FEATS OF STRENGTH

A BUSINESS-FOCUSED CYBERSECURITY MAGAZINE

COMBATTING THREATS

Interviews in this issue:

MARCH 2022
KLOGIXSECURITY.COM
617.860.6485

K logix

FEATS OF STRENGTH

COMBATTING THREATS

MARCH 2022

FROM THE Editor

Dear Readers,

Our industry continues to experience significant increases in threats like ransomware, and with geopolitical tensions escalating, the entire cyber community is constantly anticipating potential cyber attacks. At risk is the safety of employees, customers, and data. Security leaders, regardless of company size or industry, are tasked with ensuring their entire organization from interns to C-level executives, possess diligent security awareness. And safeguards are only as strong as your weakest links, often your people, partners, and third parties.

- So, how do security leaders avoid using fear when educating their workforce and executives on potential dangers? By leading with a calm, yet strategic approach. Most CISOs dedicate significant time and resources to reducing risk by:
- Instilling a robust security awareness program, blending real world news and how it may impact their organization, with recent trends the security team finds in their daily work.
- Engaging in frequent exercises and educational sessions to build and test their employee's security aptitude. Avoiding fear and leading with business language that resonates with all employees.
- Ensuring they have strong security hygiene to proactively address threats and avoid reacting only after they are impacted. This includes due diligence with partners and any third parties.

In this issue of the magazine, hear from CISOs about how they address threats, including best practices and suggestions to stay proactive. You'll also read about trending threats from K logix's penetration testing team who help keep customers safe on a daily basis. We hope you enjoy reading and would love to hear your feedback.

Kevin West

CEO, K logix

Magazine Contributors:

Katie Haug

VP Marketing, K logix

Kevin West

CEO, K logix

Kevin Pouche

COO, K logix

Marcela Lima

Marketing Manager, K logix

About K logix: Cybersecurity Advisory and Consulting Services

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

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

www.klogixsecurity.com/feats-of-strength

Marketing@klogixsecurity.com

RAVI THATAVARTHY

VP & CISO
RITE AID

HEADQUARTERS: Camp Hill, PA

EMPLOYEES: 51,000+

REVENUE: $21.9 Billion

Ravi Thatavarthy is a seasoned information security professional with over twenty years of experience. He began his career in Senior Architect roles, working in many verticals including healthcare and banking. He took on his first leadership role as Information Security Officer at Kronos, where he was responsible for establishing a security strategy and executing on the security and regulatory compliance programs from the ground-up. He had an opportunity to develop a clear strategic plan that aligned with industry standard frameworks to define the future security-state based on regulatory and environmental security trends. He also built a dedicated team for regulatory compliance.

Ravi then moved on as CISO at Haemonetics, where he was responsible for the successful delivery of enterprise and product security, policy, risk management and compliance programs to 34 countries globally. During his tenure there, he transformed and uplifted the security program to prevent next generation threats while focusing on governance, security architecture and business alignment with multi-year roadmaps.

> *“The mission of Rite Aid was very attractive to me, it is focused on providing trusted and accessible care that helps customer achieve Whole Health.”*

His next role was the CISO for iRobot, an opportunity that allowed him to establish the vision, strategy and successful delivery of a global information security program. This included a heavy focus on connected products and customer privacy.

After working at iRobot for four years, Ravi began working at BJ’s Wholesale Club as their VP and CISO. While at BJ’s Ravi helped with digital transformation by focusing on business value and customer delight. He held this role for three years before taking on his most recent position.

Currently, Ravi is the VP and CISO at Rite Aid, a role he has had for seven months. Ravi comments, “I went from iRobot, a smaller public company to BJ’s, a public retail organization and now I am working at Rite Aid, an organization that delivers healthcare services and retail products to millions of Americans each day. The mission of Rite Aid was very attractive to me, it is focused on providing trusted and accessible care that helps customer achieve Whole Health. They empower pharmacists to engage with more customers and also are good neighbors in the community which drives commitment and passion. We have more than 2,400 retail pharmacies locations across 17 states.”

