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

MEG ANDERSON
CISO, PRINCIPAL FINANCIAL GROUP®

HEADQUARTERS: Des Moines, Iowa

EMPLOYEES: 15,000+

ANNUAL REVENUE: $13.9 billion in GAAP revenues, $1.5 billion in non-GAAP revenues, $2.4 billion net income

> "I am constantly challenged and busy here, and enjoy that pace and energy. We are currently number four on the Forbes list of America's Best Employers (2018) and I truly believe it is a wonderful place to work. I am surrounded by an engaged and diverse team who understand how they impact our customers and business. Given the cybersecurity talent gap, the fact that our team has an average tenure in the 15+ years range is amazing."
>
> **- MEG ANDERSON**

Meg Anderson, CISO at Principal Financial Group®, a global financial investment management and insurance organization, possesses a unique background and exceptional leadership experience. Anderson began working at Principal® in 1987, working her way up the organization while holding a range of IT roles. In these roles, she handled a diverse set of IT issues and strongly built up her business practice experience. Her initial glimpse into information security occurred when certain components of her responsibilities exposed her to a variety of regulatory aspects of privacy and HIPAA, some time before information security became widely prevalent in organizations. In 2008, Anderson was approached about an opening for the CISO role, something she somewhat blindly agreed to, without understanding every facet of what the job entailed.

Anderson says, "I had no idea what I was getting myself into. My experience with HIPAA and privacy laws helped me understand some components of security, but I didn't understand the full breadth of information security at the time. However, having some business unit background allowed me to consider the impact of our evolving security program on our business strategies and to be in a position to use that context as we strengthened the program in the face of increasing external threats." Throughout her career, she has experienced tremendous growth as a business leader and evolved into a well-versed information security expert.

Anderson links her 30+ year tenure at Principal® to the strong company culture and fast-paced, challenging nature of work. She comments, "I am constantly challenged and busy here and enjoy that pace and energy. We are currently number four on the Forbes list of America's Best Employers (2018) and I truly believe it is a wonderful place to work. I am surrounded by an engaged and diverse team who understand how they impact our customers and business. Given the cybersecurity talent gap, the fact that our team has an average tenure in the 15+ years range is amazing."

Longevity at Principal® offered Anderson advancement in both a personal and professional capacity. She explains, “From a personal perspective, I’ve learned how to interact with executive management better, up through the CEO, board and audit committee, something I didn’t have exposure to before. Professionally, I’m at a point where these audiences are asking questions and engaging with me more than ever before.”

CUSTOMER TRUST AND INNOVATION

Customer trust is a core component at Principal®, and the information security program holds a prime position to ensure this remains consistent. Anderson states, “Like many companies, we have lots of pressure to make sure we are not the next company in the news. Aside from reputational risk associated with a breach, we operate our business on customer trust by making sure we keep their data and money safe. The amount of investment security receives has increased, which is partially fueled by our digital business strategies.

For Anderson, one aspect of digital transformation is improving customer experience to offer faster and more seamless interactions and the ability to quickly resolve any needs. She comments, “I would describe digital transformation using words like velocity and agility. Things are moving at a fast pace as we innovate and use data in new ways. We need to think about things like providing solutions that scale for larger customers, and offering secure and innovative solutions to grow revenue and our customer base. The bottom line is continuing to earn customer trust throughout this transformation.”

While many CISOs experience struggles to ensure security is involved in initial planning and conversations about digital transformation, Anderson believes in security being an enabler of innovation to solidify that speed and trust are baked in. She says, “We need to work security into the process from the start, make sure it’s built in by design and not a bottleneck on the backend. Doing so saves time and money.”

To accomplish this level of alignment and enablement, Anderson says you must understand why the organization is deciding to innovate or create new products and services for the marketplace. She believes once you understand this, it is easier to help those driving innovative initiatives in the organization. In doing so, you can demonstrate how the information security component will ultimately help them get to the end goal quicker, or avoid having to redo any aspects of their project. Anderson explains, “You cannot throw information security policies at someone and walk away. You must understand their business objectives and what they are trying to accomplish. There’s flexibility in collaboration, which leads to quicker achievement of the goals”

BUSINESS-FOCUSED METRICS

As a seasoned professional with many years of experience reporting and presenting to the board, Anderson relies on specific, business-focused metrics. She does not think Boards want CISOs to report every incident to them, but instead, barring any significant events, share select minor incidents so they gain a sense of what is happening, why it is happening and the response process. She says, “The board needs to be confident that if an incident occurs, we have a comprehensive process in place that includes the right people.”

Anderson uses board discussions as opportunities to educate members quarterly on any relevant news of interest. She explains, “For example, if ransomware is increasing in the news, we help the board understand what it is, what we are doing to protect ourselves ,and give them a level of confidence that we are doing what we should be doing.” She suggests other relevant topics to educate the board on may include identity and access management, the regulatory landscape, threat intelligence, and supply chain risk.

EMPOWERING TEAM MEMBERS

As a leader, Anderson believes in a strong company culture and enabling her team to feel empowered, to instill passion and commitment. She comments, “We embrace diversity and flexibility. Most team members can work from anywhere. We also empower our team, they are encouraged to have two-way conversations and a voice of their own. I’m a big believer in healthy debate and open dialogue for problem solving and to show people they are valued.”

Anderson puts a heavy emphasis on building the next generation of leaders. She values recognizing the need to develop successors and prepare cyber leadership for the future within her own company. By doing so, she aspires to make an impact on the upcoming group of information security leadership.

Q & A with Erin Benson:

Learning About K logix's Actionable Risk Assessment

We speak with CISOs on a regular basis about their challenges and their need to gain a clear picture into their entire security program. They want to understand prioritized action items for improvement, and for their security programs to make a positive impact on the business and create a competitive advantage.

