FEATS OF STRENGTH

A Business-Focused Cybersecurity Magazine

IN THIS ISSUE:

SHAWN KEELEY, BCBS OF RI

PATRICIA VOIGHT, WEBSTER BANK

YASHVIER KOSARAJU, SENDBIRD

Making Smart Investments in the Overwhelming Cybersecurity Technology Marketspace

MARCH 2025

IIIK logix

Cybersecurity Investments

Making Smart Decisions in Overwhelming Marketspaces

TABLE OF CONTENTS

03 **Letter**
From Katie Haug, Editor

04 **Profile: Patricia Voight**
CISO, Webster Bank

06 **Profile: Shawn Keeley**
Manager of Information Assurance, BCBS of RI

08 **Profile: Yashvier Kosaraju**
CISO, Sendbird

10 **Article: How to Make Smart Investments**
By Katie Haug

March 2025

FROM THE *Editor*

Dear Readers,

We spoke with three fantastic examples of cybersecurity visionaries and leaders. They all shared about their experiences and how they grew in their careers to reach their current roles and responsibilities. We also asked them all about how they make smart investments in cybersecurity technology.

The theme of this issue and the article included are around the cluttered, confusing and noisy cyber marketspace. While it may be challenging to navigate, most leaders have a process they follow, some type of compass to guide them on their journey. With more noise being created every day, it is important for them to ensure they are thoughtful and business focused in their decisions.

Please enjoy reading this issue of the magazine, we are proud to have included these thought leaders and hope you learn from their stories.

Feats of Strength Editor
VP, Marketing, K logix

Magazine Contributors

Katie Haug - Editor
VP Marketing, K logix

Kevin West - Editor
CEO, K logix

Emily Graumann - Graphics
Marketing and Design Specialist, K logix

About K logix

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

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

PROFILES IN *Confidence*

SHAWN KEELEY

MANAGER OF INFORMATION ASSURANCE
BLUE CROSS BLUE SHIELD OF RI

HEADQUARTERS: Providence, RI

EMPLOYEES: 1,100

After graduating law school, Shawn Keeley was applying to legal and technology sector positions because he found both to be fascinating areas of work. He also had his Masters in Cybersecurity and was looking to marry his two focus areas. By chance, he had an opportunity to join Blue Cross Blue Shield of Rhode Island in an interim role as assistant privacy officer.

He explains, "I learned a lot in the interim role and when that position was ending, I stayed by moving into a different department, starting at an associate level on the information security team. I started with leading project management and then took over the architecture of our cloud security as we were migrating to the cloud. Then it really snowballed from there, I had the opportunity to take on governance, risk, and compliance as a program while doing project management and cloud security. And it really opened me up to learning everything about the organization, how the business worked, how healthcare worked, and how everything works behind the scenes."

Shawn then transitioned into his first managerial role, taking on manager of information assurance under the information security program. Shawn says he intertwines his legal background on a daily basis, and he feels the overlap between the two has positioned him well as he moves up in his career as a second year manager.

RESILIENCY, THIRD PARTY RISK, AND ARTIFICIAL INTELLIGENCE

Shawn's responsibilities include threat intelligence, enhanced vendor oversight, governance risk and compliance, security project management, training and awareness, privileged access management review, and the artificial intelligence product risk management process.

He explains, "There's a lot of different areas underneath me. We are part of the Blue Cross Association as a licensed entity and our big focus for the year is around resiliency. How do we make this a key priority, not only in our organization, but communicate the risk that is related to a vendor, security process, or configuration to our leadership with regards to resiliency? We make sure to create a baseline appetite and tolerance level for certain situations. It is really important for us to continue to remain resilient and keep the CIA triad, the confidentiality, integrity and availability, of our information while allowing business to take place. That's a very tough area, and it's a probably my number one priority this year."

Along with resiliency, Shawn and his team are focused on their third-party risk management program. They are working diligently to perform deeper dives into the criticality of assessments and creating a risk tier system that is easily digestible by leadership so they can fully grasp the actual risk levels. They are moving from a letter grading system to one that is numerically-risk based to demonstrate exactly where gaps may exist and ensure better remediation efforts.