Ravi’s responsibilities are those of a typical CISO, with a heavy focus on protecting customer and employee data. He also oversees any compliance-driven security requirements to ensure all controls are in place.

FOCUSING ON COMBATTING THREATS

Ravi says historically security was focused on not getting breached, however it has shifted recently with a predominant focus on preventing ransomware attacks. He explains, “Ransomware is a significant focus not just for me, but for every CISO because of the level of damage it can cause. Five to ten years ago we were very focused on protecting our data and network so we would not get breached. We didn’t want anyone to get inside, steal our data, and take it with them. But in recent years, ransomware has proven to cause significant damage that can cost companies a lot of money because they can take down your entire network in a matter of minutes or even seconds.”

Another area of focus for the security industry is more proactive security monitoring, something Ravi believes has continued to evolve in response to ransomware. Ravi explains, “When focusing on ransomware you wanted to make sure that you stay ahead of the game rather than noticing it after the fact. We are now at a place where we are engaging in blue, red, and purple team exercises to continually test instead of waiting until an annual penetration test to happen. Also, by testing on a regular basis, you can constantly check to see if your defenses are good enough. I believe threat hunting has evolved and will continue to do so.”

ARTICULATING RISK WITH STRONG DATA POINTS

Ravi suggests avoiding scare tactics when discussing budget with both business leaders and the board, something that might demonstrate immaturity and hinder security initiatives. He believes in clearly articulating risk while leveraging data points to back-up any key goals. He explains, “An example would be discussing the value of a multi-factor authentication (MFA) solution with the board. If you have an MFA installed, you should know how many credential stuffing attacks can be reduced. In board meetings, you should bring up those data points when talking and let them know how you were able to stop attacks. Implementation technology doesn’t really mean anything to them, but how many negative things you avoided shows progress and provides measurement.”

For budget discussions related to adding headcount, Ravi suggests looking at any available industry data that provides overviews on how many security employees are required in relation to the size of an organization. He comments, “There are metrics available through multiple research firms. For example it may say that if you are a $100 million company with 10,000 employees, your security team should be 25 people. These types of data metrics are important because you can also see if you need to outsource any responsibilities through contractors or consultants. It’s important to look at your security program mapped to the NIST CSF Framework to see where alignment and gaps exist. You can then see the minimum number of team members needed to ensure you are covering critical functions.”

> *“...by testing on a regular basis, you can constantly check to see if your defenses are good enough. I believe threat hunting has evolved and will continue to do so.”*

HIRING PASSIONATE LEADERS

The most important thing Ravi looks for in security team members is passion. He explains, “Someone’s ability to succeed is often based on if they are flexible and if they are a team player. I don’t always look at technical skills, I instead look at their attitude, if they are interested in learning, and if they are passionate about their work. These types of people change the environment for me. Technical skills can be taught, but people skills combined with high energy and high passion are most important.”

Ravi also encourages his team members to attend conferences, whether in-person or virtual, as well as achieve relevant certifications. He believes in matching tools and technology to an individual’s responsibilities to make sure their career goals are aligned to help them advance.

To grow as a leader, Ravi attends conferences and sees a lot of value learning about niche topics. He says, “I like attending conferences focused on specific topics with groups of like-minded CISOs.”

He continues, “Security is getting more and more challenging, and it can be difficult to keep up, but I love the work that I do. It is not for the faint of heart, it is for people who are ready for a challenge. It doesn’t get easier, but the field of security will always be interesting.”

TESTER TALK:
RECENT TRENDS IN COMBATTING THREATS

Penetration testers share thoughts based on their everyday work

Security programs are tasked with the on-going mission of keeping pace and staying ahead of cyber threats, often one of their biggest challenges. From our many CISO interviews (including those in this issue of the magazine), we hear that threats are increasing in complexity and adversaries are getting smarter, resulting in a greater focus on proactively protecting organizations.

There are fundamental security actions, often a keen balance of defensive, detection and responsive measures, to stay ahead of threats. Security leaders must invoke a strong awareness program to ensure all members of an organizations share the core common goal of keeping their employees, customers and data safe.