Many CISOs complete risk assessments, however the majority tell us they are compliance-driven, done internally, and/or lack key directives to advance their program. We listened to these needs in the marketspace and recognized many risk assessments lacked executive-friendly results and failed to include specific, prioritized action items.

In response, K logix established an Actionable Risk Assessment (ARA) service, spearheaded by Erin Benson, our Security Practice Director.

In the following Q&A, Erin answers questions about ARA's impact on security leadership and business executives. If you'd like to learn more, don't hesitate to let us know; info@klogixsecurity.com.

Q: What do traditional risk assessments lack?

Erin: I worked for 10+ years in the traditional IT audit space and completed more than 100 risk assessments. What I found was companies often take a prioritized list of findings from the audit and attempt to take a "divide and conquer" approach to remediate findings. The problem with this approach is it lacks top-level strategic planning, which results in redundant efforts and a focus on the surface-level symptoms instead of underlying root causes. Successful advancement of enterprise-wide security posture demands a strategic approach to planning and sequencing of security initiatives.

Furthermore, traditional risk assessments are often done internally, which can lead to a host of problems. First, while an internal assessor may have a handle on their current security program, they sometimes lack knowledge or perspective on how it can be advanced, strengthened, or improved. Second, internal staff may be reluctant to assign blame to their coworkers (or themselves!) for problems they uncover. Finally, there is a common misperception that risk assessments create an incremental quantity of "extra work" for the security team. The reality is risk assessments often uncover time-consuming manual processes and identify opportunities for automation, integration, and efficiency. Risk assessments may "unburden" the security team by highlighting the "roots" of security problems. Vendor management, cross-functional project management and enterprise risk management – oftentimes remediation of critical security risks requires these functions to "step-up" their protocols.

Q: How does ARA provide a basis of alignment for security programs?

Erin: To start, ARA results are tailored specifically for the customer's executive teams and budget decision makers. Then we anchor our findings to the framework of their choice, whether it's NIST or ISO. We also have the ability to take previously produced findings from NIST or other assessments and plug them into our ARA methodology.

The results are grouped into twelve common 'root cause' areas, which means security teams won't have to sift through (and try to make sense of) a long list of findings. Additionally, the findings are mapped according to a customer's relevant regulatory and certification targets, such as GDPR, State Privacy Laws, HIPAA, SOC 2, and more. Finally, we provide a roadmap that concisely lays out the progress of remediation efforts, target areas, and business-focused action plans.

Q: What makes ARA results business-focused?

Erin: Simply put, ARA builds trust by clearly showing where a company's security program stands, where it needs to be, and how to get there. Importantly, our findings are based on a maturity scale that is gauged relative to similarly sized businesses in our customer's industry. This gives security leaders a simple tool for justifying budget and gives executives the ability to measure progress over time.

Q: What deliverables does ARA provide?

Erin: An effective risk assessment should provide two things: executive engagement via a compelling high-level summary and security team guidance via specific risk-mitigation recommendations. K logix's ARA does just that with a clear and concise matrix, narrative report, and business-friendly presentation. The matrix includes control-level findings and detailed recommendations for closing gaps and the narrative report supplements this information with strong reasoning and details behind the maturity scores and results. Together with the business-friendly presentation, ARA helps security leaders make compelling, quantifiable business-cases to budget decision makers to enable ongoing security program advancement.

Erin Benson has over one decade of experience in client-facing cybersecurity roles including selling, consulting and evangelizing to security management and executive leadership. She is passionate about helping companies drive the advancement of their security program and posture in a proactive and preventative direction by leveraging security solution automation and integration benefits.

Erin has a deep understanding of all aspects of security program operations, and how regulatory and compliance requirements impact security strategy & budget decision-making. Her experience includes: cybersecurity program and IT control environment analysis, remediation, readiness and compliance for: CIS Top 20, GDPR, PCI DSS 3.2, SOC 2 Type 2, NIST Cyber Security Framework (CSF), NIST 800-53 r4, PCI DSS 3.2, HIPAA, FERPA, GLBA, COBIT 4/5, ISO 27001/2, FFIEC IT Handbooks.

She has worked in financial services, pharmaceutical, healthcare, higher education, technology service providers, retail, and state/federal government.

MAKE CYBERSECURITY A COMPETITIVE ADVANTAGE

With K logix's Actionable Risk Assessment

The results from K logix's Actionable Risk Assessment (ARA) service enables you to:

Benchmark to Improve Executive Engagement

The ARA results help convey to your executives:

1. **Maturity Level:** Benchmark where you are
2. **Target Maturity:** Where you need to be
3. **Strategic Planning & Budgeting:** How to get there

Proactive, strategic planning and **justified** budgeting

Empower executives and gain their **commitment**

Correlate security decisions to **revenue pipeline**

Build Confidence with Customers

ANCHOR TO A FRAMEWORK:

NIST CSF

ISO 27001

Map results to **regulatory compliance** and **certification readiness**:

GDPR

STATE PRIVACY LAWS

SOC 2 Type 1 & Type 2

HITRUST

3RD PARTY ASSESSMENTS

HIPAA

Align to business goals and enhance security's reputation.

Accelerate the Time to Actionable Results

We group findings into prioritized, business-focused areas.