AI governance is another area of focus as they are a little over a year into their work around AI development and third-party tooling. They brought in an AI product manager that has allowed Shawn time to enhance their security controls and risk awareness around projects and vendors before entering their environment. Shawn also speaks regularly on the topic of AI governance, sharing his knowledge with the community and learning from others and their experiences.

> *"It is really important for us to continue to remain resilient and keep the CIA triad, the confidentiality, integrity and availability, of our information while allowing business to take place."*

"I'm always going to prioritize the needs of my team. I'm going to support their development educationally and help them get to where they want to be career wise. I also make sure that they have a balance of well-being in their life and understand that work is work and when they go home they need to be able to unplug. I encourage them to unwind and enjoy the time they have outside of work to enjoy the fruits of , their labor. That's one portion of it, that's the servant style."

MANAGING TIME AND BANDWIDTH

Similar to many managers working in security programs, one of Shawn's biggest challenges is time management and bandwidth for his team. He states, "I've always told my team that I'd rather have 7 great days of work than 14 days of okay work because I know we can accomplish so much more when they aren't burnt out or they do not feel that they are against the wall. It's a balance to make sure our day-to-day responsibilities can take place along with any security incident we might be working."

SERVANT AND DEMOCRATIC LEADERSHIP

Shawn says he considers his leadership style a combination of servant and democratic. He has relied on great mentors to be a sponge and learn from them, and having those mentors allowed him to put those skills into practice as he moved into a manger role.

He explains, "I'm always going to prioritize the needs of my team. I'm going to support their development educationally and help them get to where they want to be career wise. I also make sure that they have a balance of well-being in their life and understand that work is work and when they go home they need to be able to unplug. I encourage them to unwind and enjoy the time they have outside of work to enjoy the fruits of their labor. That's one portion of it, that's the servant style. "

He continues, "The democratic style allows me to empower them as well. I allow them to participate in the decisions that have either tangible outcomes or output so that they can see the reward at the end, and make sure that they have a seat at the table. I like to refer to that as "listen, evaluate, discuss". I can't make a decision until I've at least heard you out as an individual and understood what your thinking is. What we have found is that that has allowed the associates underneath me to come to me with their problem, and I'll walk them through as far as I can to the end of the rope before I say, hey, jump, and that allows them to make that decision themselves."

INVESTMENTS

"No decisions are made in silos. We include IT in any decision along with different areas of the business to make sure we understand the true impact of any new tools. And at the same time, are we getting the best bang for our buck? One of the major questions we ask as we're going through it is how are we going to balance that? We have a clear picture here of how we want to do it with the mission that we've been given by our organizational leadership. It's just getting the buy in and trying to remain proactive and not reactive in tools. We see that all the time in security. We're one step ahead and then a threat actor becomes one more step ahead. So how do we get to the finish line before they do is always something we're looking at. And also assessing the benefit and cost of certain risks versus the others," says Shawn.

PROFILES IN *Confidence*

PATRICIA VOIGHT

Executive Managing Director, CISO and Technology Risk Management

Webster Bank

HEADQUARTERS: Stamford, CT

EMPLOYEES: 4,400

REVENUE: $2.91 Billion (2024)

Patricia "Patty" Voight represents a true subject matter expert and distinguished leader in cybersecurity and risk. She has spoken at industry conferences across the world, sharing valuable knowledge with the greater security community, and forging relationships across the market. She is an avid reader and contributor to numerous publications and articles, as well as a participant and supporter of many financial services, security, and risk related groups.

Patty began her interest in security during her college years, where she started learning more about the computer industry and the capabilities that came with the internet. She explains, "Back then, the internet provided many opportunities to learn about computers and I participated in some hacking groups. Not necessarily the ones with nefarious intentions, but ones that were just teaching skill sets to other users navigating the environment at the time."

As Patty's interest and education around computer programming and engineering evolved, she entered the workforce on a clear path and her career has significantly grown from there.

Patty has an illustrious background working at organizations such as Citi, Wells Fargo, and EY, in consulting, risk management, and cybersecurity focused roles. She comments, "I came up through the big banks, working in the financial services industry. And I worked at EY, a large consulting firm where I leveraged my skillsets working with different clients across every bit of the industry. I gained extensive experience working across large global, medium-size regional, and startup clients, and consulted and advised on everything across technology risk and cybersecurity. I consider myself a technology risk integrated cybersecurity leader."

