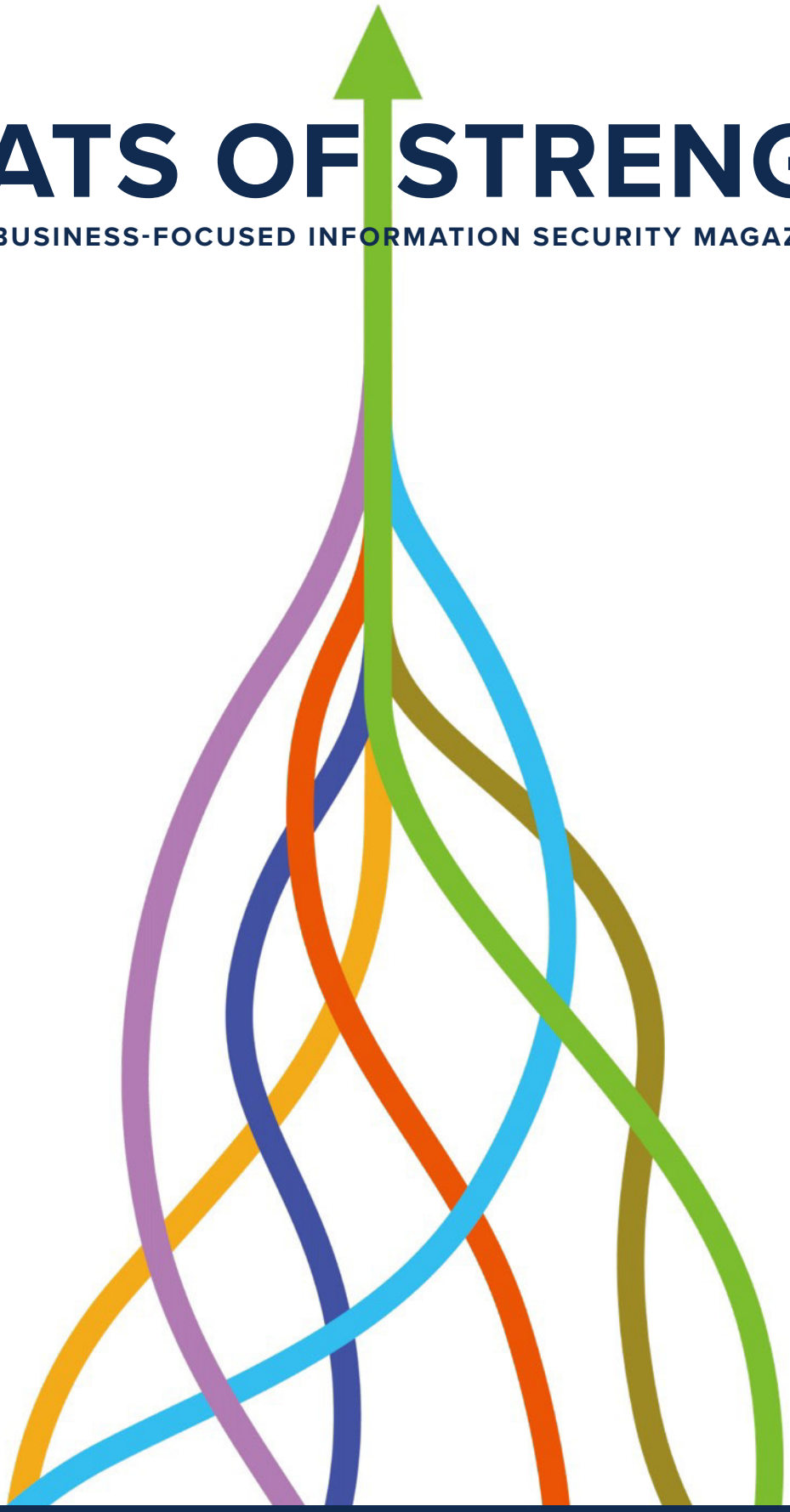
FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE



REDUCING COMPLEXITY

SEPTEMBER 2019
KLOGIXSECURITY.COM
617.731.2314

K logix

REDUCING COMPLEXITY

SEPTEMBER 2019

www.klogixsecurity.com/feats-of-strength
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.

Magazine Contributors:

Katie Haug
Director of Marketing, K logix

Kevin West
CEO, K logix

Kevin Pouche
COO, K logix

Marcela Lima
Marketing Coordinator, K logix

LETTER FROM KEVIN WEST CEO

We asked ourselves and our CISO community, what is hindering your ability to transform at the same pace as the business? The answer was often the inability to reduce complexity. To security leaders, complexity means too many underutilized security products, teams with a limited amount of time, and struggling to advance at the same pace as the business. These things combined weigh down security programs, people, and technology when they try to rapidly move forward and strategically advance at the same rate as the business.

Because reducing complexity is an on-going, important issue facing the majority of our customers and the security community, we've created services to help you transform and keep pace. I want to highlight some of these services we created in response.

Reduce Complexity and Consolidate

CISOs may leverage organizations such as K logix to take the burden off their teams, increase the credibility of security, and ensure security programs keep pace with the business. One of the ways we do this is through our Security Investment Assessment (SIA) service.

Our SIA service evaluates your security products and establishes alignment to operational maturity, risk mitigation, and financial cost. One key output of SIA is allowing you to consolidate your number of products, focusing on the ones that make the most impact and align best with the technical and business requirements of the business. By divesting overlapping products, you save time and money, and by improving operational maturity, your program is able to keep pace with business transformations.

The end results of SIA enable you to eliminate redundancy, consolidate investments, operationalize or sunset underutilized investments, and improve retention by giving your team time back. In turn, you ensure your program keeps pace with business transformation and continually increases your credibility.

We go into more details about our SIA service on page 22 in this issue.

Making Justified Investment Decisions

If you are considering purchasing a new security product, our Project Advisory service agnostically helps you determine the best investment to make, based on your specific identified risk.

Our Project Advisory service helps clear the clutter by identifying and prioritizing business and technical outcomes that need to be achieved in order to remediate key risks and advance security programs. Our approach is not focused on market hype, but on our clients desired outcomes, security maturity, and operational capabilities. Our results save your team valuable time and provide a justified business decision. Through our six-step process, we take the burden off your team and leverage our proven methodology to narrow down security products in a justified, analysis-backed manner.

Not only are you able to present business-focused, executive-friendly results to gain budget for your decisions, but we typically do so in 90% less time than it would take to complete internally within a security program.

Overall, reducing complexity results in giving your team valuable time back, saving money, increasing your credibility, and advancing your security program at the same pace as the business.

We would love the opportunity to speak with you about how you plan to reduce complexity, and how K logix may be a fit for your needs. Please don't hesitate to reach out to us to learn more.

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

GARRETT SMILEY

CISO, Serco

HEADQUARTERS: Herndon, VA (Serco, Inc.) / Hook, England (Serco Group – Parent Organization)

EMPLOYEES: 50,000+ globally

ANNUAL REVENUE: £2.84 Billion GBP ($3.44 Billion USD) globally

Garrett Smiley is currently the CISO at Serco, a Financial Times Stock Exchange (FTSE) top 250 federal contractor company that provides business process outsourcing, citizen services, defense, healthcare, justice, immigration, and transportation services internationally in both the public and private sector.

Smiley approaches his work as a CISO by focusing on being a risk management advisor. He explains, "I think that a lot of people have historically misunderstood that security is not meant to be a control. The controls must be put in place by the organization and by IT proper. We simply help them to manage the risk by identifying it, helping them prioritize the remediation of it, and then confirming the remediation of that, functioning as an advisor. When we're acknowledged that that's why we're around, things tend to be a lot more mature in the organization and they tend to be a lot more secure, quite frankly, because the role of the entity is understood better."

