FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

TRANS FORM ATION

DECEMBER 2019

KLOGIXSECURITY.COM
617.731.2314

K logix

TRANS FORM ATION

DECEMBER 2019

FROM THE *Editor*

One of the biggest challenges we heard this year from our CISO community was the ability for security to keep pace with the rapid speed of business transformations taking place within organizations. What does transformation mean to businesses? According to our CISO interviews, many said business transformation means digitization, moving to the cloud, and investments in innovative strategies and technologies.

In this issue, we profile leading CISOs who share their thoughts on this subject and how they approach this challenge. On page 6, Sean Walls, CISO of Visionworks discusses how he ensures security is brought in from the beginning of any new innovative projects. Kevin Paige, CISO of Flexport, discusses his approach to ensuring security is considered a competitive advantage in moving organizations forward in any transformation they undergo. In his profile on page 18, he goes into detail about his approach to keeping pace with the business.

We also include Q&As from non-CISOs in this issue. On pages 11 and 12, hear from Domenic Serratore, Head of Privacy and Compliance at Lionbridge Technologies, as well as Susan Wise, Chief Privacy Officer at Biogen. They both share how they work with information security to help mature and grow their organizations.

CISOs are strategizing how they can move at the same rapid speed as business, and they recognize the benefits to their security program if they are able to achieve this. They are tasked with increased communication, interdepartmental collaboration, and strong business acumen in order to achieve this.

I want to thank all the CISOs and security leaders we profiled in 2019, their contributions to our magazine are invaluable and we are looking forward to a great 2020!

Kevin West

CEO, K logix

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

About K logix:

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.

www.klogixsecurity.com/feats-of-strength

marketing@klogixsecurity.com

617.731.2314

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

CHRIS LUGO
GLOBAL CISO, DANAHER CORPORATION

HEADQUARTERS: Washington D.C.
EMPLOYEES: 60,000 Globally
ANNUAL REVENUE: $18.3 Billion
SIZE OF SECURITY TEAM: 50

"Our program and our mission really centers around how we solve for the common [risk] denominator through a services-based approach that is supporting the different business intentions we have. At the same time, we are recognizing that a one size fits all approach is not going to be as effective as something that can tailor and evolve as our businesses rapidly change."

- CHRIS LUGO

Chris Lugo is currently the Global CISO of Danaher Corporation, a Fortune 500 globally diversified science and technology conglomerate. He began his career at Discover Financial Services where he held a number of technology and information security roles spanning almost fifteen years. He then moved on to Hilton Worldwide as Vice President of Information Security and Compliance for three years before joining Danaher Corporation.

Transitioning into a C-level security role allowed Lugo to look to the experiences of other CISOs and CSOs to learn from the best leaders in hopes of accelerating the programs under his leadership. He explains, "The transition to CISO for me was often met with many curvy roads and really looking at the available options following in those footsteps of many smart people who had done really phenomenal things in this day and age, while at the same time still writing the playbook or at least writing a set of instructions that other security leaders could follow. But in short, there is no playbook. And there was a lot of pounding my head against the wall to try to figure out the right solution at the right time that managed risk, but also enabled what the business was trying to accomplish, which is what we all should be doing today."

FOCUSING ON THE CORPORATE MISSION

To ensure Lugo and his security team align to the goals of Danaher Corporation, he focuses the security program mission on embracing the differing business intentions, providing for those common services, and at the same time being able to tailor program aspects in certain areas that are meaningful in different parts of the organization.

Lugo looks at the security mission through a number of aspects including the nature of Danaher's business as a diverse portfolio of companies. The ability to solve multiple challenges by using common solutions is paramount to Lugo. He ensures they are able to scale at an enterprise-level for common threats while adapting the security program in specific areas based on the nature of

their businesses and where the threat model may be different.

He explains, "Our program and our mission really centers around how we solve for the common [risk] denominator through a services-based approach that is supporting the different business intentions we have. At the same time, we are recognizing that a one size fits all approach is not going to be as effective as something that can tailor and evolve as our businesses rapidly change."

THE IMPORTANCE OF STRONG COMMUNICATION

Lugo believes frequent communication is critically important in making sure security teams along with directly adjacent teams like IT, keep security front and center. This is key in ensuring the intention is clearly communicated for a new security program, a new policy, or a new initiative, and how these may impact important business operations. Lugo accomplishes this through three measures including voice of the customer, translating security awareness into different languages, and branding the security organization.

He comments, "First, we build our approach with the voice of the customer in mind to minimize any disruption, avoid delays, and prevent any stumbling blocks that would prevent us from achieving our goal. Next, being a global multinational organization, and this may sound simple but really goes a long way, we translate as much of our awareness and education, our phishing simulation messages, our newsletters, into at least nine different languages to appeal to our global user base. Third, we've tried to make security as visible throughout the organization as we can by giving it an identity and making it real to people in their day-to-day lives. We brand the security program to show we're really aligned to protecting our employees just as much as to protect our company's information."

LEVERAGING METRICS

"As I was transitioning into the security leader role, I was really looking for someone who cracked the nut of security metrics and had the template we could all follow and leverage. And we're still today seeing that it's a mixed bag of different metrics that we rely on," says Lugo.

Within his team, they have a standardized set of operational and mostly activity-based metrics including vulnerability density (number of vulnerabilities divided by number of assets by severity level) to understand the density of vulnerabilities across their environment. This heat map of density allows him to focus on where threats may be shifting or where

"As I was transitioning into the security leader role, I was really looking for someone who cracked the nut of security metrics and had the template we could all follow and leverage. And we're still today seeing that it's a mixed bag of different metrics that we rely on."

prioritization or resources are likely needed. He is able to answer questions such as where they need to spend the most time and attention. He is careful to avoid what he calls the 'chasing zero effect', striving to reach zero vulnerabilities, as routine software updates and system hardening should be a continuous exercise.

When Lugo starts to think about metrics presented to executives, he focuses on the critical few to tell the story of how they are performing and what good looks like within their organization, and against industry benchmarks. These include the human impact of security through education and phishing training.