To stay ahead, regular security testing should be a common practice at all organizations, each requiring a different approach, tailored to their particular business and technical conditions. Testing should be done proactively before the impact of a threat, to avoid costly and disruptive outcomes.

We asked members of K logix's highly skilled penetration testing team their thoughts on the latest cyber threats. Our goal was to better understand trends they encounter in their daily work helping customers bolster protective measures. Here's what they had to say:

Bobby Rauch

Penetration Tester, K logix

“Overseas conflict is highlighting the potential dangers of cyber attacks and cyber warfare. Threat actors are becoming increasingly well-trained and skilled, and cyber attacks are becoming more complex as a result. As a team, we spend time tracking the latest tools, tactics, and procedures used in real world cyber attacks. Armed with this knowledge, we participate in industry leading trainings, conferences, and security research projects. This allows us to emulate real world threat actors for our clients, helping them secure their network infrastructure and applications and improve their overall security posture.”

David Lane

Penetration Tester, K logix

“The human factor in security does not only relate to phishing or client side attacks. Tools and methods used by systems administrators for their convenience or task automation can be leveraged by an attacker for malicious ends. Plaintext passwords can sometimes be found inside administrative scripts, configuration files, or in shell command history. Cron jobs, Sudo or SUID misconfigurations, and lax file permissions can create a dangerous vector for privilege escalation. In these cases, the system administrator becomes a hacker's best friend.”

Jake Wnuk

Penetration Tester, K logix

“Some of the biggest threats to organizations are often the ones that get overlooked or have drifted into collective acceptance. Security can often feel like a roadblock for organizations to stay agile and focused, but not maintaining a good security program can introduce systemic risk. Issues like shared passwords and shared development infrastructure can give attackers mobility within an environment in the event of a compromise. Suppose an attacker can compromise one set of credentials from network traffic, hardcoded files such as configuration files, knowledge bases, team wikis, or social engineering. In that case, their access can quickly spiral out of control, significantly if a user has elevated permissions like a local administrator. This issue extends into systems that may not be fully hardened against attacks, such as network relaying and poisoning. An attacker can target an insecure configuration on one machine to gain access to several potentially. Good security is all about maintaining safe practices and trusting controls are in place but verifying their effectiveness with routine checks.”

George Gal

President, Security Testing Services K logix

“Threats facing all organizations are constantly evolving, as is prioritization of security due-diligence and focus needed to ensure security controls protect organizations' data, intellectual property, and other assets. SaaS vendors are increasingly being required to perform penetration testing of their applications and cloud infrastructure as part of their customer commitments and cyber insurance coverages. Product organizations are also facing increasing pressure to ensure penetration testing coverage evolves to includes the full product stack. Organizations of all sizes are being targeted daily by threat actors hoping to capitalize on weak patch management, deployment configuration, or human awareness to launch ransomware attacks. Automated testing that some organizations perform to identify cyber threats may help to uncover low hanging fruit, but over time testing must evolve and progress to include manual penetration testing which incorporates threat models of the target systems and environments and techniques and tactics used by adversaries. K logix has the skills and expertise to raise the security bar and ensure customers stay ahead of the ever-changing security landscape.”

Jeff Farrington

Penetration Tester, K logix

“Unfortunately, in today's environment everyone is a potential target for a cyber attack. Over the last year, I have seen veterinarians, small energy companies and other businesses affected by ransomware. It's important to recognize an attacker may not want your data, but they also know you may need it. Once companies understand this they are challenged with where to start and how to keep up with the evolving landscape. Don't try to go it alone. Develop a network of resources that can help you understand the latest threats and develop a strategy to prioritize and protect your data. As part of team of security consultants at K logix, we spend every day doing these kinds of things to help protect our customers. We focus on areas such as patch management, segmentation, data protection, misconfigurations and endpoint security that often allow us to move throughout an organization during a penetration test.”

To learn more visit
www.klogixsecurity.com/security-testing-services

STEPHANIE FRANKLIN-THOMAS

SVP & CISO
ABM Industries

HEADQUARTERS: New York, NY

EMPLOYEES: 100,000+

REVENUE: $6 Billion

Stephanie Franklin-Thomas' career in IT and security spans over 25 years, garnering her keen business and technical skills to strategically mature security programs and continually protect organizations. She leads her teams with a focus on open and authentic communication, creating collaborative environments poised for success.

Stephanie does not have a traditional technologist background and did not initially set out to work in IT or cybersecurity. She says, "I'm a product of being involved in a number of different engagements and activities throughout my career that led me down the cybersecurity career path."

Right out of college, Stephanie joined a large oil and gas company as part of their customer service operations center, and one of her first assignments was to work on a large enterprise resource planning (ERP) implementation. This was her introduction into the world of technology, and she quickly recognized how much she enjoyed and excelled at this type of work.

After moving into more IT-focused roles, she found herself working at one of the Big Four accounting firms at the same time as Sarbanes-Oxley was gaining traction. This enabled her to lean into compliance-focused cybersecurity functions assisting organizations managing through the new reporting regulations.

For the past year, Stephanie has worked as the SVP and CISO at ABM Industries, with a focus on driving IT strategy and transformation, building a strong security culture, and delivering impactful security solutions.

TRANSITIONING INTO LEADERSHIP ROLES

As Stephanie progressed in her career, she was able to move into cybersecurity leadership roles, by leveraging her strong business background to achieve success. She explains, "I came from an environment where I was working in the business. I became the liaison between the business and technology teams, conversing with technical people about their work and then turning around and translating it into business speak for our leaders. Having the ability to essentially speak two different languages is a strength. Thus you are quickly elevated into those roles that are more leadership-facing to create understanding."

After spending the majority of her career in oil and gas, she was excited to transition to ABM Industries where she would have exposure to different businesses which look at cybersecurity in various ways. She comments, "ABM was interesting to me because it has five industry groups and the approach that could be taken to support these areas. I always use the analogy when I talk to leaders that we are trying to protect what's important to us – so we don't want to build a million-dollar fence to protect a $20 horse. In cybersecurity you want to understand what is most important or what is most valuable. Once those variables have been identified, the focus becomes clearer on what goes into building your cybersecurity program and addressing the needs of the organization. At ABM, the real assets are the people, unlike manufacturing organizations where there is a keen focus on the products. Our people are the assets we are protecting. This was an opportunity and an approach to a very different aspect from my previous roles."

BECOMING A BUSINESS ALLY

Stephanie believes successful and strategic CISOs should always strive to have a seat at the table with business. She says there are still many organizations who view cybersecurity as the police, she analogizes – when you need them you call them and they come and everyone is happy, but when they pull you over for speeding, you don't want to see them. She continues, "At times, the business sees cybersecurity through that lens, thus the teams are not invited to the table. It is important, whether it is a transformation effort or otherwise, that cybersecurity has a seat at the table and a voice when projects are in development. You do not want to get so far down the path and implement something that is not secure, or it is going to get held up to ensure necessary security features are enforced to protect resources."

At ABM, cybersecurity has a seat at the table to truly understand what is happening in the organization and to provide guidance for any innovative projects, according to Stephanie. She comments, "It goes back to creating rapport with the business. Establishing that connection shows them what your teams have to offer, and leaders have the ability to bounce ideas off you before they move forward with projects. With the recent launch of ELEVATE, our long-term strategic priorities, we know our focus will be on elevating the client and team member experiences, and ABM's use of technology and data. The collaborative efforts between the business and technology teams will strengthen our efforts around transformation. Our unified goal is for ABM to continue being a leading provider for integrated facility services in the near-term and future, and cybersecurity will be a strong ally for our organization and clients."

When presenting cybersecurity updates and key data to boards, Stephanie tailors her presentations to match her audience. Her extensive experience presenting to boards and executives enables her to ensure meetings are productive. She explains, "Leaders receive information in different ways. The key to success is getting to know your board or your audiences and approaching them with the content that resonates best with them. Some leaders may be most interested in the narrative, others may want to focus on data visualization and some executives may just want to dialogue with you about what we are currently facing. The tried-and-true way to have effective communication is by adapting your message as needed."