BUILDING RAPPORT FOR STRONG COMMUNICATION

Smiley believes developing and maintaining rapport with both his team and other executives helps him accomplish goals in a meaningful way. He works hard to ensure he is constantly engaging with his team in a positive fashion that creates strong communication and solidifies team work. He explains, "Rapport really can't be built with individuals if you don't know something about them. And it can't just be because of the project that you want them to work on. Rapport is what sums it up. If I've gone to the trouble of building a relationship with you, then when challenges come, you're probably going to be a little more willing to work with me. This way we can achieve common goals instead of me only showing up when there's something that needs to be done."

Smiley says everyone on his team goes above and beyond and he ensures that he provides them with opportunities for upward mobility. Recognizing quality and effort among his team has resulted in promoting people in non-management roles into management roles, among many other ways his team continues to evolve.

MEANINGFUL BOARD INTERACTIONS

Smiley attends quarterly board meetings to regularly discuss cyber posture. He says, "During these meetings, cyber posture is being discussed in front of the senior executive management team, including the CEO as well as three other board members. They are hearing about it regularly. And my reports to them are pretty advanced. It covers things that we've accomplished, areas for improvement, KRIs, vulnerabilities status and dashboards, phishing campaign results, and whatever else is pertinent for that quarter. But they've definitely been seeing a lot more in the way of really detailed ground truth. Obviously, we frame it in such a way

"RAPPORT REALLY CAN'T BE BUILT WITH INDIVIDUALS IF YOU DON'T KNOW SOMETHING ABOUT THEM...IF I'VE GONE TO THE TROUBLE OF BUILDING A RELATIONSHIP WITH YOU, THEN WHEN CHALLENGES COME, YOU'RE PROBABLY GOING TO BE A LITTLE MORE WILLING TO WORK WITH ME. THIS WAY WE CAN ACHIEVE COMMON GOALS INSTEAD OF ME ONLY SHOWING UP WHEN THERE'S SOMETHING THAT NEEDS TO BE DONE."

that we can have a discussion about it."

To present in a meaningful way that translates technical into business language, Smiley follows certain rules of thumb. These include using visuals and explaining the security program in plain language. He says the more text dense presentations become, the more likely you are to lose your audience. To provide concise, business-aligned language he may not describe a tool to the board as a vendor would use to describe it, but instead put a business-impact spin on it (e.g., "insider threat" vs. behavior analytics).

To prepare for questions from board members, Smiley encourages CISOs to be armed with the ability to respond on the fly, and to deliver answers in a frank, straight-forward manner. He comments, "The people who are on our board are on other boards as well, as is common. And I could tell that they were not used to seeing this level of sophistication and level of truthfulness, to be blunt, in board presentations. I'm thrilled that I was the one that helped them to better understand these blunt truths and they've adjusted appropriately."

THE CHALLENGES OF BENCHMARKING

Smiley was recently asked how Serco stacked up against other federal contractors in regard to what they are spending on security and how others are staffing their security teams. Due to the sensitive nature of their industry, there is limited knowledge sharing taking place, and Smiley says no one is racing to divulge details about their programs.

He explains, "There are so many variables when it comes to benchmarking. Other organizations' budgets for security might exceed all the money my company makes in one year. It's not really comparable to talk dollars. And then when you get into percentages, does that make sense when you're taking a look at two entirely different industries? Federal contracting is kind of similar to the margins they deal with in retail, but it wouldn't be appropriately comparable to finance. I am not aware of there being any sort of public repository of information that would truly answer that question. I know it's something that everybody asks, but I'm unaware of where it would exist."

For internal benchmarking, Smiley focuses on Key Risk Indicators (KRIs) for all the regions Serco covers across the globe. He then compares where they are seeing risks across the number of different KRIs in that report. This provides a benchmark for risk, and he eventually plans to work with an external, federally supported group to measure risk.

MEASURING AND MONITORING TECHNOLOGY INVESTMENTS

Smiley continuously measures and monitors technology investments within the organization. This effort includes tracking contract renewal dates, evaluating cost, and determining functionality within the environment. He comments, "We take a look at old technologies that cost a fortune and see if we can do it for the same cost or cheaper with something new. Cost is always a driver and things going end of life is always a driver. Maybe this costs the same as that, but this provides me a lot more capabilities, so on and so forth. On average, throughout the calendar year, we are probably having serious discussions about replacing at least 10 to 15 technologies a year. And we're talking enterprise-wide stuff."

CONTINUING TO GROW AND LEARN

Heavily engaged in professional development, Smiley attends countless CISO events, conferences, and symposiums, and is a part-time adjunct who chairs multiple dissertation committees. He says, "I force myself to be aware of what's going on out in the academic world as far as research is concerned whether it's robotic process automation or cyber physical systems security. I've engaged in robust professional development and might even take on more than I should. But, it's smart to force yourself to continue to learn. I also try and force myself to take at least one professional certification exam a year, if not two. And the reason I do that is because, as most CISOs, I'm very busy and if I wait for an opportunity when I'm not going to be busy, it'll never come."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DEB BRIGGS
CSO, NETSCOUT

HEADQUARTERS: Westford, MA
EMPLOYEES: 2,500+
ANNUAL REVENUE: $910 Million

"Security can't be the department of 'no', it can't be shutting down everyone's projects. You want to protect your company and the data and people but at the same time you can't prevent the company from moving forward."

- DEB BRIGGS

From a young age, Deb Briggs expressed a strong interest in learning how things worked and how to take things apart, and this curious, problem solving mindset helped carve her a successful career in security. Her first job out of college was at GTE Government Systems, where Briggs first began understanding how to protect data in the organization. This sparked her interest in privacy of data and is where she gained a strong understanding of the importance of protecting data. She followed a well-defined path to security through IT infrastructure, all while focusing on solving complex problems.

Briggs spent the past sixteen years working at NETSCOUT, where she spearheaded the focus on security, eventually leading her to the CSO role. She explains, "When I got to NETSCOUT I was responsible for all of the IT infrastructure, and security was just piece of it. Security was part of my role, but it's hard when you are doing everything in IT and trying to balance security, risk, and strategy when help desk also reports into you. As the company grew, I was given the opportunity to take off all other hats and just keep security. I've been able to grow the department significantly since then."

Since becoming the CSO, Briggs expanded the security team and has experienced the increasing importance of a strong security program. Briggs discusses the shift of the security industry from being focused on perimeter to now focused on the expanding, constantly moving workforce. She comments, "Today there are so many more people who don't work in brick and mortar offices, they are now working from home and outside the office. NETSCOUT has over 2,600 human firewalls and each one is an active point into my network. There was a strategic shift of what we are protecting and how we are protecting it, and our old tools needed to change and keep up with this shift."

STRONG ALIGNMENT AND COMMUNICATION

The executive leaders at NETSCOUT are very engaged in security and the overall risks to the organization. Briggs has worked hard to ensure security is constantly aligned with the business, and that she is always communicating risk in a cohesive, understandable manner.

Briggs says security cannot be an inhibitor to the business and compares security to the brakes of a car, because without security people may not move as fast as they want to. She explains, "Security can't be the department of 'no', it can't be shutting down everyone's projects. When people come and ask for your support on a new project or initiative like moving things to the cloud, the security team must learn to balance being both agile and secure. You want to protect your company and the data and people but at the same time you can't prevent the company from moving forward."

The key to this approach is putting yourself out in the company and solidifying strong relationships with your business counterparts, something Briggs has worked hard at over her sixteen-year tenure at NETSCOUT. She believes being a strong communicator helps explain risk to the business and business users in order to gain enough budget.

ALIGNMENT AND UNDERSTANDING WITH BOARD MEMBERS

Briggs considers the drivers and projects important to NETSCOUT in order to understand how security can support the overall company strategy. By doing so, she sets herself up for success when discussing progress or initiatives within her security program.

The NETSCOUT board is comprised of some technically-minded members, allowing her to go into deeper program details than most CISOs would during board meetings. Briggs says CISOs should always remember that the board is looking at them to set the tone for the direction of cyber strategy for an organization. She says CISOs must know how to relate to board members and understand what questions they may ask. Briggs continually ensures she is polished, has thought about questions they could potentially ask, and thoroughly understands the needs and concerns of each member.