CISOs: FOCUS, LEADERSHIP, AND ENTREPRENEURSHIP

Lugo says many publications discuss the difficulty of the CISO role saying it is not a career you choose, it chooses you. He says there is no playbook or off-the-shelf program that is going to work in every organization, true to the constantly evolving and ever-morphing nature of businesses and today's threat actors.

Lugo explains, "The security function, what makes it so exciting is that threats are changing, attackers change their motives and their techniques change. And at the same time businesses are quickly becoming more and more digital, moving their on-prem solutions to cloud-based, they're coupling analytics to their product lines or embracing technology in their products and services. All organizations nowadays are driving technology investments and creativity in one way or another. To bring all this back together, the security leader is really at a great point today to not only take programs leaps and bounds above and farther than they may have ever dreamed, but also truly bring the right focus, the right leadership, and the right level of entrepreneurship into an organization to help companies grow and thrive. For me, it's a great time to be in the security leader role and we couldn't have any more support nowadays than we've ever had. Couple those things together, it's a great opportunity and a great time to tie security programs into the core of the business and the heart of the organization."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

SEAN WALLS

CISO, Visionworks

HEADQUARTERS: San Antonio, TX

EMPLOYEES: 8,500+

ANNUAL REVENUE: $947.4 Million

SIZE OF SECURITY TEAM: 15+

Sean Walls began his cyber security career in the late 90's but had his first serious opportunity to develop a well-rounded understanding of security and IT governance in 2002 while working at Black Box, an international technology solutions provider. During this time, publicly traded organizations were required to implement section 404 of the Sarbanes Oxley Act, and through his work on this, Walls had his first exposure to true security from a structured framework and governance perspective, including policies, procedures, and standards. After moving on from Black Box, Walls spent almost ten years at Presidio, providing security consulting services to organizations through extensive work with security policy, standards, process, compliance, PCI, HIPAA, as well as penetration testing, social engineering, and risk assessments. He went on to lead their external security practice, as well as lead their internal Information Security Office as Sr. Director of Information Security (CISO).

Walls comments, "While I was at Presidio, I was tasked with leading their cyber security division, which was an external facing consulting practice, but I was soon promoted to their CISO-equivalent. I spent about nine years at Presidio running their external facing cyber security division, as well as their internal facing security programs, including Governance, Risk Management, Compliance, Incident Response, Security Awareness, and so on."

After leaving Presidio, Walls worked at Eurofins, an international organization operating in 49 countries with over 55,000 employees. He held the title of Vice President of Cyber Security at Eurofins, and then moved to Texas to take on his current executive leadership position as Vice President and Chief Information Security Officer at Visionworks, one of the largest optical retailers and healthcare provider in the United States with over 700 locations nationwide.

SECURITY AS AN ENABLER TO THE BUSINESS

Joining Visionworks meant Walls had the opportunity to work for an organization where security is viewed as an enabler to the business and an integral part of the security strategy. Leaders at the organization believe technology and security should play an important role in helping meet and protect goals and priorities of their business strategy. Walls saw great opportunity in working for an organization where IT and security play an integral part of business strategy.

Walls comments, "Security needs to be an integral and valued part of any business strategy. And we need to manage cyber security risk the same way we manage financial risk, operational risk, strategic risk, and all other aspects of a business. We need to be doing the same thing for security. What we're seeing is a trend where more and more organizations are allowing their CISO to sit-in and present at board meetings. As a result, board members are getting visibility into the importance of security, compliance and cyber risk management; however, I read an article a few days ago,

Enhancing the Brand and Creating Value Through Cyber Security

"Security has traditionally been thought of as a hindrance to business. I would propose that it can be the opposite. Of course, it's there to preserve value and sometimes it does slow things down, but it can also be a creator of value, not just a preserver. And you can do that, for example, by certifying to SOC 2 or ISO 27001 and becoming a preferred partner to other businesses and customers in your market, demonstrating your commitment to security and privacy for your customers, and using that as a brand enhancer. Being able to have a well-tuned compliance program can also create value when you move into new markets. Whether it's overseas or a regulated market like California which has CCPA, you can ramp-up and become compliant quickly, helping to increase your company's speed to market and earning the company money because you're able to get into the market at minimal risk and fully compliant as quick as possible." - Sean Walls

that 38% of Fortune 500 companies still do not have a CISO appointed, which is a shocking statistic to me. We have many large organizations lacking a dedicated security executive in charge of managing risk and the security program. However, what I do see is a trend in the right direction, where security is becoming an important part of the business strategy."

Just over three months into his CISO role at Visionworks, Walls has focused on key goals to help him align security to the business and set himself, and the security program up for success. His goals include ensuring security has buy-in from executive leadership, understanding the business, and gaining clarity into risks, controls, technology, and governance, while ensuring that compliance requirements are being adequately met.

He comments, "I've meet with the various Vice Presidents and Senior Vice Presidents, along with the functional group leaders and other folks throughout the organization to understand not just what they do, but more importantly, how it's important to the business. What are the priorities for the business? How does the business function? What are the critical assets for the organization? And when I say assets, I mean not just technology and applications, because those are obviously important, but also the data, people, resources, and processes that run the business. In order to protect the business, you must understand the business and what's critical to its survival. So, that was the first thing, but there was a lot of things happening in parallel including understanding the technology stack, compliance gaps, and risk profile."

BUSINESS GOALS AND DIGITAL TRANSFORMATION

Being on the executive leadership team has enabled Walls to speak with other leaders to understand their priorities and goals. He says first and foremost, the goal is to improve the end-to-end customer experience. He explains, "Our goal is to make the customer experience as smooth and seamless as possible and to maximize customer satisfaction. And my role in this process is to leverage technology to enable the vision, and to ensure we control risk and meet compliance obligations in the process."

Furthermore, Walls says they are focused on growth and expansion, including increased market share and strengthening their competitive advantage. Visionworks is currently undergoing a full-scale digital transformation, something Walls has an opportunity to be a part of. He says they are adopting certain emerging technologies, business analytics tools, as well as migrating some systems to the cloud. This transformation will enable them to be more efficient, competitive, resilient, and nimbler, but also provide visibility into the market, their customers, their performance, and how they can improve their service offerings.