> *"The key to success is getting to know your board or your audiences and approaching them with the content that resonates best with them."*

PEOPLE: TOP ASSET, TOP THREAT

Stephanie says an organization's greatest asset is their people, which may also be their biggest threat. She believes it is the way in which people interact with their environment that poses significant threats. She explains, "Most of your security vulnerabilities happen because someone did or did not do something, it all drives back to an individual."

When asked about the balance of people, process, and technology in addressing threats, Stephanie says, "All three are equally important, as you must have the policy and/or standard in place, educate and train employees on best practices and implement the technology to support. Your underlying automation is the guardrail, so processes are enforced, and no workarounds are available."

CELEBRATING WOMEN AND DIVERSITY IN CYBERSECURITY

"I recently attended a CISO meeting and at one point I looked around at the attendees and thought to myself, 'WOW, every person in the meeting is a woman.' I was so accustomed to being the only one in the room, either the only woman or the only minority, that I had a moment of amazement. To see all these different women working in the cybersecurity world, I'm impressed with how far the industry has come in recent years and in awe of the diversity I see within my own team," says Stephanie.

Women now account for 25% of the cybersecurity workforce (according to ISC2), but Stephanie believes more could be done. She recommends that leaders striving to develop more diverse teams should consider creating an environment where all members at the table have unique differences. For potential talent looking to join an organization, being able to identify with someone who resembles them could be a factor in their decision to accept an offer. This also extends to how companies engage with students or young professionals, especially women and minorities, about opportunities in the technology space. This awareness could open the doors for someone who never knew this could be a path to a successful career. Stephanie hopes more women and minorities will step into CISO and other IT leadership roles in the future.

CRIS EWELL

Chief Security and Privacy Officer
NRC Health

HEADQUARTERS: Lincoln, NE

EMPLOYEES: 500+

REVENUE: $133 Million

Cris Ewell had an eclectic background leading up to his career in cybersecurity. He dropped out of college and bought a restaurant, where he learned key customer service skills, before deciding to become a paramedic. He then became a director of paramedic service, responsible for protecting patient data and addressing access control, which spurred him to go back to school to finish his undergraduate degree in information technology. After achieving his degree, Cris continued his education and completed his graduate and Ph.D. degrees in information technology and systems with a concentration in information security.

Cris has over 25 years of experience in information security and spent over 19 years in CISO or equivalent roles. He held CISO positions at PEMCO Corporation, Seattle Children's Hospital, and University of Washington Medicine before joining NRC Health as their Chief Security and Privacy Officer. He has worked as an Adjunct Professor specializing in risk management and operational controls courses throughout his career. Currently, he teaches two to three classes per year and sits as an advisor to graduate students at City University of Seattle.

He says, "I love being a CISO. I love leading organizations and seeing how I can help them navigate the field of risk and threats. But I also know that I need to give back to the community and I need to train the people who will take over my position someday. It's great to see students learn. It's really exciting to see people I've had a small part in educating over the last 15 years, prosper and blossom in their positions."

RISK MANAGEMENT

When evaluating security programs, Cris always starts with understanding the risks and threats faced by the organization, something that should always be grounded in an understanding of how the adversary thinks. He explains, "It is important to know the difference between opportunistic attacks versus targeted attacks, and all of the controls in place for the organization, from your security operations to your development operations, to the systems teams. Then put those all things together with the current climate and the current resources you have available."

Cris believes in order for security leadership to appropriately address threats, they must have strong knowledge around risk management and quantitative risk analysis. He says, "It is important for CISOs to really understand quantitative risk analysis, so an actual risk and financial number on the level of risk for the organization. And that's the language of business that really resonates with CFOs and other executives. It also resonates with cyber liability insurance companies that may be taking a look at your organization's real financial risk. It's about understanding the whole insurance spectrum, understanding the real difference between qualitative and quantitative, you can't just put numbers on colors and call it quantitative."

Another focus area for reducing risk is situational awareness in relation to threat intelligence and understanding the adversary. Having a level of threat awareness that goes beyond what is happening locally, ensures CISOs know what is going on in the rest of the world. Cris believes situational awareness is a minimum requirement for CISOs to gain holistic risk insight and ensure they are proactively prepared.

He continues, "I spent 10 years researching and understanding risk management and it really has helped me deliver something that our business leaders and boards can understand. I think that's still a failing in the information security education department, in getting CISOs to understand everything about proactive risk management, especially with data centers, third parties, and risk assessments. How do you understand all of those intricacies to be able to come up with that risk management report?"

DATA VISUALIZATION

Cris says he is passionate about data visualization, especially when it comes to presenting to boards and executive audiences. In meetings, he provides a mixture of strategy documents indicating the overall strategy, key threat areas, and projects they are working on to mitigate risk and threats. He also includes visuals for an executive dashboard, often leveraging red, yellow and green indicators.

He explains, "I look at both the overall risk of the organization, and a view of what's the information security overall program risk. When I look at the program risk, it really is answering the question, is the organization resilient enough to be able to respond to the current threats and risks? It looks at all the different security domains and being able to say that you are prepared. It's measuring your ability and your maturity to information security controls. Then I look at attack vectors and our organizational asset risks. I always throw in compliance if you're an organization that has compliance, healthcare definitely is. I also include some very high-level performance measures. Those things make up my executive-level dashboard that I typically give to the board of directors so they understand the different components. Hopefully that will spur conversations about the information security program and risk from there."

CHALLENGES

For Cris, the most pressing challenges CISOs currently face are around data, legacy systems, threats, competing priorities, and human error.

Data: "The challenge comes in knowing all the areas that data is kept and which controls are in place. Most of us do really well with primary, secondary, and maybe even tertiary data sets. If you've ever done research and been part of academic medicine, academic institutions, or research institutions, there ends up being many copies of data sets and they can be difficult to identify. Whether it is limited datasets, healthcare-related, restricted or public data, or if you have PII for a financial institution, understanding where all that data is and understanding what controls are in place is essential."

Legacy systems: "A fact of being a CISO in 2022 is you have to have a plan to support the legacy systems still required by the business. These systems may not have the latest software version, latest patches, or the latest code development. These systems may not be at that highest level across the entire spectrum of things you have to protect, but you still need to provide information security controls that help to reduce the risk of unauthorized access or use."

Threats: "There is a rapidly expanding spectrum of threats to our systems networks and data assets. It is enormous, we have zero days that come out, we have code or exploits that are stolen or purchased that are now utilized against organizations. As CISOs, we need to have security practices that are robust enough to help mitigate these threats and understand – how do I continue to keep ahead of the threats?"

Competing priorities: "You can't fix a hundred percent of all your risk, it's not possible. We need to understand all the threats, vulnerabilities, and risks to the assets and data in an organization. The question then becomes how we prioritize the remediation with the limitation of the resources that we have underneath the control of the organization."

Human error: "How do we help our users understand the real threat? How do we help the user understand the world that we live in and, for example, where we have to question every single email that we receive or putting a pause in our actions before we post a change in a system. Simple actions by our users can decrease the risk to the organization - such as understanding their responsibility in protecting the data, not clicking on that link, not installing software, or not accessing our data without a VPN. Education and awareness is a very important element of our security controls and should not be underestimated in its importance to the overall program."

DIVERSITY

"Having a diverse team that has different life experiences is critical to your success. I don't want a team that just says 'yes', I want them to challenge my decisions when appropriate. If you have an incident or critical incident that is time critical, it might not be the time to challenge. It is the right time when you're talking about the right technology to use or strategies on how to implement zero trust. That's where having those different experiences is so important for the team and something that I have promoted over the last fifteen years. Where I am today, I've hired almost my entire team, and we have a very diverse team. There's just so much to learn at all levels from everyone's perspective. I believe that the diversity and ability to work together is a core requirement for what makes a really great team."

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM

COMBATTING THREATS

FEATS OF STRENGTH
MARCH 2022