When updating the board on progress, Briggs leverages an agnostic third party that provides risk scores based on vulnerability scans. She explains, "I don't control the risk score from our third party, but what my team does can impact it. We can do things to affect that score, but I can't just call up and make it happen. Our board has faith in that third-party assessment because they get a sense of how we are doing from a vulnerability and risk perspective."

Whether she's asking for additional headcount, a new technology, or consulting service, in order to justify budget, Briggs starts with discussing the risk involved. She says, "As an example, I went to the executive cyber board and told them we had two customer inquiries for us to have Soc 2 Type 2 completed. I told them we should do this because customers have started asking for this. We are now in the process of getting that accomplished and it is part of our strategy for the next 18 months."

NETSCOUT sells into Fortune 500 and 1000 companies, who want to ensure they are protecting their data. Briggs says, "I don't recall a recent customer in the last two years who hasn't asked for a security amendments or equivalent audit."

ASSESSING CURRENT TECHNOLOGY BEFORE MAKING NEW INVESTMENTS

Briggs believes in conducting an annual assessment of their current investments. She says, "You can go out and buy tools today and most likely some will overlap with what you already have, some will be best of breed, and some may fall short. In my annual assessment, if a product is coming up for renewal, I will evaluate if it should be replaced. I will evaluate if there are other tools out there that offer more, or it could mean getting rid of two to three of my current tools. It's important to understand what tools we have, the function and data we have from these tools, and if we can combine or get rid of certain tools. We have all heard from vendors that they have AI and ML. We need this, we need to see indicators of compromise earlier in the kill-chain. Tools need to be providing this to us. No one can afford to have a bad actor on their network for 100+ days."

LOOKING OUTSIDE OF SECURITY FOR TALENT

With a competitive hiring market, Briggs looks for potential team members in unique places. For example, an open security compliance role could be filled with someone who has a finance degree and is highly trainable and interested in security. She says, "I look for people in unique places and I try to bring two to three interns in every summer. For interns, they are given the opportunity to get real world experience and it also allows me to get exposure to people I may want to hire in the future. You don't have to just look at people in security, it's important to have the ability to train people with different backgrounds."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

MARK FERGUSON
FORMER CISO, HONEYWELL

HEADQUARTERS: Charlotte, North Carolina

EMPLOYEES: 130,000+

ANNUAL REVENUE: $40 Billion

Formerly the CISO of Honeywell, Mark Ferguson has worked in a number of security roles over his 15+ year career in security. In 2004 he worked at an organization specializing in safety and control systems that was acquired by Honeywell. After obtaining his CISSP certification, he took on many security roles during his time at Honeywell, starting as an Infrastructure and Security Architect, working his way up to eventually become the CISO. He explains, "It was an interesting journey for me to become a CISO. In 2008, due to the economic downturn companies were doing less external recruitment and more internal hiring. So, I was able to benefit and the opportunities for internal candidates were there. I eventually moved out of my role as a Security Architect into the corporate global security team within one to two years. I had the opportunity to interface with the CIOs, the business CSOs, and business leadership. That helped me gain reputation and credibility, both externally within the business, but also internally within the security function."

ALIGNMENT & TRANSFORMATION

Throughout his career, Ferguson has instilled security as a trusted advisor to the business, making sure he was constantly advising them on risk and continually ensuring he understood what the business was trying to accomplish. One challenge Ferguson and many of his CISO peers face is keeping pace with rapidly growing business transformations.

Ferguson says today businesses are transforming in many ways including digitization and moving to the cloud, something that enables the business to grow, yet security departments aren't always equipped to keep up. He explains, "Security teams just weren't ready for the cloud. They lacked either the capabilities or knowledge to keep up and you almost had a perfect storm. Security wasn't capable of delivering on the business needs, and cloud took off leaving security teams scrambling to keep up. I discovered when I went through this myself and we thought we had a plan for cloud, but when you actually dig into it, you realize cloud is different. And how you provision, secure, and manage are completely different. I think a lot of security toolsets are sold as being cloud-enabled when really, they aren't. That was one of the things we discovered. You find out they can operate in the cloud, but they're not cloud aware. And that's a big difference. These types of things keep the security teams from being able to move at the speed that the business needs to operate."

SECURITY STRATEGY STARTING WITH THE BASICS

Ferguson says doing the basics and doing them well are always his top priority. He explains that if you do the basics such as patching, configuration management and managing identities, then you rapidly shrink the attack surface, and if companies do things such as these, they are much better positioned to avoid a significant cyber event.

He shares that any security plan must be founded on a strong and robust strategy for identity and data protection. He says, "You've

got to be able to manage and secure your identities, and everything that goes around that including access and authorizations. Securing your identities is crucial. And then having a strong plan to protect your data, which I feel is a place we're failing in, securing data."

Agile technology and services are also important for Ferguson's security program, with a heavy focus on automation, scalability, and being frictionless. For him it means having technologies that are adaptable and if he cannot automate, then he does not invest in them. The same goes for his internal processes or services, which must be frictionless otherwise the business will just work around security.

Ferguson says culture and a strong awareness program help drive good cyber hygiene. He comments, "We did things like launching a global security ambassador program. Rather than having the corporate security team telling people how to practice good cyber behaviors, we brought employees on board and had them go and evangelize on our behalf. We found people that had an interest in cyber and an interest in security and wanted to get a little break from their normal day job. We equipped them with the knowledge and the messages to evangelize on behalf of security. It sounds better if it comes from somebody in the business rather than a corporate security person telling you. I'm a big believer that people are the weakest link in the chain, and why they're so often the target of the bad guys, so you have to try and equip them as much as possible with the knowledge to make the right choices."

RISK-BASED, THREE-TIERED APPROACH TO BOARD METRICS

When preparing and presenting to the board, Ferguson believes it comes down to knowing the personalities and finding a strategic balance of what to present. He created a three-tiered approach to metrics, with operational metrics or things that he works on every day at the bottom, then a tactical layer which is what he presents to functional leadership. Then there is the strategic layer at the top which is presented to senior leadership and the board.

For Ferguson, discussions with leadership teams must be risk-based and translated in meaningful terms. He says, "When we say risk, I mean risk to the business, not a cyber risk because that's meaningless to them. They want to understand what the business impact of that attack is, whether it's reputational, financial, or some other risk to the business that might impact operations."

He takes a stoplight approach with green, red, or amber colors to show trends and the impact of those on the business. Ferguson prefers having a qualitative dialog with leadership, backed up by solid metrics. He believes in making sure the board understands the impact of each risk and the plan to solve it in an impactful, business-focused manner.

Ferguson said he was often asked by the senior leadership team about how they benchmark. He comments, "You always get asked, "well, how does it compare?" It's difficult to baseline data. Most companies don't really share, but we're always ready with an answer on how we're positioned against the industry or competitors. We've participated in benchmarking surveys but there's so much context in the data and until you've understood that context, it can be a little meaningless. For example, we took part in one survey and it looked like we were spending a fraction of what some of the others were spending on awareness. But we just didn't know who we were up against, their risk appetite, or awareness strategy. It helps if you've got the full context to better articulate your position."

INDUSTRY TRENDS - HYBRID MODEL AND CRISIS MANAGEMENT

Ferguson says the security industry will eventually end up in a hybrid model, with humans and machine learning working together. He explains, "The humans will be there to do what they do best - add context to the answers machines are producing. I see AI and machine learning having so much potential in the security space. I don't think people are necessarily looking at it holistically, but all this is going to come together at one point. And if you look at the use cases from data protection to threat detection to email security to automating risk assessments, everything is going to be powered by AI, and then in this hybrid model, value and context will be added by the human element to drive better decisions."