Walls believes many CISOs struggle to be involved in strategic planning discussions around digital transformations, but since enterprise architecture is rolled under Walls, he strives to ensure technologies properly align with the future state reference architecture model, which focuses on standardizing and consolidating the technology stack. Walls and his team ensure architectural reviews are performed for infrastructure, data, application, and security on all new projects. He advises other security leaders to ensure these four core areas be addressed at the design phase of any technology project, and to make sure they tack and align with the business goals and standards all the way through the SDLC.

In regard to security being involved in the early phases of digital transformation planning, Walls says, "If you own enterprise architecture like I do, then it's easy because you just change the process so that you inject yourself right at the beginning of every project. This allows enterprise architecture to review all projects to ensure standards are followed, security and compliance requirements are met, and the project aligns with business objectives. If you don't own enterprise architecture, then I would recommend meeting with the enterprise architecture team to make sure that they have a security architect on staff. If they don't, offer to let them use your services, if bandwidth permits. Often, enterprise architecture will look at a project and focus on infrastructure, data, and applications, since most think that's the core of enterprise architecture, but they're missing a really important aspect, which is security."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

STACY WILLIAMS
CISO, Zappos

HEADQUARTERS: Las Vegas, Nevada

EMPLOYEES: 1,500+

ANNUAL REVENUE: $2 Billion

SIZE OF SECURITY TEAM: 15

Stacy Williams' 29+ year tenure in information security began while working at a telephone company where he was first exposed to IT security during the organization's largescale migration from mainframe systems to distributed client server systems. Williams undertook the responsibility of setting up controls and boundaries around what people could and couldn't do, along with what they should and shouldn't have access to.

After working across many verticals, including information security roles at JP Morgan, the U.S. Department of Energy national laboratory, and Sears, Williams sought a new vertical to explore, leading him to Boyd Gaming in Las Vegas. He saw this vertical as a challenge and took a leap moving from Chicago to Las Vegas for the role.

While living in Las Vegas, the opportunity of being the new CISO at Zappos was brought to Williams. He explains, "I had an opportunity to get to meet and know both CISO predecessors at Zappos that sat in the seat before I did. The one before me, she had reached out and told me she was leaving and was tagged with finding her replacement and she thought that I would be a really good fit. She thought that my personality would fit within the management style that Zappos practices. And I looked into it and had some conversations with some folks and I saw that as another challenge, another opportunity to do something that I hadn't done before, learn a different vertical and hopefully bring something to the organization that they didn't have or hadn't had in any of their previous people that had sat in the seat."

During this process, Williams had conversations with other members of the Zappos team and researched Zappo's Holacracy management approach. Holacracy is defined as a method of decentralized management and organizational governance, in which authority and decision-making are distributed throughout a holarchy of self-organizing teams rather than being vested in a management hierarchy, something that peaked Williams interest.

Williams says, "I love the environment. It's different from the standpoint of a traditional corporate environment where you have that top down management approach. Within our current environment, things are a bit different with everyone being self-managed under the Holacracy structure. I can't directly go to someone and say, you need to fix this and fix this now because they have a set of priorities that they're working on, and their priorities don't always align directly with mine. I'd actually have to go through the process of not necessarily negotiating, but explaining to people why they need to care about things at the same level as I do. I can tell you one of the things that has definitely increased for me are my negotiation skills, just from the standpoint of being able to convince others that, hey, you need to care about this as much as I do. We probably need to put a plan in place to fix this sooner than later."

PROACTIVE VS. REACTIVE SECURITY

For Williams and his security program to remain proactive, it

RETAINING AND ATTRACTING TALENT

"I'm not a micromanager at all. Our Holacracy management style doesn't provide for that. I believe in giving my team the opportunity to exhibit and show the strengths that they bring to the table. I'm not the manager that'll have someone go in and write and develop a PowerPoint presentation or put together a Word doc that describes a process and then I take it forward and show it to leadership and to our board. That's not me. I will bring my subject experts into a meeting and give them an opportunity to explain things that they know and understand, and it gives them the ability to be comfortable with speaking in that forum.

The culture at Zappos is unlike anything I've seen and that helps a lot in attracting talent. A lot of people are interested in joining Zappos both because of the culture and what they've heard about us. We try to sell the fact that we live in an area where there's no state income tax and the housing market is reasonable here. There are a lot of things that give us the ability to attract talent. Showing that we're willing to invest in our people by paying for certifications, paying for continued education, those kinds of things go a long way in helping us attract and retain good people."

requires identifying tools or technologies that enable them to stay one step ahead, giving them the opportunity to identify more avenues of a layered security approach. He says, "Those things will give us the ability to have greater insight quicker. For our environment, we may have 25 tools in our toolkit and understanding that each one of those individually were intended to provide a certain level of protection or do certain things in our environment."

Validating that the tools in their environment are functioning as intended is key for Williams to be proactive, especially measuring this through a reoccurring audit. He comments, "We must validate that if we bought a particular endpoint protection tool to protect our endpoints that it is working closely enough with other tools that we have in our environment. We ask ourselves if it is providing us the level of protection that we thought when we invested in it or when we were sold it. Having some way to effectively measure that and then do that on a routine basis is important. But then also if you find that the tool isn't quite hitting the mark, you have to be able to assess that, identify it, and then go back to the manufacturer to make them aware of the fact that we were told that this tool would be able to do X and it's not."

Furthermore, Williams believes in making yourself visible with open lines of communication with other C-levels within your organization in order to think strategically and create ties between security and the business. He relies on understanding exactly what other executives' objectives are in terms of their priorities and the missions they operate on so you may help them achieve their goals.

"WE ARE ALWAYS TRYING TO KEEP UP WITH THE BUSINESS AND BE IN THE BEST POSITION POSSIBLE TO SUPPORT GOALS AND INITIATIVES THAT THE BUSINESS IS LOOKING TO ENGAGE IN."

BUSINESS TRANSFORMATIONS AND KEEPING PACE

Williams says time is one of the biggest challenges in trying to accomplish strategic goals. He says, "We are always trying to keep up with the business and be in the best position possible to support goals and initiatives that the business is looking to engage in. So that's always a big issue for us as we're looking at tools and technologies, we'd like to take our time and go through them to make sure that we can identify the best number of use cases for a particular tool. We don't always have the luxury of time and being able to give the level of review that we would really like to. But we try to put our best effort forward in doing so and making sound decisions."

People, process, and technology are how he approaches this challenge. Having the right people is the first component to ensuring they are doing the right thing by the organization. This includes identifying good talent and trying to attract and retain strong security-minded people. Having sound processes helps minimize what many organizations face on a regular basis. He explains, "If we have really good people, if we have really sound processes, then technology is third on the list. If you have those first two and it's really solid, I don't want to say you can take any technology and put it in place and it will work for you, but I think it makes the technology decision a little easier to over overcome because you've got really good people that will be running the technology. You've got sound processes in place to kind of check the bounds of those technologies and investments. The technology is important but having those first two pieces in place makes the technology decision a lot easier to make."

Q&A WITH
DOMENIC SERRATORE

Global Head of Privacy & Compliance

Lionbridge Technologies, Inc

1. What are your main responsibilities?

My role involves managing the entire compliance, governance and privacy function for Ironshore Inc. and all of its' worldwide subsidiaries. This included, however wasn't limited to, implementing and managing the following matters: Privacy Implementation and Management, Anti-Money Laundering (AML), Global Data Protection Regulation (GDPR), Know your Customer (KYC), OFAC and Global Sanctions Compliance, Global Compliance and Governance, Program Development, Risk Management, Global Licensing Specialist including Startups, Code of Conduct, including privacy and anti-bribery.

2. Are privacy and information security aligned at your organization?

Yes, my team & I work very closely with the InfoSec team in regards to privacy. The compliance team creates the processes and procedures with reference, however the InfoSec team with IT must implement the system requirements such as email encryption, secure file transfer portals such as FTP and the secure destruction on information at the owner's request or once retention periods have expired.

3. What do you rely on from the information security team at your organization?

As noted, the InfoSec team in conjunction with IT are responsible for the implementation and maintenance on system security in relation on privacy. They must implement and maintain encryption and information transfer secure portals.

4. What kind of relationship do you have with the information security leaders?

Extremely well. We have quick weekly meetings and I always involve the InfoSec team in all facets on a new or amended process or procedure that my team & I are implementing. The InfoSec team must be aware sooner rather than later as to what is required to determine what is needed from their side to implement the requirements.

5. What is the ideal relationship between CCOs and CISOs?

They must always have a very open and frank relationship. Both must be aware of what either is doing, what changes are being implemented in either direction, a weekly catch up call/ meeting should occur even if its only a 5-minute catch up.

6. What topics and questions does information security approach you about?

They always let me know of any changes that are being considered or being implemented. Matters such as operations system upgrades (Win 7 to Win 10, for example) are communicated in advance and matters such as record storage and in particular changes to storage are always discussed.

7. How have GDPR and CCPA impacted your work? How does information security fit in your work on these mandates?

Both require their own set of procedures and training initiatives and in particular, the GDPR as we need to involve local members such as the local Works Council in Germany of any changes, in particular any upgrades and storage from local servers to a cloud solution.

8. In general, how do you see future relationships between CCOs and CISOs evolving?

They really need to be situated in the same location and in close proximity. The InfoSec teams need constant access to the compliance teams and vice versa as in truth with the move to paperless and cloud storage solutions which cannot operate efficiently without the assistance and buy-in from the other.

9. Anything else you'd like to add about your work and/or your relationship with information security?

As discussed, the two teams InfoSec & Compliance must be close together and work closely on effectively all projects that are being considered and implemented either by necessity due to law changes, such as the GDPR or for company efficiency such as moving to cloud storage solutions. In future, they may be the same team reporting to a board committee as a joint effort.

Q&A WITH
SUSAN WISE

Chief Privacy Officer

Biogen

1. What are your main responsibilities as Chief Privacy Officer?

I actually have a broader role as Chief Privacy Officer than you might expect. In addition to leading our Global Privacy Office, which now has team members in US, EU and APAC, I also have responsibility for Information Governance (data lifecycle management and records retention/management programs), and the Risk and Governance programs for Cyber, IT and Privacy. These latter two teams are responsible for defining and helping operationalize our SOX and security controls framework (NIST-based), and identifying and tracking gaps within those, along with other identified risks. With respect to data privacy, our Global Privacy Office is responsible for ensuring our teams have the training and tools necessary to handle personal data responsibly as part of their business activities. My background prior to moving into Privacy about five years ago was in strategy and operations, so I very much enjoy the opportunity to advance and operationalize all of these programs at Biogen.

2. Are privacy and information security aligned at your organization?

I actually report into the Security organization (CISO), so that drives inherent alignment, but there is definitely a balance between leveraging our operating model for synergies and maintaining an independent lens on privacy considerations. In this respect, it is helpful the GDPR mandates require the Data Protection Officer to be appropriately resourced and and helps ensure programs appropriately consider how to respect and protect data subject rights and freedoms. Also, I have responsibility for governing our technical controls framework, so I ensure our technical and organizational controls are aligned with expectations of privacy regulators. It doesn't necessarily solve all the execution and prioritization considerations in implementing those controls, but at least it gives me confidence the right foundation is there.

3. What kind of relationship do you have with the information security leaders?

There are really two different sides to the interactions I have. The first relates to partnering on new programs and capability building the CISO organization is undertaking to mature our cyber security posture, and the analysis that needs to be done on these programs to ensure they are designed in a way that fully considers the potential impact on individuals. This is particularly important in areas like monitoring, DLP, and DRM. We advise using the Privacy Impact Assessment process, and partner with legal if country-specific legal analysis is needed. Being part of the same team, we can start these conversations early.

The other area is helping provide the review of vendors from a privacy and security perspective. My risk team has responsibility for the vendor risk assessment which gives the Cyber Ops team confidence our vendors have reasonable cyber/privacy capabilities to handle our data.

4. How have GDPR and CCPA impacted your work?

GDPR was the genesis for Biogen to develop the Global Privacy Office in 2015. We've tried to approach this with an intent to design global elements that can be leveraged and tailored as required for other regions. As an example, we might not be able to rely on 'legitimate interest' as the basis for processing in APAC as we can in the EU, but we do have many areas where consent is required in the EU, and we can use these as springboards to create other consent templates. We also leverage our core 'Data Subject Rights' process we defined for the EU for requests from those regions, or by extension, under the pending CCPA. We post all of these on an intranet site to make them easily accessible to the business.