SUPPORTING GROWTH AT WEBSTER BANK

Currently, Patty is the Executive Managing Director, CISO and Technology Risk Management at Webster Bank. In her previous consulting roles, Patty had experience with both Webster Bank and Sterling Bank, who recently went through a merger, so she was familiar with the culture and the environment before she joined.

Patty joined Webster Bank because she believed in the vision of the leadership team, and knew it was an opportunity to strategically mature and grow the organization. In her role, Patty is responsible for technology and cyber and information security risk. She explains, "I oversee the cyber and technology risk team that helps mitigate risk across the business as well as the corporate information security team that focuses on resiliency, security, architecture, and engineering. Each of these teams focus on the framework we use across the business. The security operations team runs the day-to-day operations to include threat intelligence and monitoring events and activities in our view."

She continues, "All of these teams work together and it is important for me to understand the crossovers between them to make sure I know how they are operating and aligning back to the business with the value they are providing. Our customers, shareholders, and stakeholders

"I gained extensive experience working across large global, medium-size regional, and startup clients, and consulted and advised on everything across technology risk and cybersecurity."

care about what we are doing, so we make a lot of what we do public, in things like our published cyber fraud index."

MAKING AN IMPACT

One of the most important aspects of Patty's role is to collaborate with the CIO and board to ensure they understand cybersecurity and how her program is shaping the organization. She says, "One of my biggest successes has been my relationship with the board and executive leadership. I make sure I am transparent about our strategy and roadmap, so they are part of our journey. I meet with three different committees and the full board as well. Our board has a hunger for information, and I always show them what we are doing with clear status updates. I'm moving into risk quantification to show them what we are doing from a business perspective, to make sure I'm transparent about how we are bringing value to the corporation from a risk lens."

Patty values that her board enjoys learning about cybersecurity, and she prioritizes sharing, educating and providing them with opportunities to absorb more about what they are doing. This might even include having them sit in on tabletop exercises to gain a first-hand perspective.

Another focus area is growing the team and ensuring she provides a clear path for each member. This means not only focusing on their current roles, but ensuring she helps them achieve any future career goals. She connects with each team member to discuss opportunities both internally and externally that might help them further their ambitions, whether it is gaining a certification or engaging in cross collaboration.

Growing the culture of cybersecurity within the organization and their community is another focus, and something Patty believes to be pivotal in continuing to mature her program. She says, "There are many opportunities for us to share things like cybersecurity awareness training across Webster Bank but also communities that we support."

CYBER THREAT CHALLENGES

The dynamic threat landscape poses challenges for Patty and her program. She states, "We are seeing the increasing sophistication around cyber threats, supply chain vulnerabilities, and regulatory scrutiny, that is requiring a constant amount of vigilance. We are always watching where cyber criminals are evolving, because they're getting faster than traditional defenses. With AI-driven attacks, there are concerns with deep fakes, and with geopolitical cyber risks, we are preparing for what that impact might be."

"We are seeing the increasing sophistication around cyber threats, supply chain vulnerabilities, and regulatory scrutiny, that is requiring a constant amount of vigilance."

She continues, "For firms especially in the financial services industry, there is a large amount of navigation around regulatory complexity and compliance adaptations. That is always high on my list. We are constantly staying ahead of evolving regulations."

MAKING SMART INVESTMENTS

"When making investments it is important to have clear business alignment. Investments are sometimes driven by trends or vendor influence rather than business needs. It's important to base investments on what is truly needed and ensuring those decisions are inline with the business need. It is also important to focus on the long-term sustainability of where the company is going and to make very strategic investments aligned to our investment strategy with strategic objectives, the risk appetite for the firm, and long-term value creation in the forefront," says Patty.

PROFILES IN *Confidence*

YASHVIER KOSARAJU

CISO
SENDBIRD

HEADQUARTERS: San Mateo, CA

EMPLOYEES: 300+

REVENUE: Private Company

Yashvier (Yash) was first interested in cybersecurity when he took a cryptography course in college, getting him excited about problem solving and the impact of hiding information. After completing his undergrad, Yash decided to further his education in security by attaining his Masters in Security Informatics from Johns Hopkins University. This degree positioned him well for a strong career trajectory in the security industry.