Another important trend is crisis management, something that still concerns Ferguson. He says, "One thing that concerns me is whether organizations are really ready to handle a major breach. The ones that handle breaches well have thought about it and prepared. They've got a plan, they've tested it, but the ones that go badly, they haven't planned for it. Cyber teams are going to have to get smarter at crisis management, because when something bad comes up, the business will ultimately look to them for answers. You must also be engaged with your HR, legal and comms teams, and understand the decision-making process during a cyber event. And when the media calls, are you ready with a response, do you know who to call, who is going to own the message, and test for basic things like what happens if your email system gets attacked. How are you going to contact people? Do you know their phone numbers? Details and responses to these kind of questions should be in a playbook. I don't think a lot of teams have really worked through that."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

SARA BERKSON

Chief Privacy Officer and Head Global Privacy Counsel, Vertex Pharmaceuticals

HEADQUARTERS: Boston, MA

EMPLOYEES: 2,500+

ANNUAL REVENUE: $3.04 Billion

When Sara Berkson, the Chief Privacy Officer at Vertex Pharmaceuticals Incorporated, graduated from Yale Law School, she imagined a career of lobbying for changes in health care laws. But the federal privacy law, the Health Insurance Portability and Accountability Act (HIPAA), had just gone into effect and her law firm, Ropes & Gray, needed associates to help with compliance projects for their health care clients. "It was an all hands on deck type of moment," Berkson remembers, "and I was hooked." What intrigued Berkson the most about the new health care law, and the myriad of state privacy and security laws that soon followed, was the risk-based nature of the determinations – the laws themselves were not so black and white and the interesting questions involved the areas of interpretation in between.

After leaving Ropes & Gray, Berkson worked in-house at Genzyme, a rare disease biotech company, then moved on to another law firm, Verrill Dana, to help grow their life sciences practice in Boston. In both of these positions, she worked heavily in privacy on areas such as clinical trials, patient support programs, and international data transfers. One of these projects was for Vertex, relating to a new division they were setting up that would involve the handling of data about enrolled patients and, after the project was complete, Vertex hired Berkson in January of 2015 to help set up the data protection standards surrounding the new program. "I wasn't focused on going back in-house at the time," Berkson recalls, "but the opportunity to join an organization that felt so passionately about bringing new treatments to patients was not something I could pass up."

In May of 2016, the European Union passed its privacy regulation, the General Data Protection Regulation (GDPR), which had a wide territorial scope, applying directly to many companies outside of the EU. Berkson, along with the Chief Compliance Officer, approached the Executive Committee to address how they would handle GDPR and the impact it would have on Vertex. So began a two year implementation project, led not just by Berkson and a colleague in the Compliance department, but by an individual in the IT group as well. "While you can have security without privacy, you cannot have privacy without security," Berkson says. "It is simply impossible to design and implement a data privacy program without a strong partnership with information security."

Vertex rolled out a new global privacy program, built on the principles of GDPR, across all of its affiliates and in March of 2019, the company created a designated privacy office with Berkson as its Chief Privacy Officer. One of the aspects of the new privacy office that was imperative for Berkson, and heavily supported by her leadership, was the need to have technical IT expertise alongside the legal. With this in mind, the company decided to hire an additional full-time employee on the information security team who would have a dotted line up to Berkson – an individual who could bridge the

THE CPO/CISO RELATIONSHIP

"Ultimately, information security and privacy really need to be aligned in order to best protect a company. Information security is best positioned to make sure that the development of systems account for data protection requirements through a principle called privacy by design. It's a true symbiotic relationship because, in order for IT to fully understand and appreciate what those requirements are, they need to work closely with the privacy office."

Given this, Berkson feels it is "extremely important that CPOs and CISOs have close relationships and are working together." Berkson herself has bi-weekly meetings with Vertex's CISO, discussing many topics including protecting intellectual property, privacy laws, upcoming information security initiatives, vendor contracts, and a multitude of other areas. She comments, "There's a lot of intellectual property and highly confidential clinical trial data that we worry about in the biotech space. And the information security team is tasked with making sure it is protected. The CISO and I will talk a lot about what projects he's working on, what new initiatives they're rolling out, and then I advise on how we can do so in a way that's compliant with privacy laws."

privacy office and IT, and help translate the legal and company requirements into technical ones.

WORKING CLOSELY WITH INFORMATION SECURITY

"I think that privacy and security are often different sides of the same coin, working towards the same goals." Berkson continues, "I really look to information security to help me make sure that we're being compliant as an organization. Usually when there are security requirements baked into a legislative framework, whether it's in the U.S. or otherwise, they are not directive in that they don't say 'you have to do these exact things.' They say, 'you must take reasonable security measures based on the risk of what you're trying to protect.' There's a lot of discretion in those frameworks and I rely on my colleagues in information security to tell me what those reasonable measures are for a given project."

In order to translate legal or privacy language into security requirements, Berkson also relies on the information security team to interact with vendors and work closely with the business as they are developing initiatives. She explains, "For example, if we have a project that's being set up where we need to transfer information and it's a transfer that makes sense legally, I'm always asking the business if they have worked with people in our information security team. The information security team can walk them through the options to help make sure that the transfer is protected."

Berkson also has advice for companies that are just starting to think about how to weave together a privacy office and information security. She says, "Some companies still put privacy within the IT group, but with GDPR, there has been a movement away from this. The European regulators have recommended organizing a privacy office outside of any part of the business that makes actual decisions on how data is used so that privacy can be truly an independent function. Because of that, we are starting to see companies with a global presence set up privacy outside of IT but with a close connection between the two."

GDPR AND CCPA

Being compliant with GDPR requires Berkson to work very closely with the information security team to tackle the many complex questions it has raised. She explains, "While GDPR was meant to harmonize privacy laws across Europe, that's not exactly what we're seeing, and a lot of the member states in the EU are allowed to pass their own derogations, or exceptions, under their member state law about how they want to handle something. And often, especially in the information security space, you need to look at specific country-level laws in addition to GDPR to see whether you're allowed to do something."

To tackle these challenges, Berkson says she takes a cross-functional approach, with her team presenting the legal/privacy aspects and her information security colleagues translating those into technical considerations. For example, under the GDPR, individuals have certain rights with respect to their data. Berkson works closely with her IT colleagues more broadly on handling such requests, as they often necessitate not only locating but accessing data across multiple systems.

Having set up their global program in-line with GDPR will help Berkson ensure they will meet the California Consumer Privacy Act (CCPA) requirements as well. She says, "When we're looking at complying with CCPA, we're going to be able to leverage a lot of the processes we set up for GDPR. For example, one of the big areas under CCPA is that data subjects in California are going to have similar rights to what people in the EU have. So, you can leverage a lot of your procedures and ways of working between IT and privacy when those sorts of requests come in."

REDUCE COMPLEXITY: THE INFOGRAPHIC

CREATED BY K LOGIX

One of the top challenges CISOs face is reducing complexity within their security program so they may instead focus on business alignment and strategic advancements while continuing to reduce risk. Reducing complexity most often means the combination of an under-resourced team and too many security products.

Furthermore, as businesses transform, the complexity will continue to increase and security will be continually tasked with keeping pace with changes within the business.

TOO MANY SECURITY PRODUCTS

An abundance of underutilized security products hinders productivity and may inhibit strategic focus. On average, CISOs believe 80% or more of their products are underutilized. Managing too many products is a drag on resources, from both a budgetary and time aspect. With consolidation as one of CISOs and security leaders' top priorities, they must focus on reducing the number of products in their environment to free up money to spend on other important areas, as well as give their team time back.

In the article about K logix's Security Investment Assessment, we discuss how this service provides an evaluation and analysis of our customers' security products in order to provide them with the ability to consolidate and operationalize.

CISOs should leverage a service such as K logix's Security Investment Assessment to reduce redundancy, eliminate waste, increase the value of investments, and in turn improve retention.

TEAMS SPREAD THIN

Today, security teams are spread thin. With one million or more unfilled cybersecurity roles, CISOs and security leaders often struggle to find qualified candidates who possess a balance of business and technical expertise and acumen.