Both IT and security are key in operationalizing privacy, as we look for ways to build data protection considerations into other processes, rather than making them stand alone.

5. In general, how do you see future relationships between CPOs and CISOs evolving?

For me, I think it will be interesting to see how the relationship between privacy, security and risk-as-a-function evolve in organizations. Outside of financial services, I suspect not many companies have highly formalized risk functions, but I think we will see this changing as boards and regulators like the SEC expect more focus and discussion in a more actionable way on how privacy and security create risk for companies. This will require more explicit conversations in the organization about risk tolerance, risk thresholds, and risk acceptance. Creating a common taxonomy will be the first step to drive these discussions. Cyber and privacy are of course only two areas of risk in the enterprise, but if there is a coordination between cyber and privacy, there is a real opportunity to help organizations advance not only risk management in these areas, but across the enterprise as well.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

SEAN MACK
CISO & CIO, WILEY

HEADQUARTERS: Hoboken, New Jersey

EMPLOYEES: 5,100+

ANNUAL REVENUE: $1.7 Billion

SIZE OF SECURITY TEAM: Undisclosed

"More software will be developed in the next four years then have been developed in the previous 40. That puts into perspective how much change we are going through every day and that means there's also new challenges every day."

Sean Mack has extensive background in all aspects of technology leadership including DevOps, security, cloud, infrastructure, enterprise applications, development, and program management. He has led global teams across a wide range of companies from large financial companies such as Experian to innovative technology companies like Etsy. Throughout his career he has held a variety of technology leadership positions ranging from Vice President of Operations and Applications for Pearson Education to CIO for a start-up in the streaming media space. Mack is currently just shy of two months into his role as CIO and CISO at Wiley, a digital education and research company.

TRANSFORMATION AND INNOVATION

Mack recognizes the increasing pace of innovation in every industry from banking to healthcare, but certainly in education and he says Wiley is currently transforming from a publishing company into a technology and education company.

At the same time, Mack says there are numerous changes within technology that create more challenges for security professionals. He explains, "More software will be developed in the next four years then have been developed in the previous 40. That puts into perspective how much change we are going through every day and that means there's also new challenges every day."

In order to address these challenges, Mack sees the need for an unrelenting drive for innovation and continuous improvements in automation. He says he is especially excited about the innovation occurring with containers and infrastructure as code. Mack believes in bringing information about increasing threats and potential attacks together using big data and combining that with machine learning and AI. By doing so, he can leverage machine intelligence,

rather than human intelligence, to try and detect and prevent threats and even anticipate and stop them before they occur.

MANAGING CISO AND CIO RESPONSIBILITIES

"I was at the CIO leadership forum yesterday and they were talking about aligning priorities between the CIO organization and the CISO organization. And I thought, why wouldn't they be aligned? And then I thought it's quite easy for me to say that because I'm both," explains Mack.

Mack acknowledges there may be friction between security and the need to move faster and deliver value. He focuses on enablement and looking at ways to empower the business to move faster and more securely, building 'fast lanes' instead of creating gates. He continues, "We see a lot of this when we start to talk about DevOps and DevSecOps. Instead of putting up more gates, let's automate our security so that it's part of what we do every day. You can release fast and you can release securely. It's also about being transparent. By sharing the issues with the other parts of the business you can increase awareness and get everyone involved in ensuring security."

Mack encourages security leaders to look at increasing security by building collaboration and engagement across an organization instead of making security a blocker. He values security being part of every aspect of an organization, including strong security awareness amongst employees. Something that worked for him in the past has been implementing a security hack week. This may include taking a day to try to attack or find vulnerabilities in your own product or an adjacent product, then fixing those things. By engaging in a company-wide initiative, a groundswell of interest and excitement grows around building things that get to market faster and more securely.

TRANSFORMATIONAL LEADERSHIP

Mack considers himself a transformational leader who is passionate about building things. He comments, "When I look back over my career, some of the things I feel most proud about are the organizations and the ways of working that I built in various companies throughout the years. It is amazing to look at places I've worked 10 or 15 years ago where the fundamental structures and teams that we put in place are still in place today. It's an amazingly gratifying thing to do. It's really exciting to be able to come into a business and help them transform."

This type of leadership stems from Mack's commitment to having a vision and executing that vision in a dedicated manner. For a shared vision to exist, Mack gains mindshare and commitment from his team, so everyone feels they are part of the strategic progress. He says the combination of vision and execution are the key things that have helped him drive organizations through transformation, similar to what is occurring at Wiley.

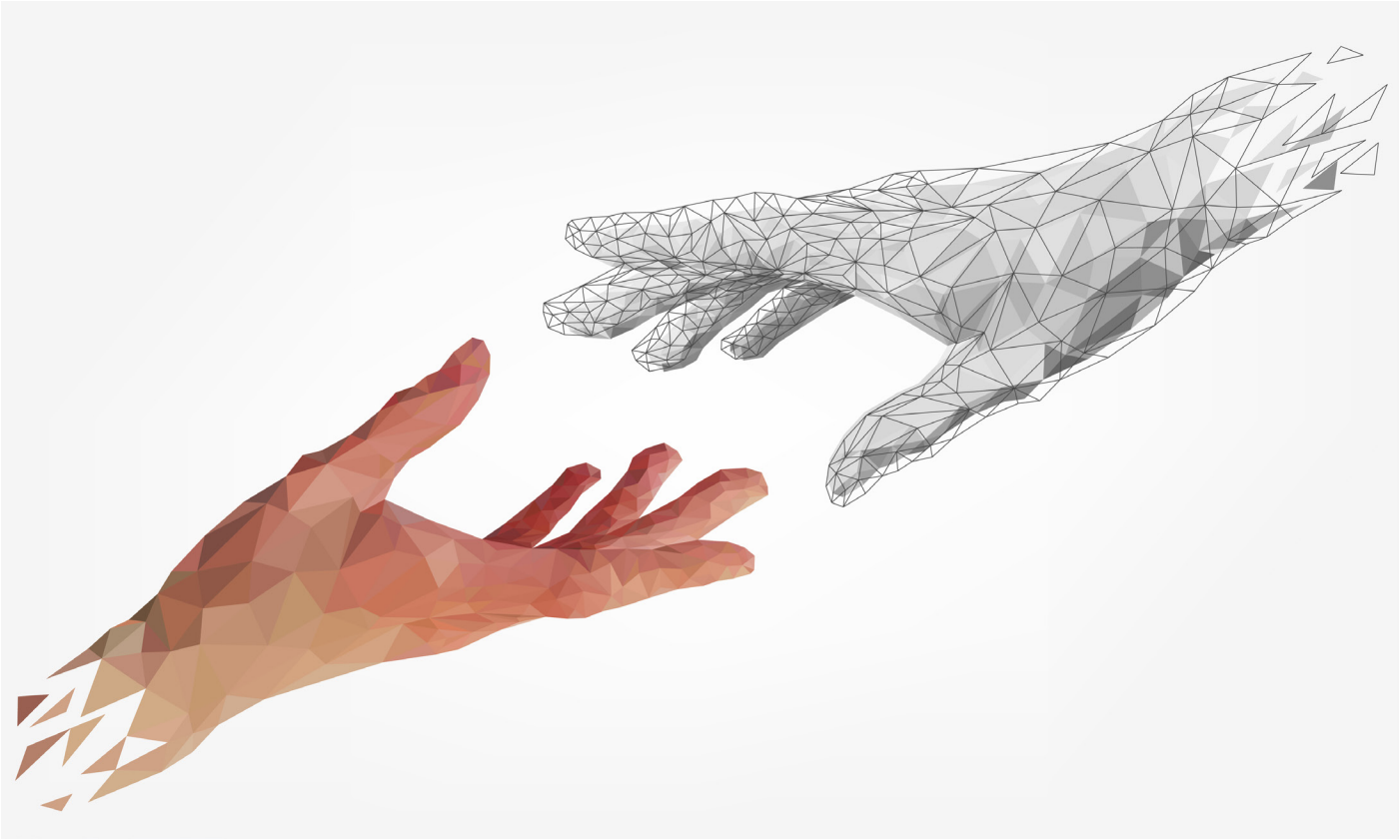
"Instead of putting up more gates, let's automate our security so that it's part of what we do every day. You can release fast and you can release securely. It's also about being transparent. By sharing the issues with the other parts of the business you can increase awareness and get everyone involved in ensuring security."

FINDING AND RETAINING TALENT

In order to attract talented individuals, Mack says Wiley is diversifying their global footprint. They recently opened a technology center in Sri Lanka, which is helping to rapidly grow their security team. They also build partnerships with outsourcing providers, along with attracting people by being an innovative company and great place to work.

He comments, "Wiley is a company that has been around for a while, about 200 years. It's only been here 200 years because of the amount of innovation that goes on. That's something that's very attractive to technologists, a company that's innovating and changing, and continuing to do new and exciting things. I also think people want to be part of a company that's focused on education. One of the things that attracted me to the company is that ultimately, it's about using technology to help people learn and grow their lives. Technologist security professionals who have a choice today, want to be part of something that's bigger than just making the next widget or the next dollar. At Wiley, they have the opportunity to do that."

TRANSFORMATION: IMPACT ON BUSINESS AND SECURITY



Businesses are transforming at a faster pace than ever before and security leaders are recognizing the need for their programs to keep pace. What does transformation mean to businesses? According to our CISO interviews, many said business transformation means digitization, moving to the cloud, and investments in innovative technologies.

HOW THIS IMPACTS SECURITY?

Chris Lugo, Global CISO, Danaher Corporation (profile on page 4) says, “You have to keep the business intentions front of mind. Otherwise, as we’ve seen with advances in technology, our business partners, our stakeholders will move on without the security organization when the security organization isn’t able to move fast enough.”

Stacy Williams, CISO of Zappos (profile on page 8) says, “We are always trying to keep up with the business and be in the best position possible to support goals and initiatives that the business is looking to engage in.”

Furthermore, Mark Ferguson, the former CISO of Honeywell (profile on page X), 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.”

As a security professional, there is a need for speed and agility, and it may be challenging to keep with the pace of the business. Often, every additional cycle you spend on a security review or building out a security control, could be a differentiator in how quickly a product or service goes to market. And often, the first company that gets an innovative product out could potentially dominate the market share for that particular space.

There is a great challenge as a security leader to attempt to understand how to inform the business on risks without being viewed as an obstructionist or an alarmist. Part of the objective is to provide a sense of calm in security leader’s evaluation of risk.

HOW TO KEEP PACE?

We asked our CISO community how they keep pace with the business transformations rapidly taking place. Some of their answers include being involved in enterprise architecture to inject security at the beginning of every project, building collaboration and engagement across an organization, and structuring a program around trust.

On page 6, we interview Sean Walls, CISO, Visonworks. Walls believes many CISOs struggle to be involved in strategic planning discussions around digital transformations, but since enterprise architecture is rolled under Walls, he strives to ensure technologies properly align with the future state reference architecture model, which focuses on standardizing and consolidating the technology stack.

Walls says, "If you own enterprise architecture like I do, then it's easy because you just change the process so that you inject yourself right at the beginning of every project...If you don't own enterprise architecture, then I would recommend meeting with the enterprise architecture team to make sure that they have a security architect on staff. If they don't, offer to let them use your services, if bandwidth permits. Often, enterprise architecture will look at a project and focus on infrastructure, data, and applications, since most think that's the core of enterprise architecture, but they're missing a really important aspect, which is security."

Sean Mack, CIO and CISO at Wiley, (profile on page 12) encourages security leaders to look at increasing security by building collaboration and engagement across an organization instead of making security a blocker. He values security being part of every aspect of an organization, including strong security awareness amongst employees.

He says, "...Instead of putting up more gates, let's automate our security so that it's part of what we do every day. You can release fast and you can release securely. It's also about being transparent. By sharing the issues with the other parts of the business you can increase awareness and get everyone involved in ensuring security."

On page 11 Susan Wise, Chief Privacy Officer at Biogen shares her thoughts on cyber security in a Q&A. She says, "Cyber and privacy are of course only two areas of risk in the enterprise, but if there is a coordination between cyber and privacy, there is a real opportunity to help organizations advance not only risk management in these areas, but across the enterprise as well."

Kevin Paige, CISO of Flexport, says trust is key to helping advance the organization. In his quote on cyber security and competitive advantage on page 18, a few key excerpts include, "When I'm talking to business partners, I use the word trust. It's all about trust, right? We want our customers to trust us. We want our employees to trust us. We want our business partners to trust us. Especially if you're a cloud platform or you want somebody to use a new cloud platform or technology or capability. You've got to trust it, and how do you trust it? How do you create that trust? How do we evolve that trust? People are going to use what they trust. If you have a brand that's trusted, if you have capabilities that are trusted, if you have people that you work with who are trusted, that is the key. That is the competitive advantage, right?"

We want to encourage our CISO community to strive to keep pace and make a significant impact on the organizations they work for. This often means establishing a strong security program that directly aligns with the goals of the business. Executive and board alignment is key in ensuring security is brought into all strategic conversations about growth, expansion, and innovation taking place within organizations.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JAKE MARGOLIS

CISO, METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

HEADQUARTERS: Los Angeles, CA

EMPLOYEES: 1,400+

ANNUAL REVENUE: Undisclosed

SIZE OF SECURITY TEAM: Undisclosed

"I think there's different levels of education because people need to understand what risk there is to them based on their role, what responsibilities they have in leadership for roles and responsibilities within a holistic security program."

- JAKE MARGOLIS

Early in his career, Jake Margolis served as an Officer in the United States Army Forward, deployed to Afghanistan as the Combined Joint Signal Officer, a role some would equate to that of a CIO. When he returned to the United States, he was asked to become the Information Assurance Manager for the California National Guard and California Military Department, a role comparable to that of the CISO. He was chosen for this assignment because he had the correct Department of Defense (DoD) certifications and security was the responsibility of all people working in IT within the U.S. Army. Shortly after stepping into this role, his first major responsibility was to prepare for, and pass, the U.S. Cyber Command, Command Cyber Readiness Inspection. He says, "That was really how I got into information security as a discipline, if you will, because they put me in there. And that was just an assignment for me as an Army Officer. I didn't set out on a career path to become a CISO one day, or even a pen tester or anything like that. I just bounced around the IT profession, largely within the DoD. And because of the level of rigor put on things in the DoD, I had this level of exposure to security."

He continues, "When I came up doing this in the military, the security guys didn't harden servers for you. We were responsible to meet standards that were published by the security team. So, I've been doing security probably my whole career. I had my CISSP before I was officially in security. I was a network operation center manager and the DoD required me to have my CISSP to perform that job, so security was just part of it. For me, the journey has always been different, because when I talk to other people that haven't had that upbringing in security, their experiences are very different with it," explains Margolis.

After working in a number of roles for the Army, California National Guard, and serving as the CISO for the County of Orange, Margolis is now CISO for the Metropolitan Water District of Southern California.

STRONG SECURITY AWARENESS

Margolis believes security awareness is vital to a strong security culture within an organization. He says this starts with embarking on holistic and multi-layered security education, and a strong security awareness program should encourage people to consistently think about being secure, both inside and outside of the workplace.

For example, he says it is important to educate your workforce about small adjustments to their everyday routines such as taking off their badge when they go to Starbucks. To fundamentally instill a security-aware mindset for employees, he suggests publishing threat intelligence summaries around the holidays to tell parents what IoT enabled toys are less secure or educating about parental controls that may be complimentary from your internet provider.

Margolis approaches security awareness with business executives in a more specific manner, one that resonates directly with their responsibilities, goals, and challenges. He comments, "I think there's different levels of education because people need to understand what risk there is to them based on their role, what responsibilities they have in leadership for roles and responsibilities within a holistic security program."

BEST PRACTICES TO CREDIBLE RISKS

Margolis emphasizes the importance of avoiding fear, uncertainty, and doubt when presenting to executives or the board. His advice is to avoid this because scaring people only gets you money one time and runs the potential of your board or executives losing confidence in your abilities as a strategic leader. He says you must educate them on what is considered best practices to credible risks.

He explains, "Make it about risk-based decisions. They're not good decisions, they're not bad decisions, they are decisions that are centered around managing risk to the organization financially and operationally. Because you want to make sure they understand that you understand there is a dollar amount associated with whatever it is you're trying to deal with. Also, there is an operational risk that would then lead into reputational damage and things like that if you fail to produce your product or keep your servers up and running."

BATTLEFIELD MANAGEMENT AND TECHNOLOGY ROADMAPS

To address the clutter of security products, both those already in an organization's environment, and the myriad of options when looking to invest, Margolis believes in a strong strategy of what technologies you are trying to manage and basing your program on a few core pillars. He says one pillar should be leveraging cyber threat intelligence to understand and respond to threats. He views cybersecurity and investing in technology as a paramilitary science in a sense that he is doing battlefield management.

He says, "Cybersecurity is not hierarchical like police or fire, which is commonly associated with paramilitary. But I consider cyber to be paramilitary because you must apply a certain amount of military science to do battlefield management. You must understand who the bad guy is, what their techniques are, how they're going to approach you, and how you're going to defend against them. And then when they do launch their attack, how is that attack managed and how do you respond. Understanding all of that allows me to understand what technologies I need."

Margolis suggests leveraging strategic documentation such as ISO 27001 and 2, NIST 853, the MITRE Attack Framework, and CIS Controls. He explains, "The technologies and capabilities we have are arrayed against an ability to manage part of the cyber-attack kill chain. And the better I can leverage technology to do that, the more easily I'm going to see gaps, because if I start seeing that one technology is doing too many things in that management, then I start recognizing single points of failure. And then I realize I need augmenting technology. So that helps me develop a technology roadmap."

TOP CHALLENGE

"I would say the one of the top challenges for me in the public sector is job classification issues and getting the right people hired into jobs. And this would resonate with the federal government and state government. In the public sector we must deal with job classification constraints. Say I have a job opening and I want to hire somebody to be a SOC analyst. That's a common job these days, but I look at the skillsets for a SOC analyst and I look at my current job classifications. I must try to figure out how I'm going to pigeonhole that into an existing classification. So, some skills that I want, I may not be able to get. That's one thing. I think that's a challenge for a lot of public sector folks. There are ways around it, but it's a challenge."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

KEVIN PAIGE
CISO, FLEXPORT

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 1,600+

ANNUAL REVENUE: $471 Million+

SIZE OF SECURITY TEAM: Undisclosed

At the beginning of Kevin Paige's career in the Air Force, he focused on law enforcement and physical security. He had the opportunity to work with some investigations related to computers, and then was given the opportunity to move into computer operations. During this transition he realized he had a deep passion for technology. While working in technology in those early days, many people correlated his early security work with computer security work, so before he knew it, he was assigned to the network security team. This was Paige's first experience with information security and sparked his passion and desire to follow this path as he progressed in his career.

After leaving the Air Force, he then moved on to government consulting, working on building security capabilities, and later transitioned into a network and systems operations security architect for the Navy and Army. He then became a civil service employee, running data centers and created one of the first cloud-based infrastructure-as-a-service offerings for the federal government.

"Flexport takes a security-first approach on IT and data security. And instead of hiring a CIO, they wanted to hire a CISO with a security-first mindset to make sure that we're making all of our decisions with risk and security in mind, to make sure that we're protecting our data and goods, and protecting our people in a forward thinking manner."

With a desire to leave the public sector, Paige moved on to work at a small disaster recovery startup before joining Salesforce. During his time at Salesforce, Paige helped establish their infrastructure security capability. Paige eventually left Salesforce and worked at MuleSoft as their first CISO, building out security holistically from the ground up for the company, before his current role as CISO for Flexport.

As CISO at Flexport, Paige oversees the entire security function as the organization focuses on their mission of moving freight globally by air, ocean, rail, and truck for the world's leading brands. He comments, "I own IT, physical security, and logical security. Flexport takes a security-first approach on IT and data security. And instead of hiring a CIO, they wanted to hire a CISO with a security-first mindset to make sure that we're making all of our decisions with risk and security in mind, to make sure that we're protecting our data and goods, and protecting our people in a forward thinking manner."

BUILDING A SOLID SECURITY FOUNDATION

In order to build a solid security foundation, Paige emphasizes

the importance of a risk-based approach, strong security culture, motivated team, and robust identity and access management program.

Risk-based Approach. Paige focuses on risk and building a maturity model based on where he is today, and what the path looks like to increase maturity, especially around data security and data protection. By taking this approach he understands where gaps exist, areas of strength, ways to become stronger, and how to prioritize resources, while also tying everything to compliance.

Security Culture. Paige believes in a cohesive approach to security awareness, that makes protecting the organization interesting to all employees. He says, "Making security awareness interesting is very important to me because the security team is always going to be small compared to the company's relative size. We need eyes and ears all around the company that know how to ask the right questions and know who the people are that they need to ask those questions to. Establishing the security culture was my top priority. But it's always a continuous process."

Motivated Team. Paige says hiring team players is consistently one of his top priorities. He explains, "Hiring is hard, there's no doubt, but from my perspective, I like to operate as a team, not as individuals. Depending on each other, communicating with each other, and making it about more than just the technology. Every company in the world needs the same type of security people, but are you treating them like people, are you giving them the career advancements they need? Are you giving them the education? Do they feel like they're part of a team or do they feel like they're just showing up to work nine to five to run their security tools?"

Identity and Access Management. Paige says, "Security begins with strong identity and access management capabilities. Across the company, I took a strong look at making sure that we've got great identity when it comes to accessing IT systems, when it comes to accessing our product capabilities, and when it comes to accessing our infrastructure. Holistically, I wanted to look at how we were doing it, what our gaps were, and then make solid plans to make sure that we're doing the right things. Strong identity and access management capabilities are critical to having a solid security foundation."

MEASURING PROGRESS

"In the very beginning, the easiest thing to do when you're building programs from scratch is really a project management approach. I built a 12 to 18-month roadmap using the V2MOM approach - vision, values, method, obstacles, and measures. And then we hyper focus using Objectives and Key Results (OKRs) for each quarter, based on priority, risks and capabilities, and we measure those OKRs based on project capability to see where we're at and how we're doing," explains Paige.

He leverages this agile methodology to measure where his program is and how they are doing based on the project capability. This enables him to gain valuable visibility around the process in place, tracking the overall security health, and the maturity level over time to ensure they are improving.

Paige values the ability to continuously show progress while continuously improving. He explains, "We have to set good rules and capabilities that we're measuring ourselves against. In security, we must stay ahead of the curve. We must stay at least on par with our technology brethren as they're bringing in these new technologies such as new cloud type capabilities. We have to stay on top from a technology perspective and really understand the technology they want to bring in, why they want to bring the technologies in, what problems they're solving, so that we can really understand the risk and give them meaningful security responses in order to help them."

The Competitive Advantage of Trust

"A lot of the times I don't even use the word security anymore. When I'm talking to business partners, I use the word trust. It's all about trust, right? We want our customers to trust us. We want our employees to trust us. We want our business partners to trust us. Everything is all about trust. Especially if you're a cloud platform or you want somebody to use a new cloud platform or technology or capability. You've got to trust it, and how do you trust it? How do you create that trust? How do we evolve that trust? People are going to use what they trust. If you have a brand that's trusted, if you have capabilities that are trusted, if you have people that you work with who are trusted, that is the key. That is the competitive advantage, right? I worked at Salesforce, and for their CEO Mark Benioff, trust has always been one of his core company values. And I've seen firsthand how a company like Salesforce has built that level of trust with their customers and that's what keeps them coming back. That's what keeps them buying more. Customers see and feel the trust value in all aspects of how Salesforce operates and I believe that more companies will adopt this approach as the future of security because the old-fashioned ways we have been doing security in isolation for the last 20+ years are not effective, it's time to evolve with a trust first mindset."

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

TRANS
FORM
ATION

DECEMBER 2019

K logix

WWW.KLOGIXSECURITY.COM
888.731.2314