Yash began his security career at a consulting firm where he gained deep technical skills, working across various Fortune 500 clients. He then moved to Box for over three years, where he strengthened his skills in application security, penetration testing, vulnerability management, and much more before taking on product security roles at Twilio. While at Twilio, Yash moved from manager, to senior manager to interim director of product and infrastructure security managing a large global organization. He had a unique opportunity to help the organization achieve hyper-growth while maintaining strong security maturity. After almost 4 years at Twilio, he moved to his current organization, Sendbird, as their first CISO, to build out their security program. Sendbird is an omnichannel AI agent and communication solutions platform.

BUILDING A STRONG PROGRAM

As the CISO of Sendbird, Yash oversees all aspects of security, compliance & IT. One of his first responsibilities was to take somewhat disparate areas and fuse them together under the security umbrella to create a cohesive security organization with a unified vision. His goal was to build out the program with transparency and trust and to not only ensure security reflected the business goals but that security became embedded into the corporate culture and eventually make security a key differentiator for the business.

He comments, “It was intimidating but exciting to transition into a CISO role at Sendbird. I always love taking on roles where there is some level of unknown to it. I was tasked with building a team and building on the security foundation they had started to establish. It has been really rewarding to help the company get to where they are now. The team and program have grown from almost nothing and have experienced a lot of maturing.”

To build the program, Yash first established strong communication and working relationships across the business, evangelizing for security while ensuring he aligned with the corporate goals. He says, “While it wasn’t really starting from scratch, all the parts of security were in different areas of the organization, so I brought them together under one organization and ensured they shared one vision. From the start, I had to make sure the company understood that security is here to enable the business and protect Sendbird’s customers. The key was building strong relationships and making sure there was alignment across the board.”

Yash believes building relationships across the business takes time, and is not something you can do in a few hours or a few days, it requires effort to grow on both sides. He is a believer that if you go to someone with a security related ask, it better not be the first time they are seeing or hearing from you. You must ensure that a relationship has already been established. He comments, “Security should never be the hammer. It must be a collaborative approach to

“It has been really rewarding to help the company get to where they are now. The team and program have grown from almost nothing and have experienced a lot of maturing.”

"Security should never be the hammer. It must be a collaborative approach to understand what you can do together and then work towards that common goal. Build over a foundation you've established over time."

understand what you can do together and then work towards that common goal. Build over a foundation you've established over time."

ARTIFICIAL INTELLIGENCE

Artificial intelligence is a primary focus for Yash and his team. They are working to ensure that the organization has the necessary tools and procedures to maintain its pace with the advancements in AI. He remarks, "We have been using AI internally for some time now, and we are diligently continuing to build on that maturity. The most difficult aspect is ensuring that we remain ahead of any knowledge gaps. His team is dedicating time to learning about AI's capabilities, potential legal issues, applications for our organization, and more. We strive to thoroughly understand new technologies before establishing policies and procedures. This presents a significant challenge due to AI's novelty and rapid rate of change. Ultimately, I want to ensure that we can continue to utilize AI responsibly."

To ensure that security remains a facilitator for the business in regard to AI, Yash initiated communication about the value with executives early. He explains, "We obtained the ChatGPT enterprise license early to position us ahead of the curve; we also have Zoom AI & Google Gemini enabled for the company." His team reviews terms and conditions surrounding AI features of SAAS platforms like Zoom, GSuite or Slack to confirm that their data is not being used for training LLMs and that they have control over their data, ensuring that the use of these features maintains the security and privacy standards that Sendbird upholds.

LEADERSHIP STYLE

"I like to hire smart people who want to do the right thing," says Yash when discussing his leadership style and approach to building a strong team. He works with each team member individually, helping them set achievable goals and providing the resources to accomplish whatever goals they have set. He is a big believer in personal growth to make sure each individual on his team is moving in the right direction for their career. He strongly encourages his team to work towards their goals, but does so without micromanagement, he is rather there when they need him and always available.

To continue to grow and learn, Yash reads as many books as he can, some that help him with leadership ideologies or management styles, and some specific to security. Podcasts also help him stay up to date. One of the most important sources of knowledge for Yash is relying on his peer community to bounce ideas off of, including any current challenges or program hurdles. Having a strong network of peers is incredibly valuable.