Not only are many security teams small, but budget often plays a factor in the ability to expand, or meet salary demands of potential candidates. It also leads to higher employee turnover compared to other industries, with the allure of more money and perks moving people to different organizations. Security teams must be nimble and wear many hats in order to strategically protect the organization and make a positive impact on the business.

As noted in our infographic, teams are dealing with a plethora of tasks including things such as SOC alerts, complex security architectures, and IoT, to name a few. Many CISOs we speak with say their teams' tasks vary daily based on what alerts, new threats, and requests from the business come in.

CLOSING THE COMPLEXITY GAP

We recommend CISOs to partner with organizations to help evaluate their security products and alleviate the time their teams spend on managing underutilized or not fully operationalized products. Before investing in new technology products, they should assess what they currently have.

Security should also be factored into all business decisions. By doing so, security avoids adding complexity to business decisions such as moving to the cloud. If security is brought in after the fact, they are often viewed as roadblocks and impeding progress.

Automation and orchestration are ranked as one of CISOs top goals in 2019. Not only do both of these reduce complexity, but they help transform the security program to keep pace with the changing business.

Integration and collaboration enable security programs to reduce cost. For example, an open, connected, cloud-based security platform brings security products together and closes the gaps that point products leave in your defenses.

If you would like a poster-sized version of the infographic we created, please let us know and we will happily ship it to you.

To learn more about reducing complexity, visit:

www.klogixsecurity.com

THE CHALLENGE:

Under-Resourced Team + Too Many Security Products

leads to

INCREASED COMPLEXITY

TOO MANY PRODUCTS

Enterprises use as many as **40** different security products from **80** vendors[1]

77% report they have too many point products to track and manage[2]

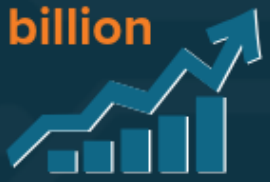
Yet, **45%** of CISOs are focused on acquiring new tools & solutions[2]

TEAMS ARE SPREAD THIN

55% handle more than 10,000 SOC alerts per day[1]

68% believe it is essential to reduce complexity within their security architecture[3]

The number of connected devices in use is expected to grow to **125 billion** by 2030[4]



CLOSING THE COMPLEXITY GAP

Assess the products you have before investing in more

Security must be factored into all business decisions

Automation and orchestration

Integration and collaboration

K logix

Research by: Katie Haug
Graphic created by: Marcela Lima

Sources:

1. "Break Through Cybersecurity Complexity With New Rules..." Security Intelligence, 28 Jan. 2019
2. "Simple Is The Goal: Reducing Complexity In Security." Forbes, 10 June 2019
3. Ponemon Institute Research. "The Cost & Consequences of Security Complexity Study." MobileIron
4. "The Security Risks Presented by Complex Networks." Fortinet, 1 May 2018

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

BILLY SPEARS
CISO, IOANDEPOT

HEADQUARTERS: Foothill Ranch, California

EMPLOYEES: 6,000+

ANNUAL REVENUE: $1 Billion+

EVOLVING INTO A BUSINESS STRATEGIST

Billy Spears believes his knack for strategic problem solving combined with strong communication skills from a young age prepared him well for his career in cyber security. Currently the CISO of loanDepot, a fast-growing national consumer lender that matches borrowers through technology with the credit they need, Spears is focused on helping with continued innovation and growth.

He began his career with a strong technical understanding as a solid foundation for his cyber security experience. During this time, Spears worked on tactically solving problems, growing his understanding of business challenges, and becoming a dependable resource for organizations. He then grew into a business strategist, melding his technical skills with the skills necessary to improve productivity, increase morale, and take the strategic corporate vision and help execute it through his security program. He says, "In order to become a business strategist, I had to learn how to be a leader, not just a manager and not just a deep technical expert. I learned from a lot of mentors and I think I've been fortunate throughout my career to have phenomenal mentors that continue to grow me, even when I didn't think that I needed growth."

He continues, "I learned early on that I could make impactful changes. I could get a breadth of experience in places that I wouldn't otherwise be exposed to and I could learn how to accomplish these very tough concepts in other vertical sectors. On my resume, you'll find that I've worked in almost every vertical sector and accomplished significant things. That was the allure for me. I wanted to go places where I could make a difference, where my skillset was a benefit, and where I could work on challenges that hadn't been solved before."

IMPACTING INNOVATIVE TRANSFORMATION

Joining loanDepot provided Spears the opportunity to work at an organization with futuristic and innovative ideas. He was sold on the idea of being able to build something that didn't already exist. Being in the mortgage industry, Spears recognized that historically the industry was very manual driven, with not much technology and no way to speed up, create efficiency, or lower the cost of a loan. Working at loanDepot enables him to be part of a team who strives to use

"THE BEST ADVICE I CAN COMMUNICATE WITH LEADERS IS THAT CLARITY IS KEY. A GREAT LEADER IS SUCCINCT IN THEIR MESSAGING, STRATEGICALLY NEGOTIATES FOR MUTUAL OPPORTUNITIES, AND LISTENS FOR ALIGNMENT."

technology to disrupt the mortgage industry and establish a new digital transformation that allows customers to increase their speed to market and improve their ability to acquire services and products.

Spears believes that aligning security with digital transformation requires agility and a true understanding of the company culture. He explains, "If I need to advise the business about a security related risk, if I need to talk to the board, or if I need to talk to the CEO, they are all very supportive, which provides a unique opportunity to establish rapport and influence how other leaders approach problem solving within their areas of responsibility. This softer approach allows the infusion of cyber security and privacy at the beginning instead of the middle or end where it's much more costly to revise plans or start over."

He continues, "The misalignment with executive leadership tends to come from not understanding the culture of the company, and it is imperative to stop yourself because it's a natural reaction for security professionals to just dive in and understand the detail surrounding cyber risk. It can be overwhelming to consume by business executives so you must build an institutional baseline before communicating these types of risk. You must understand what the company's about and what are their market conditions? What are the internal structures and politics that affect change around the business? What type of corporate services or products do they sell? They might have a different audience. And then lastly, what are their technologies and core systems?"

STRATEGIC GOALS FOR IMPROVEMENT

Spears lays out his top goals for the next twelve months including efficiency, maturing the information-governance posture, and improving awareness. The top goal for Spears is improving strategic alignment with the threat landscape and business priorities. He considers the social and economic factors driving change outside the business, then establishes his strategy for success, and scopes these changes to the ever-changing business priorities that come from the senior most executives.

Another goal is maturing the information governance posture to ensure it is defendable, repeatable, and sustainable. He believes this provides the business with comfort that core capabilities are implemented to proactively manage risk. He seeks to constantly improve as technology evolves into more of a digital ecosystem.

In the governance layer, Spears wants to improve awareness, training, and outreach. He explains, "It's important to speak to people in a way that they'll receive information well, instead of the traditional lectures or just e-learning courses. You should never deliver training once a year and check the box complete as your staff population will not retain the knowledge and perform associated actions according to company requirements. It is vitally important to engage staff continuously to simplify the message. I love the idea of a universal resource hub where new content is created weekly and customized for role-specific needs across the business. This allows more versatility to develop user heat maps and understand risks by channel while supporting targeting investments with low performing areas. It is also important to include calls to action within your messaging strategy that directly result in higher engagement and longer knowledge retention. Lastly, make learning fun. I love gamifying the experience across the company."

He also wants to increase efficacy around the security architecture integration across critical functions and improve security operations. He says, "You should be integrated with product development, DevOps, the identity and access teams, legal, HR, product development, marketing, etc. And then obviously your networks, you want to understand what's coming in and out and you want to understand how traffic moves east and west. For security operations, you must have precise intelligence gathering, which increases performance for everyone. You want to automate your security operations group and ensure active monitoring increases the speed of discovering risks while naturally decreasing dwell time and reducing noise."

CLARITY IS KEY IN THE BOARD ROOM

When addressing the board, Spears says, "I heard a quote once that the words a leader speaks are important, but how they're delivered makes the difference. Security leaders don't tell stories. They come in with a lot of numbers and they're looking for boards to give them answers. The best advice I can communicate with leaders is that clarity is key. A great leader is succinct in their messaging, strategically negotiates for mutual opportunities, and listens for alignment. Tell them the story, give them a highlight of a couple of things in terms of themes that are important. Provide options such as A, and B, here's the implications of both, and then offer a recommendation for a strategy to mitigate the associated risk."

Spears believes in showing how the program is doing, where it should be, the gaps in place, and the future strategy. By following this approach, CISOs are able to gain support, improve their audiences understanding for cyber risk, achieve confidence from key stakeholders about their ability to be successful, and manage organizational risk in a more cohesive way.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

PABLO MOLINA

CISO, Drexel University

HEADQUARTERS: Philadelphia, Pennsylvania

EMPLOYEES: 9,800+

ENDOWMENT: $779 Million

MOVING FROM CIO TO CISO

During his time as a seasoned CIO, Pablo Molina attained his security and privacy certifications, created security policies for many organizations he worked for, and eventually realized he wanted to instead work as a CISO. Currently the inaugural CISO for Drexel University, Molina initially sought out to ingrain the idea of how information security shows strong business value to the institution's community. Doing so required Molina to speak in both business and technical language. He explains, "I'm talking about business and technical language and I'm very fluent in both. I'm an expert in higher education administration and have a doctoral degree in this topic. I've worked for many institutions, so I understand the business of research and teaching and everything I do. Whenever I bring up the issues of risk management or incidents or policies or initiatives, I do so by translating that into the business value and the risk management for the organization. Because we speak the same language, I think that I'm a very effective communicator."

LEVERAGING BUSINESS KNOWLEDGE FOR BOARD INTERACTIONS

Molina works closely with all senior executives, from the President to the Chief Information Officer, along with meeting with the Audit Committee of the Board and other Board Members. He says he is often requested to meet with these individuals because of the strong interest in managing risk for the institution.

He relies on communicating in the language the board understands by being well prepared to anticipate questions they may ask. He does not overwhelm them with technical terms or with reams of information. He shies away from 'scare tactics' and instead leverages his business knowledge to correlate security to things most important to the running of the institution.

Molina comments, "I think that we have very talented board members. They're very smart people. I like to provide written information. I like to provide some concrete metrics. For example, financial information is critical both for risk management, for savings, and for contributions to the bottom line of the business. I also like graphical presentations because when presented with information, humans oftentimes prefer this type of presentation. I do not overwhelm my audience with scores and scores of numbers."

MAKING SMART TECHNOLOGY INVESTMENTS

Making smart, purposeful investments in technologies are key for Molina's program. He explains, "Our advanced next generation firewalls are helping us protect the community, combined

"WHENEVER I BRING UP THE ISSUES OF RISK MANAGEMENT OR INCIDENTS OR POLICIES OR INITIATIVES, I DO SO BY TRANSLATING THAT INTO THE BUSINESS VALUE AND THE RISK MANAGEMENT FOR THE ORGANIZATION. BECAUSE WE SPEAK THE SAME LANGUAGE, I THINK THAT I'M A VERY EFFECTIVE COMMUNICATOR."

with our ability to respond to incidents, by using security information and automation technology. Also, security training and awareness tools for our thousands of faculty, staff and students are important to impact the culture of the institution."

To reduce complexity and ensure the technology investments continually meet needs from a security perspective, Molina has instituted a vendor assessment program. This program ensures they select vendors that are secure, have both security and privacy by design, and follow responsible computing principles. He says, "Everything becomes much simpler because it is not that you bought a product or a service and now you have to figure out how to make it secure; it is by definition that the company was thinking of making the product or service secure. Sometimes it requires making what may initially look like more expensive purchasing decisions, but in the end you realize that the total cost of ownership and the total risk profile are much more beneficial to your organizations."

Furthermore, Molina believes many CISOs have invested in security products and services yet are not taking advantage of the full business value they offer. He says you must maximize their use and master your own knowledge in order to get the most out of those products for your organization. He comments, "You have to be strategic about it. In my case, I have limited resources, and because they're limited, I may pay attention to new and interesting technologies, but in the end, I concentrate my efforts into doing business with a handful of vendors. And for those, I know the executives, I know their roadmaps, I know the application cases, I know the adoption patterns within the organization. That's the way I do it."

Molina encourages CISOs to work through their vendor and reseller channels to convey to them that they are strategic partners and attend their executive briefings whenever available. He also suggests for any vendors who host annual conference, to make it a priority to attend them.

FOCUSING ON FRAMEWORKS AND ASSESSMENTS

Drexel University is a complex institution with many divisions and units that are regulated differently, creating a unique challenge for Molina. He explains, "We do align to some different frameworks. For example, we have to be HIPAA compliant and for that we use specific frameworks. We have to be compliant with the Department of Defense Regulations for Contractors, so we need to follow those specific frameworks. We also consider the maturity index by organizations like Gartner. And then finally, because we are a higher education institution, we use many of the models and metrics for our specific vertical."

Molina conducts annual assessments, either internally or externally depending on what they are specifically evaluating. In some instances, he may conduct certain assessments every four years with an external partner, yet he prefers to conduct other assessments internally. He comments, "Internal is cheaper because you are re-purposing the resources that you already have in house. Internally is much easier because you reduce the friction of having to receive requests from the consultants, translate those and then securing those, the process is much more streamlined. The problem when you are internal is that on the one hand you may not have an objective point of view, as you are involved with day to day operations. And also, it could be the case that at the end of your assessment, you lacked the credibility that an outside party would have."

TRAINING AND RETAINING TALENT

Molina strongly believes in offering training and certification opportunities to his team and solidifies budget to accomplish this each year. He says, "I've always faced an interesting question from budget committees and board of directors, when I ask for a training budget, they have the argument that well, you train new people and then they leave. And my counter argument has always been: training people and having them leave is better than not training people and having them stay because they are not qualified to continue doing their jobs."

Molina sends his team to vendors conferences, large-scale conferences such as Black Hat, and specific training for sophisticated technologies like computer forensics. He also encourages minorities and women to enter into the cybersecurity field. He makes it a point to recruit both women and minorities. He is an active supporter of the Philadelphia Women in Cybersecurity group and helped create a Women in IT group on Drexel's campus. He is also one of the early members and board members for the Hispanic information Technology Executive Council, helping their mandate of finding a more diverse pipeline of talent.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

SOHAIL IQBAL
CISO, j2 GLOBAL

HEADQUARTERS: Los Angeles, California

EMPLOYEES: 2,700+

ANNUAL REVENUE: $1.3 Billion+

When Sohail Iqbal began his career, he worked in pure technologist roles and as his career evolved, he shifted to focus on strategic information security positions. When working at Quest Diagnostics he asked management if he could work on any upcoming audits, something they openly welcomed. He was able to conduct audits and was exposed to learning how to identify security gaps, which sparked his interest in shifting his role to be more focused on information security. He attained his CISSP and moved onto Dow Jones/WSJ where he worked on many projects including their transition to a cloud-first practice. At Dow Jones he was responsible for the strategy to help mature the security posture of many products under the Wall Street Journal including MarketWatch and Barron's. After eight years at Dow Jones serving as Head of Global Cybersecurity Operations, Iqbal was offered the CISO role at j2 Global.

For over one year, Iqbal has held the CISO role at j2 Global, a leading internet information and services company consisting of a portfolio of 48 brands, reaching over 180 million people per month. j2 Global's brands include businesses such as PCMag.com, Offers.com, Mashable, and Everyday Health.

"I LEAD THEIR BUSINESSES ON THE JOURNEY THAT HELPS THEM SELL MORE EFFECTIVELY WHETHER IT'S MAKING PRODUCTS MORE SECURE OR ACHIEVING LEVELS OF COMPLIANCE."

As the organization continues to acquire a multitude of brands in different verticals, Iqbal is tasked with analyzing the risk and evaluating the security stance at each brand before they join the j2 Global environment.

KEEPING PACE WITH ACQUIRING BRANDS

j2 Global purchases companies at an incredibly rapid pace and they are all integrated into j2 Global's security program, overseen by Iqbal. He manages security for all j2 Global's brands, and if the acquired brand had a security person already in place, they would then report into Iqbal.

Iqbal wrote a quantitative analysis for assessing the risk state and identifying gaps for the many brands j2 acquires. He comments, "This quantitative analysis of risk has built significant clarity in terms of portfolios that we bought, how risky they are, how to address gaps, how to prioritize budget, what resources are needed, and the timeline for all of these efforts. It provides a way of estimating what we need to do with each particular organization before they are inducted into our network and we open up our firewalls."

The biggest challenge for Iqbal is getting to know each of the businesses they acquire since it is not a singular business model, but instead a large portfolio of brands. He must understand each business and their culture, ranging from tech-savvy startups to legacy companies. He explains, "I have to understand the various threat landscapes for each of the brands we acquire, and in some cases

understand the legacy nature of operations or cutting edge demands for those portfolios. I have to do an assessment to get a pulse of the business and assess across the organization to see how I am going to customize and cater to each brands' needs. Every business unit is independent and had their own technology shop prior to being acquired, so I sit down with technology and development leaders to understand their needs and customize the overarching security strategy to address these requirements."

Iqbal works hard to educate each of the acquired brands that security is not there to block or create hurdles, it is instead there to create a paved road for them to drive their businesses faster. He uses the analogy of security building the right guardrails to make it difficult for cars to veer off the road. He says, "I lead their businesses on the journey that helps them sell more effectively whether it's making products more secure or achieving levels of compliance."

QUANTITATIVE REPORTING AND ANALYTICS

Iqbal leverages quantitative reporting and analytics to demonstrate progress and build clarity around the security program, rather than using qualitative results such as heat maps. He feels quantitative reports enable meaningful conversations, so he can clearly see what percentage of projects have been completed, what is pending, and how to align dates on specific timelines.

On a quarterly basis he meets with the executive management and discusses progress from a high-level, strategic roadmap perspective. He explains, "I came up with 11 initiatives we want to accomplish in 2019, so I give the executive management a state of where we are. I stick to a 12-month roadmap focused on how we help shape the organization by focusing on strategic and technical goals and starting with a baseline of maturity."

GROWING A STRONG TEAM

Iqbal has grown his team from four to eight members and plans to leverage employees outside of his team to help ensure strong security through innovative programs. He comments, "We plan to build a program called Security Champions that will be across the entire organization, where we leverage one person from each business entity. We will follow the model of train the trainer, so security champions become the bridge between security and the business entity they represent. They will help to run initiatives on our behalf and will be a soft extension of our team."

To retain talent, Iqbal relies on three things. First, he says there should be a clear definition of the responsibilities for each role. Instead of having people wear multiple hats, he makes sure they have a clear mission of their role and what they are responsible for. Second, he ensures each member of his team has a plan to grow their career. This could include sending them to appropriate trainings based on skills they would like to acquire. Third is making sure the compensation plan is aligned with the market and no gaps exists in terms of perks or salary.

He says, "My goal is to help my team know what their growth plan is. If someone is more interested in application security, then we need to make sure they are aligned to those initiatives and projects. I help them at a personal level by understanding these growth plans and their desired career path, making sure they are compensated in the right manner, avoiding micromanaging them, and giving them space to improve and grow. My philosophy is to empower them to mature and grow at their own pace in the direction they are interested in going."

CISO TIP OF THE DAY

Iqbal believes in shifting corporate cultures to avoid over-reliance on computer-based training tools. Instead, he designs a comprehensive, interactive process and program. For example, he writes a 'CISO Tip of the Day' that is sent out to the organization. These tips may be related to something on the news or a relevant topic to employees' everyday lives. He does not only focus on security from a corporate standpoint, but focuses on how security impacts their personal lives, whether it is protecting kids online or how to responsibly use social media. This opens communication channels between security and the rest of the organization and makes more people feel responsible for security.

TRANSFORMING BUSINESS LANDSCAPE

Threat vectors and motivators are constantly changing, and Iqbal believes a strong and embedded process and security culture help manage those risks, rather than relying on technologies. He explains, "I've seen some organizations look to technology tools to solve their problems and address risk. However, if you aren't addressing culture at an organizational level or you don't have processes that can be easily adopted or workflows that can be easily incorporated, then fancy tools will just collect dust on shelves. There is a clear gap in the market to keep up the pace with the industry and business. I look at transforming processes that are frictionless and user friendly, and that incorporate initiatives, so you are able to achieve value."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JOHN HEASMAN

CISO, Chegg

HEADQUARTERS: Santa Clara, California

EMPLOYEES: 1,000+

ANNUAL REVENUE: $255 Million

"As the CISO of Chegg I'm putting into practice all of the skills I've learned both on the technical and the leadership side."

- JOHN HEASMAN

John Heasman has had three chapters in his career so far, starting with the first chapter working as a cybersecurity consultant advising companies on how to build secure products and services. His second chapter was his career at DocuSign for five years, working his way from more technical-geared roles building out the application security team, to eventually becoming the Deputy CISO. During this time, he learned how to build, lead, and manage teams, and grow his influence as a leader. The third chapter of his career has been the CISO at Chegg, an education technology company that provides student services such as homework help, online tutoring, test preparation, scholarship searches, internship matching, and college application advice, as well as both digital and physical textbook rentals.

He says, "As the CISO of Chegg I'm putting into practice all of the skills I've learned both on the technical and the leadership side. The thing that really attracted me to the role at Chegg, beyond Chegg's mission, was this opportunity to lead a small but talented security team where I would be responsible for both the hands-on work because we're a small team, but also thinking strategically of how I could build out the team and put in place the foundations to get the team to the next level."

REACTIVE TO PROACTIVE SECURITY

Heasman focuses on being proactive and solving problems by anticipating challenges as the company rapidly grows. He is tasked with building out the risk management side of the information security program in order to have a framework for identifying, categorizing, and prioritizing risks. He comments, "Without a framework to do this, it's easy to become distracted and chase the newest shiny object to go work on and then suddenly the whole team is working on that thing. This is something I was very keen to avoid. I went through a period of fact finding, talking to as

many people and leaders in the company as I could and getting them to talk candidly about areas that we needed to improve upon. Then my team started to form a prioritization for our risks so that we could really boil it down to what are the key things we need to get done in the next six months."

By establishing this framework, he says it will allow him to have strong communication with the C-level staff and board on what they are doing to improve security. It provides the ability to drill down initiatives and projects to the right level of detail for those audiences. By articulating their top risks and what the plan to address them is, he will be able to demonstrate progress and that they are moving the needle in a meaningful way.

AUTOMATION AND SELF-SERVICE FOR SCALE

"One of my ideas coming into this role at Chegg was that I wanted to build a security organization that is relatively lean and relies heavily on automation and self-service. We need to put foundations in place for when the company is at a much greater size than it is today, so that we can scale with the needs of the business. Everyone must realize that simply adding more people in security, for fast growing companies, is not scalable. It's hard to find those people. There's a cost in time and money of training them up," explains Heasman.

For example, Heasman explains that a system to scan for vulnerabilities when developers deploy code historically required the security team to run the tool, analyze the findings, and email back and forth with developers, or create a ticket. He says this kind of process does not scale, but by leveraging static analysis companies that tailor findings to developers rather than security teams, the security team is no longer responsible for taking a large list of vulnerabilities and trying to work their way through it. He says this self-service approach is scalable but still has certain challenges, namely other teams may require training and the tools themselves require constant tuning to minimize false positives. When Heasman and his team integrate new security tools, he always considers how he can make the product or service available to other users outside of the security team that may benefit from having direct access to the data.

CLEARING THE PRODUCT CLUTTER

When addressing the cluttered security product market, Heasman focuses on understanding exactly how the solution will fit into the broader program and specifically what gap the solution addresses.

Heasman says, "There are a few key things I always look for in technologies. A few years ago, having products with API was a "nice to have" but nowadays I feel API support is an absolute necessity. An organization like ourselves, we're often not running these tools in isolation. They're often not run by humans, they're orchestrated by other processes and we want to pull the results down, manipulate them, store them elsewhere, and aggregate them with other tools. That's something I will always ask a vendor. I like to see vendors that have really considered their API and really understand how customers like us are going to use their product."

Heasman also speaks with Venture Capital companies and always asks for references from any security product he is interested in purchasing. He seeks references from companies of similar size and scale to understand how the product will address his specific challenges.

ALIGNING TEAM GROWTH AND LEARNING

Heasman fosters a team environment of continual learning, and in turn encourages his team to always share what they learn with one another. He believes it is everyone's responsibility to level-up the team, regardless of them being in junior or senior roles.

He explains, "Often a team member will come to me and have a certification, conference, or seminar in mind. I will ask what value that individual is going to get out of it, how that aligns with what we're trying to do as a team, and how that will help the company. That's the key thing. I want to make sure that our training efforts are aligned. I want the individual to get new knowledge out of it that will help them in their career development. But I also want them to share their newfound skills with the team and for this to help us on our mission."

The Huge Potential of the Education Technology Space

"When I consider a role, I'm looking for a company with a very clear mission. DocuSign and Chegg both have very clear missions. And, digital transformation, when it comes to the education space, historically it's been lagging behind other industries and I feel we're on the cusp of that changing. The education tech space is going to undergo massive growth. One of my goals here is to build the foundations of a program that will enable Chegg to scale and expand, whether that be through acquisition or expansion into international markets. The ed tech space has huge potential, but then of course this brings security and privacy challenges along with it. I'm really excited about the company's plans and the interesting security challenges that come along with those." - John Heasman

REDUCE COMPLEXITY WITH K LOGIX'S SECURITY INVESTMENT ASSESSMENT

Today, CISOs believe over 80% of their security investments are underutilized. They also believe many investments they have purchased do not correlate to specific security control areas and in some cases, they may be overspending.

Through trends such as the one above, K logix ingests this data to mold and mature the programs and services we offer to our clients. One of the top trending services K logix offers is our Security Investment Assessment (SIA) service.

The goal of our SIA service is to simplify your investments to mature your security program. CISOs are tasked with doing more with less and SIA provides the tools to achieve this. We help CISOs and security leaders improve and maximize the outputs of their investments while also reducing the number of security products required to protect their organizations.

THE CHALLENGE

Many solutions are purchased to solve a point problem, without considering the impact to operations, overall risk landscape, and total financial allocation. Many investments do not address the problem they were intended to solve.

With small teams, they may be overburdened managing too many security technologies. Many times, they lack a clear understanding of what products existed, who owned each product, if they were achieving their original purchase intention, and an overall handle on financial implications.

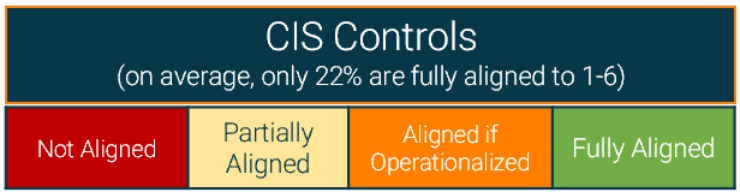
The key to improving security programs is to close the complexity gap by effectively managing the inherent complexity of technology investments and keeping pace with the environments in which they reside.

SECURITY INVESTMENT ASSESSMENT

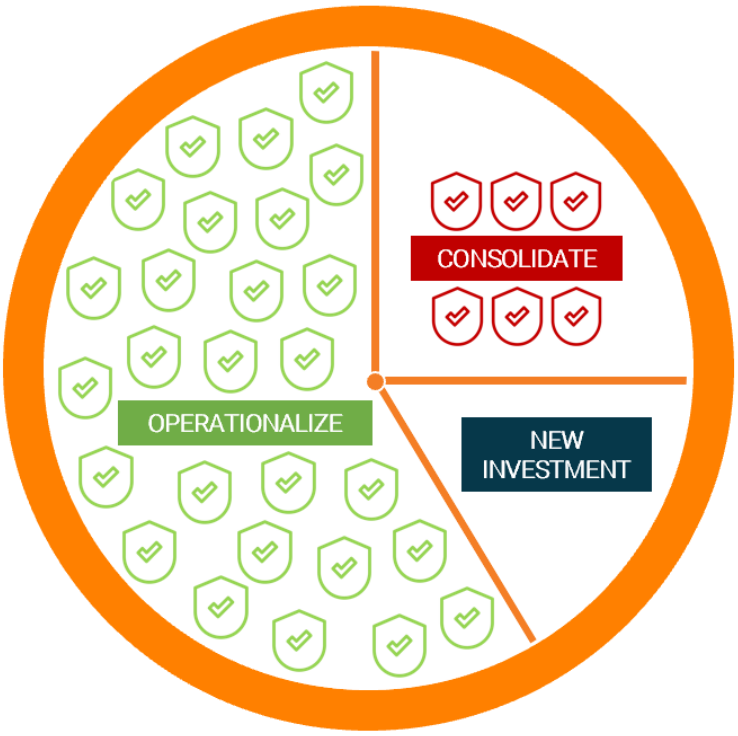
We simplify investments to mature your security program. K logix's SIA reviews your current technology investments through three lenses: Operational Maturity, Risk Mitigation, and Financial Cost.

OPERATIONAL MATURITY:

Through our in-depth analysis, we determine the operational maturity score of each of your security products. On average, most security products only score a 2.55 out of 5. After determining the scores of your products, we identify areas of improvement and actions required to increase their



CONSOLIDATE INVESTMENTS AND KEEP PACE WITH BUSINESS TRANSFORMATIONS



operational maturity. We take into account:

- The established outcome the investment was brought in to solve
- If feature sets are being maximized to keep pace with changes within the product and changes taking place within your business
- The product outputs and their ability to help you make decisions
- The standard operating procedures around the product – if the lead product stakeholder leaves, can someone take over without interruption?

Operational maturity helps you determine areas for improvement, actionable recommendations to increase the operational maturity score, and strong justifications for your decisions around investments.

RISK MITIGATION - CIS CONTROLS ALIGNMENT:

We correlate your security products to the twenty CIS Controls and score their alignment in keys areas ranging from 'not aligned' to 'fully aligned'. We look at each investment and provide details on how well it meets the spirit of each of the twenty control areas. In our experience, only 22% of security programs are fully aligned in control areas 1-6, which are the six most important and critical areas.

When evaluating alignment with mitigating risk through the CIS Control areas, we consider:

- How well each investment identifies and mitigates risk
- Maturity alignment with CIS Controls

FINANCIAL COST:

By gaining a clear picture into where you are spending money, you are able to observe areas to divest or consolidate. On average, our SIA service is able to divert 20% of budget away for products that were redundant or non-performing into risk areas.

During the review of financial cost, we take into account:

- Understanding of over-or-under investments
- Justification for sun-setting investments
- Justification for future investment decisions

BENEFITS OF SECURITY INVESTMENT ASSESSMENTS:

We provide in-depth details including an executive, business-friendly presentation, extensive findings report, and straight-forward, actionable recommendations.

With these deliverables, you will know:

- Which products to consolidate and how to do it
- Which products to operationalize and how to do it
- Where products overlap so you may divest and save money
- Where gaps exist and recommended products to fill them

By following our recommendations, you will be able to:

- Make justified, business-driven decisions
- Benchmark product maturity levels and understand where they need to be
- Receive a prioritized plan to mature your products

If you would like to learn more about our service, please let us know: info@klogixsecurity.com.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446