12 Root Cause Areas

(Unique to InfoSec industry)

Receive actionable, independent 3rd party results in 6-8 weeks.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

RICHARD LICATO
CISO, THE AIRLINES REPORTING CORPORATION

HEADQUARTERS: Arlington, VA

MEMBERSHIP: 229 airlines, 7,000 travel agencies, 12,000 points of sale

ANNUAL REVENUE: $88.5 Billion airline ticket transactions settled in 2017

Rich Licato describes the path that brought him into information security as “almost by accident, then by design.” Licato began his career as a developer, moving into coder roles, then management and delivery of larger projects over time. He eventually transitioned into enterprise architecture, where he moved from the delivery of systems to the design of how systems were delivered. By performing more strategic responsibilities, he gained an understanding of how a multitude of program components work together, instead of working in silos. He says, “I gained more exposure into an enterprise-view and had my first opportunity to manage security and enterprise architecture. From a corporate perspective, I saw different challenges. I also had the opportunity to work in an operational risk role before becoming CISO at The Airlines Reporting Corporation (ARC).”

As CISO of ARC, Licato ensures the organization meets their mission, which includes driving air travel intelligence and commerce, providing business solutions and travel agency accreditation services, and processing financial management tools and data. Now over six years into his role, Licato has a clear picture into the organization’s operations and business functions, all of which are owned by eight major airlines.

The opportunity at ARC presented Licato with the ability to re-establish a security program, and re-energize and re-focus the organization from a security perspective. Licato explains, “I was doing consulting work for ARC and able to see how the organization operated and what challenges they faced as an outsider. I was then invited to become an insider as their CISO.”

Licato felt the personal and professional growth opportunities significantly appealing as he became ARC’s full-time CISO. He comments, “From a security program perspective they were in a place of transition. There wasn’t a dedicated leader in the security space for them and there

> “Three things I’ve always been taught are to take stock of where you are, where you want to be and have the ability to articulate how you’re going to get there.”

was a large hole to fill. In the past, I've been a problem solver and I had the ability to set a strategy and vision. I was excited to make my own program and put my stamp on it. I was also lucky to have a leader and boss who supported me."

Not only did the growth potential appeal to Licato, but ARC's culture and environment were ripe for providing him a platform to build his program. He says, "During the interview process I made sure to understand the organization's attitude towards security. It was clear I had an opportunity to make an impact. CISOs must understand they might be able to affect the culture, but they might not be able to change it significantly from a process perspective. CISOs need to know what their constraints are and the attitude of management towards risk and security. Understanding the top down view of whether security will be supported is important."

BUILDING A STRONG PROGRAM

On building a program from the ground up, Licato states, "Three things I've always been taught are to take stock of where you are, where you want to be and have the ability to articulate how you're going to get there." Taking stock of where you are involves a great amount of self-evaluation, something Licato relied on his team to help understand. After engaging with the current team and gleaning valuable program information, Licato says creating a baseline using a framework must be done along with developing relationships with business leaders.

Licato states that establishing strong lines of communication with executives is important. "It doesn't matter what your opinion is, what's most important is their opinion on how security should function," he says. "What I mean by this is sitting down with each business leader of legal, product development, services, among others, and understanding their perspectives and expectations for security. I need to know what challenges they are facing, what problems they have, and how I can address them."

After partaking in crucial conversations and aligning with executives, Licato comprehensively understood the important business functions, how the business makes money, and was armed with information to build his program with a robust strategic focus. Licato explains, "It was clear to me I had to protect our most important assets. We make money through our settlement business that accredits travel agents, and back-end settlements from a financial transaction perspective. I need to make sure transactions are secure from beginning to end with no ways of compromise. We also have facilities for agents to charge for their services, and a data business. My mission from a business view is to secure information and ensure it will not be compromised. I am focused on less friction in a transactional environment, not putting up roadblocks that stop the business from settling transactions more efficiently, and handing the agents facility."

STRATEGIC TEAM GROWTH

Due to ARC's security professionals taking on more responsibilities and functions, Licato's team continues to experience significant growth. When Licato started at ARC his team had only a few people, which he has now grown to more than twenty members.

On building a successful team, Licato says, "For me it's about passion and intelligence. I'm looking for smart people who I can train in security functions. I'm looking for people who have an analytical nature and are always asking questions. Also, some level of skepticism sometimes works well in security." Licato leads his team with openness and honesty, to encourage them to have effective communication. He does not micro-manage, but instead creates a safe environment with everyone on the same page.

BOARDROOM FOCUS

"To me, boards are always asking if we are okay. And that can mean a lot of different things to different people. What does okay really mean? You normally don't figure it out in just one board meeting. Typically, from a program perspective, it means 'are we protected if something occurs?' Sometimes it can be a hard conversation for a board. CISOs must make sure they communicate the inevitability that something bad could occur and have adverse effects in terms of reputation or operations. Trying to have that conversation is hard, but it is necessary. There are ways to illustrate that we are okay and doing the right things and spending the right amount of money. Boards want to know what kind of protection the organization is getting for what they're spending on security. The bottom line is they want to know how you are enabling the business."

Chris Porter
CISO, Fannie Mae

Cory Scott
CISO, LinkedIn

David Levine
CISO, RICOH

Meg Anderson
CISO, Principal Financial

Mike Raeder
CISO, OrbitalATK

Patricia Titus
CISO, Markel

Richard Rushing
CISO, Motorola Mobility

Rich Licato
CISO, ARC

Here's *who* we interviewed:

CISO ▸▸ Quickfire Q & A:

Top trends, challenges, and insight

During the RSA conference, we asked leading CISOs their thoughts on current trends, and in this article reveal their answers.

Throughout quickfire 30 minute interviews, we asked each CISO the same questions and compiled them to provide insight into current CISO challenges, approaches, and strategies. The topics we asked included:

- Digital transformation
- Clearing the security product clutter
- GDPR
- CISOs top strategic goals
- 3rd party assessments
- RSA conference trends
- Metrics and benchmarking

All of the statistics, polls, and content you read in the next few pages are directly from the CISO interviews we conducted over the course of the conference.

The first question we asked CISOs was - what words would you use to describe your own information security program?

EDUCATE
OPERATIONAL EXCELLENCE
PROTECT
RESPOND
MEASURE
CULTURALLY AWARE
SECURE
COMPLEX
ENABLEMENT
LIGHT
MATURE
RESILIENT
PLAN
TRUST
CONSULTATIVE
HELPFUL
INNOVATIVE

The top words used by CISOs were **enablement, protect and respond, and trust.**

ENABLEMENT. CISOs who value enabling the business are working hard to align with, and educate, executives in order to embed this approach in the organization’s culture. These strong cybersecurity programs fuel innovation by encouraging the expansion of digital offerings and business strategies.

Furthermore, it means allowing the organization to function and operate as a revenue generating, innovative organization without security being perceived as a negative impact. It is all about enabling business strategies so CISOs can encourage innovation as organizations grow, without the implications of security challenging the ability to do so.

PROTECT AND RESPOND. Not only do CISOs want to fully enable the business, but they want to ensure they are protecting and responding at the same time.

“We are here to protect the digital assets of the company and to respond appropriately when there is something averse happening to us. Every good CISO is a good risk manager and not necessarily a technologist. They must understand their business and the risks their products and services face. From a cyber perspective, they build an investment portfolio around protecting and mitigating those risks in the long-term,” says **Mike Raeder, CISO of OrbitalATK.**

TRUST. There are different types of trust that CISOs strive for, including customer trust, executive trust, and team trust. One core component of a CISO’s program is ensuring security is baked into all facets of the organization and to ensure customer data is safe and protected. In many organizations today, organizations are transparent with customers about the level of security in their services or products, encouraging trust.

On describing his security program, **Rich Licato, CISO of ARC** comments, “I would say trusted, secure and culturally aware. What are you doing for security awareness? Cybersecurity is not a department, but an attitude. It must be ingrained within the culture for it to be effective. That’s probably the toughest thing for a CISO to establish because culture is so hard to change and it’s about trying to find the ways to change that conversation in order to change the culture and get everybody on the same page.”

Other CISOs have cohesive missions they use to describe their programs. **Christopher Porter, CISO of Fannie Mae** explains, “I’d describe my program with – get right, get small, see big. Get right is continuously fixing all the things that are broken and building in the culture that it’s OK to find broken things and track them until they’re fixed. Get small is shrinking attack footprint, and consistently doing this across all phases, whether it’s network, data, access. See big is having visibility to proactively and quickly respond and remediate any known security issue that you have.”

Overall, CISOs don’t differ drastically on words they use to describe their programs. When asked if their executives would use similar words, most CISOs believed they would.

Q: What is the impact of Digital Transformation on your program?

Anderson: “There’s all kinds of things that are wrapped up into digital transformation that we need to pull out and figure out what they mean from a security point of view. Meanwhile, we still have demands from regulators, customers, and our supply chain to be sure we are doing the right thing with our data.”

Porter: “Security has definitely become a little bit more of a culture change in the last few years that I’ve been there, but we’re part of those discussions about protecting that data, but also just the discussion about how long we need to retain that data. It’s my job to ask those questions. Our security journey is wrapped up in the digital product organizations journey to have better customer service and transform the business.”

Raeder: “It’s a race to keep up with digital transformation and everyone wants to take advantage of benefits from digitizing the enterprise. We, as security technologists, have to work alongside IT peers, like the CIOs and CTOs within our organization, to make sure we are part of the strategic planning at the upfront. Security should be working side by side with enterprise functions from the beginning and not coming after the deployment of digital implementations.”

Rushing: “We have been undergoing digital transformation for 7 years now and are on version 9 of our cloud strategy. It has been my job to ensure security is embedded in digital transformation in a frictionless way.”

Scott: “We’ve always been digital. So, what’s interesting now is, what does the next type of digital transformation mean for a company like LinkedIn? I think it’s adoption of additional advanced technologies such as machine learning or AI, determining how those can have an impact on the security of the products that we build and how we can leverage that technology to actually make our products more secure.”

Titus: “Digital transformation is a huge effort that a lot of companies are undertaking. What does digital transformation mean to your organization and how does security overlay into it? How do we overlay

Biggest challenge facing digital transformation?

1 Struggling to be included in conversations from the beginning

2 Ability to keep up with innovation

security operations to make sure that we're supporting the business needs as they become more flexible and agile?"

Q: What is the impact of third party risk management?

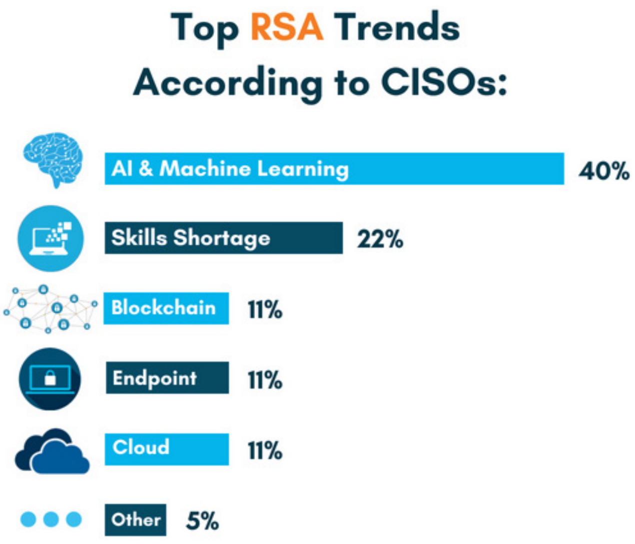
Anderson: "I think it's painful for the industry as a whole. Ever since the Target breach, regulators have been scrutinizing third party risk management practices. And especially with digital transformation, we're going to use more and more partners. The expansion of API's has also made this very critical to get right. We need to know more about who we trust with our data and the data of our customers and employees."

Licato: "It's an additional risk exposure because now their security posture is your security posture. Depending on the criticality of the vendor, it's really what you need to figure out. You must take a risk-based approach in terms of vendor assessments."

100%

of **CISOs** believe 3rd party assessments are a pain point for the industry

AI and Machine Learning: Fighting Through the Hype



AI and Machine Learning inundate marketing messages, and from the RSA conference to the industry as a whole, they are feeling the hard push of these concepts. Through our interviews, we learned how CISOs are overwhelmed and increasingly alert about security companies touting the AI/Machine Learning message.

When asked about the top trends at the RSA conference, **David Levine, CISO of RICOH** responded, "AI is definitely a buzz word. The real question is what are companies actually doing regarding AI? In theory, it sounds great, but how do you translate the theory to practicality and put it to good use?"

The bottom line is the majority of CISOs don't believe, or buy-in to the hype. They question the viability of many security companies actually engaging in true AI and Machine Learning capabilities, showing us how the mania in the market is engendering distrust and extreme caution.

Another factor impacting security leaders is many companies offering different variants of AI capabilities, causing attention when it comes to layering these solutions. Levine continues, "If everybody's now trying to do machine learning, AI, and behavior analytics, how is this all going to play together/integrate? I think it's going to be interesting to see how that actually pans out. For example, if you have multiple solutions deployed at different "layers" all utilizing AI/AI variants, and a user calls in and says I can't get to a particular website, you may have to chase down multiple solutions to figure out which one is trying to declare that it's a threat of some kind. You can experience this dynamic today to an extent, but multiple solutions all using variants of AI may complicate that process."

Levine: “I finally indoctrinated someone on my team to help review the assessments we are asked to complete because I do think they are important. You have to be able to evaluate the risk and security of your third and fourth parties, but the way we do it today is broken. It’s just not effective. We keep trudging down the same path, and I have yet to see a silver bullet solution to solve this.”

Titus: “Third party vendor risk management is finally getting the type of attention we’ve been hoping it would get, so we’re seeing contract language changes. Also, a lot of changes based on GDPR, so we’re getting more questions starting to filter out of our European theater than we do in the US. The US is still lagging a bit.”

Q: How do you report on metrics and benchmark?

Levine: “Like everybody else, we still struggle with trying to find what the best metrics are to convey to the business. At the end of the day, it’s about knowing your audience, what’s important to them, and what level of detail they like. For example, I do a quarterly governance report where I focus on high-level metrics and initiative updates. I also conduct a Global Information Security report that has far more detailed metrics and operational data.”

How CISOs Track Metrics:

NIST Assessments

KPIs and KRIs

Benchmark against industry peers

Specific benchmarking tools

Licato: “I have 13 metrics that I look at on a monthly basis that either talk about the effectiveness of the program or operations. I’m trying to keep them at a high level and when we talk about metrics, a lot of people like to see colors. So, we talk about being red, yellow and green, but in a different context. Red would mean management needs to take an immediate action, yellow would mean management needs to monitor this area and green means management does not need to take action at all.”

Porter: “We report metrics to the board quarterly. We also talk to the board about what our target state is, and where we want to be in the next two years. They absolutely want to know how we stack up against others in the industry and whether or not we’re doing the right things.”

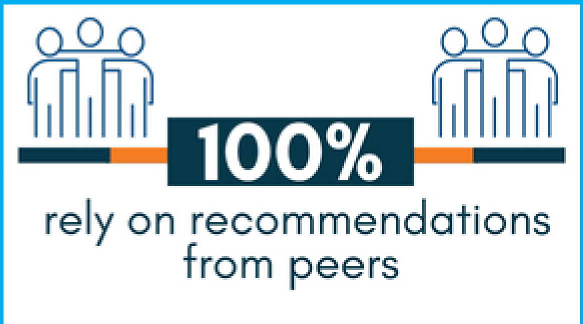
Rushing: “I think about two factors. One is collecting true metrics around my program maturity and framework and the ability to define where I am. I need to understand that if I want to move up in maturity what that means from a policy, procedures, and budgetary perspective. The other is technical benchmarking against competitors that I can then use on my own program.”

Scott: “I think it comes down to ensuring objectives are aligned on what the security organization is supposed to bring to the table. At LinkedIn, the focus is on ensuring member trust with the products we build, securing and hardening our infrastructure, and being resilient when bad things happen. It’s really important as a CISO to have a very clear and crisp narrative about what those security objectives are and receive buy in from additional internal stakeholders.”

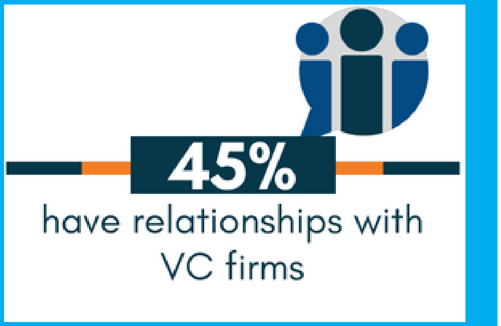
Titus: “KRI’s are really a great way to do it. Board reporting is a challenge because every board is not created equal. Some companies I’ve worked for have wanted to tell the board everything. Other companies have been more about making sure that we’re giving information that is relevant. Figuring out that balance with your board of how much or how little information is key.”

Q: How do you clear the security product clutter and select the right product for your needs?

Levine: “Step one is to determine what your requirements are, what problem(s) you are trying to solve, and what the business purpose for the product/solution is. Once you have that documented, the field of available options is usually narrowed down. Next, looking at business viability, integration capabilities, and general fitment with your existing tool sets all come in to play. For example, we were recently looking for a Cloud Access Security Broker (CASB) solution. While there are numerous solutions out there, once we evaluated the options based on some very specific requirements we were down to just a few to evaluate.”



Licato: “You must have a process. What is the business, and what are the business goals? First you must align to strategic goals. You have a conversation about who the leaders are, and you start with the leaders. Is it going to enable the business and create less friction for you in your environment? Then for us, it really comes down to getting to know yourself and what you are willing to do.”



Raeder: “I don’t put all my eggs in one basket when it comes to relying on industry publications and reports. Those help me narrow down options, then I depend on reaching out to my peers and talking within my own industry about how they are solving a particular problem. When I do have it narrowed down, getting references within my own space is invaluable. I ask peers how they used the product and what their feedback is on its ability to solve my specific problem. I’ve done this with the last four to five major investments we have made.”

Rushing: “To clear the clutter, you have to look at your own environment and understand how it best functions. I see the biggest thing as people trying to find an ‘easy button’ or some product that is overly simple to leverage and use. It is a nice place to be, but in this world of different options with 2400 security companies, it’s not because they all solve the same thing. You must test your products, see how they fit, that can provide that kind of force multiplier that you want to actually have.”

Titus: “Some CISOs are on the more cutting edge and are leaning into some of the newer stuff, and they’ve got the money to be able to bring them in as research partners. But many of us don’t have that capability. So, I’m going to listen to my peers a lot to see what they’re doing. I have to think about what industry they’re in. Are they regulated versus non-regulated and does that make sense for my own industry.”

Q: What impact does GDPR have on your security program?

Anderson: "If you think of the old adage, if you have a good security program, compliance isn't going to be a problem for you, I think GDPR is a little bit different. It's really about the privacy of the data and the scope of the data has expanded. How data governance has been approached has varied across industries and programs. Understanding all the data that's been collected, our rights to the data and how we anonymize it has been and will continue to be quite a big focus at our company and across the financial services industry in general."

60%

of CISOs polled say their organizations are impacted by **GDPR**

Scott: "GDPR has reinforced the importance of making sure that we adhere to privacy principles about providing our members clarity, consistency, and control. What we've done as part of our security program is ensure that all of our products continue to meet that bar and make sure that they're aligned with the regulatory standards."

Q: Why are business alignment, revenue generator, and competitive advantage top strategic challenges for CISOs?

Anderson: "We all have finite resources and we need to be sure our security priorities align with our business priorities. I'm lucky to participate in our strategy process which starts with the business."

70%

of **CISOs** believe business alignment is the most important strategic goal

Porter: "With impacting revenue, I think it depends on what type of company you are. If you're a B2C company and you can tie your security technologies and trends that you're implementing to reduction of fraud, then you can make that play that you're reducing cost, reducing bottom line. When you're a B2B company like we are, that's a bit harder to quantify."

Titus: "How do you influence up, and then how do you think more broadly about what are the impacts to the business and what are the things that could hurt us from generating revenue?"

Rushing: "If you are not already aligned to the business, you're late to the party. Where we are today, security should already be aligned and now be a business enabler."

Market Trend: What are the most cluttered security product spaces?

After walking the RSA conference floor and getting inundated on a daily basis with security product pitches, CISOs made it clear there is an increasing amount of clutter in the market. We spoke with CISOs who told us about the 2,500+ security product companies currently in the marketspace, and how some areas stand out as more cluttered than others.

From colorful, fun booth displays, to creative draws to get people to visit their booths, vendors went above and beyond previous years to stand out in the even more crowded space. The time of 'one-upping' the next vendor and investing a tremendous amount of money into marketing and messaging at conferences is ever present.

CISOs we interviewed commented on the increase year-over-year of security companies at the RSA conference (and most other security conferences). For security companies, it is a chance for them to get their product name out there or solidify their place in the market. Newer security companies have a rare opportunity to garner attention and gauge market interest in their offerings.

According to CISOs, the top 4 most crowded product marketspaces are:

1 → **Endpoint**

2 → **CASB**

3 → **IDAM**

4 → **SIEM**

So, when asked what areas are the most cluttered, the majority of CISOs we interviewed gave the above results.

Endpoint remains to be the top most cluttered space. When asking the CISOs why they think this is the case, they believe the need for endpoint protection remains to be a top concern. Threats continue to increase at an accelerated pace and endpoint vendors are utilizing AI and machine learning in order to keep up. Many CISOs believe threats are proliferating too fast for humans to keep up with in real time.

7 out of **10**

CISOs say **Endpoint** is the most cluttered security product marketspace

To clear the clutter and understand what products to invest in, CISOs told us they first identify top players in the space. By doing so, they are able to start with 3-5 leading companies and narrow down from there. They next reach out to their network of security leaders, trusted advisors, and peers. Their networks are prime spaces to discuss others' experiences using specific products and feedback on real use case practice.

Leveraging a network of security peers enables CISOs to speak with trusted, unbiased sources in order to make their own security product investment decisions. They recommend first doing a detailed research on which products match your business and technical requirements. While many CISOs' use cases for purchasing a product may be similar, there are instances where they may not be.

Along with endpoint, CISOs we spoke to said Cloud Access Security Brokers, Identity and Access Management, and SIEM to be the other top crowded spaces.

We hope you enjoyed reading our Q&A with leading CISOs. If you are interested in being featured in future trends-based articles, let us know.

[All statistics, graphs, and results in this article are direct property and analytics of K logix]

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

CHRISTOPHER PORTER
CISO, FANNIE MAE

HEADQUARTERS: Washington DC

EMPLOYEES: 7,200

ANNUAL REVENUE: $23 Billion

In the late 1990s, Christopher Porter visited a friend working in IT at Cisco in Silicon Valley where he had the opportunity to witness innovative IT work first-hand. This experience sparked his interest in the IT field and he went on to work at a law firm specializing in a wide range of technical support. He then took a position at the LSU Health Sciences Center in the early 2000s where a malware incident, SQL Slammer, prompted the organization to place an entire network behind firewalls in a period of a few days. It was through this incident that Porter developed a passion for information security.

Porter continued his career working at an information security consulting firm, where he traveled throughout the U.S. working with clients to provide them baselines of security and help build programs from the ground up. He then landed a formidable, yet rewarding role, working on the Verizon Data Breach Investigations Report (DBIR) for over seven years. Porter comments, "My work on the DBIR opened my eyes to a lot of different issues in this industry. I saw there was a clear lack of data across the industry when it came to security incidents. I was reading thousands of incident reports about how data breaches were happening and it was my job to break them down and analyze what happened."

"The entire organization is passionate about improving the security program. When I started, I was really pleased with the support from the top to bottom."

- CHRISTOPHER PORTER

TRANSITIONING INTO CISO

Porter decided to move over to operations and work in a role to protect an actual organization. Before becoming CISO of Fannie Mae, the leading source of financing for mortgage lenders, his first role was that of their Deputy CISO. He says, "What I really like about Fannie Mae are the people and the mission of the organization. Those are intertwined with one another. One aspect of the mission is that we are ultimately putting people in houses. When we create liquidity in the market, we make it possible for people to buy homes."

GROWING AND LEARNING

Porter emphasizes the value of having mentors throughout your career, something he has had the opportunity of experiencing. He says, “I have several mentors I talk to regularly, some I’ve worked with directly as my bosses in the past. It’s a way I can continuously improve. My mentors’ expertise and insight are invaluable to helping my career.”

He continues, “The entire organization is passionate about improving the security program. When I started, I was really pleased with the support from the top to bottom. It also coincided with a transformation in the overall strategy. Fannie Mae wanted to focus on delivering a strong customer experience, and part of that means always being available for our customers. Developing a strong cyber resiliency was, and still is, a huge component of that.”

Mission and culture were key components of Porter’s interview process and he recommends understanding these facets of a business by asking how a company generates profits and the level of support it provides for information security. Porter explains, “You must ask business-oriented questions to understand how the company makes money and what kind of data they are protecting. It is also really important to understand the culture and what kind of program you will be coming into.”

GET RIGHT, GET SMALL, SEE BIG

Coming in as a Deputy CISO enabled Porter to establish a strong relationship with the previous CISO. Porter worked diligently alongside the CISO to define and create an information security strategy. He says, “Our mission was to get right, get small and see big. This meant to fix things in the environment that needed fixing, shrink the attack surface and get better insight into the business, technology and network so we can be more proactive. We then had to build the right team and get the right people in the organization to lead. We were in build mode at that time.” After the prior CISO left, Porter took on his role and now carries on this mission of building a world-class information security program.

Porter describes culture and education as key components of a strong information security program. He comments, “Our CEO talks about cyber risk as a top concern in our town hall meetings. There’s a clear message from the top down that security is important to the organization.” This support includes board meetings where security dominates a large portion of the conversation. Porter says, “Our board has a packed agenda, but security is something they have a great interest in covering. They always want to understand more about what we are doing.”

Porter works hard to be direct and transparent with his senior leadership. He explains, “They want to understand the risk to the organization. Often, there will be one or two technologists on the board who are good allies. If you keep it simple and provide strong metaphors to explain complex security issues, you will send a direct, clear message to them.”

KEY POINTS FROM PORTER’S PHILOSOPHY

Porter believes CISOs should focus on innovation, collecting data and aligning to the business as they continue to positively mature in their roles.

Innovation. “Innovation is one of the most important aspects of their role that CISOs can engage in. We have to start doing things differently and start looking at our security problems in different ways. Some of that is leveraging more early stage venture-backed technologies. There is a lot of funding going into cyber security in order to solve problems and there are some really good partners we can work with.”

Collecting data. “It is important to measure findings across the organization and the security program, and baseline that activity to really drive data-driven decision making. We can’t make decisions based on gut, and it is easier to influence people across the organization when you have data as support. When you can show how something actually helped save money or prevent fraud, you gain more backing. If you know your audience well, you will know what kind of metrics to present to them. It’s all about using your best judgement.”

Aligning with the business. “It is important to understand what your business does so you know what to protect. I can’t stress that enough. When I was at Verizon, each report had a table focusing on which threats impact which industries. If you know your organization, you can increase your understanding of the threat profile you are facing. If you understand your business and the threats that affect your business and industry, it will help guide the decisions you need to make so your program runs strategically.”

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

ANDREW BJERKEN
GLOBAL CISO AND CPO, CATALINA

HEADQUARTERS: St. Petersburg, Florida

EMPLOYEES: 1,300+

ANNUAL REVENUE: $640 Million

Currently the Global CISO and CPO of Catalina, a big data company focusing on shopper history, Andrew Bjerken possess a strikingly unique background. Starting his career in the Air Force as an electronic warfare officer and then transitioning to the red team, Bjerken tested physical and cyber security controls across a multitude of bases and systems. Along with his team, they spent their time trying to break into networks and facilities to exfiltrate data. They would then brief commanders on what kind of unclassified/classified information they were able to either exfiltrate or piece together. This work exemplified Bjerken's first plays into information security and sparked his interest in replicating his Air Force work in his transition to the corporate world.

> "Be yourself, be humble, be approachable, and be credible in your job. If you can be those things, you're off to a good start. When you don't know the answer, don't try to bluff your way through it, because no one expects you to know everything. Be confident in what you do know."
>
> - ANDREW BJERKEN

HONEST, STRATEGIC CONVERSATIONS WITH SENIOR LEADERSHIP

Holding previous CISO and Privacy roles in a variety of verticals strongly prepared Bjerken for making an impact and embedding strategic alignment at Catalina. Bjerken reports into the Chief Legal Officer who reports directly to the CEO, enabling him access and a strong working relationship with senior leadership and the board. He comments, "You have to be cognizant of your audience and what's important to them. You must make sure you deliver on your promises and you need to be careful that you don't falter early on, you can't misspeak or oversell, it's going to leave a lasting impact. You must establish your expertise early on and establish a trusted partner relationship."

Honesty ranks high on Bjerken's approach to communication with senior leadership. He is consistently open and honest about where challenges exist within his information security and privacy program and what his needs are to fulfill business requirements. Most importantly, he clearly articulates his strategic roadmap to show where they are and where they need to be so allocated budget does not get wasted.

When providing advice to other CISOs preparing for their board presentations, Bjerken explains, “Talk to other folks who have been in front of the board, so you know the audience and what’s important to them. Be yourself, be humble, be approachable, and be credible in your job. If you can be those things, you’re off to a good start. When you don’t know the answer, don’t try to bluff your way through it, because no one expects you to know everything. Be confident in what you do know.”

REPORTING ON RISK METRICS

Bjerken does not subscribe to in-depth technical details and statistics when reporting to senior leadership on metrics. He comments, “For me, the most important metric is the risk profile. What is the risk of the organization and how are we tracking it? I show where our current level of risk is, broken down into five different categories of risk, then I show key things we need to do in terms of reducing risk. This allows for informed decisions to be made based on risk appetite. When married up to my overall strategic plan with project goals, one can easily see where the weight of my team’s efforts are focused and in which risk category we are trying to affect. If they see a discrepancy later or wish to reprioritize based on changes to business goals, then we can adjust the roadmap.”

He continues, “The board and senior executives feel more comfortable when I have a holistic plan in place versus saying something off-hand like I need a tool ‘X’. When they can see why you need a SIEM, how it fits into the strategic plan, how it reduces risk, and what the anticipated ROI is, they have a greater sense of comfort in terms of expending those dollars. The ROI is often explained in laymen terms such as the tool ‘X’ gives me greater fidelity, which means the team can identify a threat quicker and we can mitigate them faster. The downtime for the business is going to be less as a result. Knowing our revenue generating lines of business and the associated business impact assessments allows me to give an educated answer associated with dollars, if our system goes down, that could be ‘$X’ Amount an hour depending on the system but tool ‘X’ reduced that estimated downtime. Always driving the discussion back to the business requirements and goals. Bottomline, making that correlation so they can see the risk in true dollars has really helped me.”

COMMUNICATION, STRATEGY, AND PASSION

According to Bjerken, key traits of success for CISOs include effective communication, a strategic approach, and being passionate.

Communication. “You have to translate between technical and non-technical. You’ve got to take the non-technical and tie it into business requirements. Today’s CISO must speak business language more so than technical language, in many cases. Business language is PNL (Profit and Loss) and Risk. What is the risk to operations, to revenue, how much is this going to cost, what is the ROI, all of those things. We can’t just talk threat, threat, threat.”

Strategy. “We must be strategic in thinking, but we must be able to tactically execute on our ideas. I’m a strategic thinker in terms of having a roadmap and vision that enables the business, but when it comes to doing the work, I’m big on having goals that focus on the tactical tasks to ensure we accomplish the strategic objective. Diversity is key in any capability, as a CISO, I want to surround myself with a diverse group of people that are smart and take pride in their work. However, that diversity won’t help the company if we’re not willing to listen to them. That’s how we grow. You have to listen to all voices. I don’t like the doom and gloom messages that I hear sometimes, everyone is aware of the doom but a CISOs job is to identify the potential doom and determine the best courses of action to avoid or mitigate the potential negative impacts. CISOs must be willing to make the decision. Regardless of how much data you have, if you don’t move forward and choose a direction, you will fail.”

Passion. “One of the things that makes a good CISO is truly caring about the company they’re with and really wanting to make a difference. I love my job, and I love what I do, therefore I want my team to feel the same way because when they do, they’re much happier which means they work harder and inevitably they want to make a difference. When things go wrong and they have to stay late, they’re not doing it necessarily because they have to, but because they want to; they feel a sense of responsibility in the success of security and privacy. If you can encourage and foster that type of environment in your organization chances are you’ll have a high functioning team which increases your chances of success in your role. At the end of the day, without your team being successful, a CISO won’t be successful.”

GDPR FOCUS

“Shopper info from retailers are sent to us and we provide coupons back using real time analytics. We have lots of data from around the global to include the EU. As both the Global CISO and CPO, most of my time lately has been consumed with GDPR and ensuring security and privacy are aligned and of course that we’re compliant by May 25th, 2018. We were building it from the ground up and are pleased with the final program. For any company or organization, the fines associated with GDPR are large enough to make your board and CEO, sit up and pay attention and want to know what’s going on.”

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

JUNE 2018

K logix

WWW.KLOGIXSECURITY.COM
888.731.2314