INVESTING IN NEW TECHNOLOGY

Yash says, "We don't start with the question of asking ourselves what product we need, we start with what capability do we need." Next, we evaluate our current technology stack to ensure that we do not already possess a solution that could address our challenge. Subsequently, we conduct extensive research, examining open-source options versus purchasing enterprise software; this is the classic build-versus-buy evaluation. If we decide to purchase, we must consider whether to procure a new offering from an existing vendor or to invest in a new vendor. We assess if the vendor is best in class for this particular feature or if it offers multiple capabilities; cost is also a factor. Additionally, we consider how well the solution integrates with our existing technology stack. We then conduct a proof of concept with three to four vendors that offer the capability that aligns with our needs. Throughout this process, we ensure that we consult with different groups of people who will be impacted by this technology investment and make sure we have their buy-in . For instance, if we are implementing a new endpoint security tool for our fleet of laptops, we select a diverse group of individuals across the company and during POC monitor if their laptop performance is being impacted. Once we have gathered sufficient data, we make an informed decision based on what will provide us with the most value."

How to Make Smart Investments in Cybersecurity Technology Solutions

By Katie Haug, VP Marketing

In an oversaturated market of cybersecurity solutions, making the right investment is crucial for safeguarding your organization without draining resources.

Understanding Your Organization's Unique Cybersecurity Needs

Before diving into the pool of available cybersecurity solutions, it is crucial to understand the unique technical and business requirements of your organization. In addition, understanding your organization's compliance requirements and regulatory mandates is essential. Different industries have different standards, and ensuring that your cybersecurity solutions meet these requirements can save you from costly fines and reputational damage.

Evaluating the ROI of Cybersecurity Investments

Evaluating the return on investment (ROI) for cybersecurity solutions can be challenging but is necessary to justify the expenditures. Look beyond the initial costs and consider factors such as long-term savings, potential risk reduction, and the value of protecting sensitive data. Quantifying the benefits can involve calculating the potential financial impact of a data breach and comparing it to the cost of the cybersecurity solution.

Additionally, consider the operational efficiency and productivity gains that come from implementing robust cybersecurity measures. A secure environment enables smoother business operations and can enhance customer trust and loyalty, indirectly contributing to increased revenue.

It is vital to also evaluate your current solutions and ensure they do not offer the specific functionality you are looking to add to your stack. Many times you can upgrade existing technology, however, if you need to invest in a new solution then truly understanding the ROI is important.

Navigating the Overwhelming Market of Security Solutions

The cybersecurity market is flooded with vendors claiming to offer the best protection. To navigate this overwhelming landscape, start by creating a shortlist of solutions that align with your identified needs and priorities. Use industry reports, analyst recommendations, and trusted sources to narrow down your options.

Engage with vendors to conduct thorough product demonstrations and proof-of-concept trials. This hands-on approach allows you to see the solutions in action and assess their effectiveness in real-world scenarios. Pay attention to the scalability and flexibility of the solutions, ensuring they can grow and adapt with your organization.

Key Criteria for Selecting the Right Cybersecurity Products

When selecting cybersecurity products, several key criteria should be considered. First, evaluate the solution's ability to integrate with your existing infrastructure and other security tools. Seamless integration minimizes disruptions and enhances overall security posture.

Look for solutions that specifically address your needs - both from a technical and business perspective. This may be a time consuming, yet incredibly beneficial step because a comprehensive evaluation of those capabilities will save you time later on in your investment journey. Additionally, consider the vendor's reputation, customer support, and commitment to ongoing updates and improvements. A strong partnership with a reliable vendor can significantly enhance your cybersecurity strategy.

Leveraging Expert Insights and Peer Reviews

Expert insights and peer reviews can provide valuable perspectives when making cybersecurity investments. Engage with industry experts, attend conferences, and participate in forums to stay updated on the latest trends and best practices. These interactions can offer practical advice and help you avoid common pitfalls.

Peer reviews and case studies from organizations similar to yours can also be insightful. Learning from the experiences of others who have faced similar challenges can guide your decision-making process and provide confidence in your chosen solutions. Additionally, consider joining industry-specific groups or associations that focus on cybersecurity to build a network of trusted advisors.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM