FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

JUNE 2016 | DEAR C-SUITE

WWW.KLOGIXSECURITY.COM 888.731.2314

K logix

Earning the right to be confident in Information Security

FEATS OF STRENGTH

BY K LOGIX

JUNE 2016

PROFILES IN CONFIDENCE

FEATURES

LETTER FROM

KEVIN WEST

CEO

TO THINK LIKE A MEMBER OF THE C-SUITE, LEARN LIKE A KID

As another school year winds down, I was chatting with my kids about all they have learned. My fourth grader rattled off how she's continuing to progress in English, Mandarin Chinese and coding, "three languages dad!" It's been 34 years since I was in the fourth grade and things have definitely changed. I thought to myself, "I can't learn another language", and then it struck me – that is not the attitude children have towards learning. Instead of "I can't learn", they are more likely to say, "I haven't learned yet".

It is an important distinction because my way of thinking implies that I have a finite amount of knowledge, and learning a new language will never be in my repertoire. But, by acknowledging they, "haven't learned yet", children are open to the opportunity to acquire that knowledge. It turns out, openness is all we need to be adept learners of second languages, whether it is English, Mandarin, or more relevant to our industry, the language of business. In other words, when it comes to learning new skills, we should think like kids.

LEARNING ON THE MOVE; MAKING STRIDES WITH THE C-SUITE

In this issue of *Feats of Strength* we focus on the CISOs relationship with other senior executives in the company. We examine the roles the CFO, CEO, General Counsel and others who play in information security decisions. What do they need to know, and how can the CISO best communicate with them? In our article about the CFO relationship with the CISO, and in the Boardroom advice column, we hear these executives come back to the same theme – CISOs need to speak to us in our language, about the things we care about.

These executives need the CISO to provide a better understanding of information security, but they want that education to be set in their comfort zone. As you will see in our article "How to Talk Security", executives are asking us to speak in business language when we present risk factors, and make requests for security programs, processes and technologies.

So, while the rest of the C-Suite is working to acquire the knowledge they need about information security, we need to work harder and smarter to learn their language. This will improve collaboration, communication and overall security posture, while also raising the CISOs profile in the company.

SPEAKING THE LANGUAGE OF BUSINESS

In this issue you will read about tying information security to revenue, shareholder value and time to value, all the things your C-Suite cares about. We will ask you to consider that maybe the way we have approached security conversations and decisions in the past marginalizes us because it prevents CISOs from having an impact on the things that make a business successful.

Instead of the old approach, let's try to focus our conversations with other executives on the things that matter to them. We know that list includes revenue (information security can be a competitive differentiator in a lot of industries), shareholder value (because information security can reduce business risks and avoid costly fines and penalties), and time to value (reducing the time between technology purchase to when it is demonstrating value).

While we are making strides, the C-Suite is asking us to do more to communicate in business terms. It might just be as simple as this: in order to transition from technical leader to senior business executive we need to remember to learn like a kid.

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.

HOW TO: TALK SECURITY

CISOs must speak to every part of the organization, and sometimes it can feel like each part of the organization is speaking their own language. As security professionals, we often fall back on our own tech-centric jargon. This makes meetings less effective and less successful. We have to admit, some members of the C-Suite will never come around to technology-focused language. For CISOs to be most effective, they must speak in the terms their C-level colleagues prefer. Here's a quick (not exhaustive) primer:

The CFOs goal is to ensure that budgeted spending results in costs savings or increased revenue. They frequently use ROI as a key component of reporting, yet this may be hard to measure in information security. CISOs must find another measurable solution, such as Key Performance Indicators, to make their case.

CISOs must prepare themselves with suggestions for measuring the success of an investment when engaging in a budget conversation with CFOs.

When CISOs highlights information security's role in growth products, like mobile banking in the financial services industry, CFOs see security positively impacting the bottom line.

CISOs must help CEOs understand the long-term impacts of not adequately protecting data.

- Talk about the resiliency of customers – will they stick with us through multiple attacks?
- How will the company's financial ledger be impacted by civil law suits resulting from PII being compromised?
- Price wars – With access to the company's secret sauce, can competitors and Nation-States produce the same product more quickly and at lower costs?

Customers, especially those in heavily regulated industries like healthcare and finance, are becoming savvier about security. In that regard, security can be a competitive differentiator that creates customer value. By building security into products and services, companies may increase their value to customers.

- Collaborate - Show value and collaborate. Ensure security is involved in the program from the get-go and focus on building out security-aware processes.
- Weigh security investments against risks – Be certain technology protects assets and outweighs its impact on performance. Articulate the reasons why security is needed in business-friendly terms to all users.
- Test, test, test - Understand a security technology's impact on performance before roll-out.

The role of technology in business requires a tight partnership between the CISO and the CIO. When talking about digital transformations with the CIO focus on:

- Creating secure programs and processes from the beginning – security should be built into innovations – everything from new products to process improvements.
- Helping the CIO understand security within cloud-based solutions – be their partner in evaluating vendors.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

KEVIN BROWN
CISO, BOSTON SCIENTIFIC

HEADQUARTERS: Marlborough, MA

EMPLOYEES: 24,000

OPERATIONAL REVENUE: $8.1 Billion

"I have strong knowledge and experience in cybersecurity, but I also have a business background, managing significant cybersecurity profit and loss portfolios," said Kevin Brown, CISO at Boston Scientific. "That combination helps me make a difference in the CISO role at Boston Scientific."

Brown started his information security career with the Federal Government as a U.S. Navy officer where he worked with the National Security Agency. After leaving the Navy, Brown was an early member of SAIC's startup information security division, where he spent seventeen years growing the business unit to $180 million in annual revenue. As a Senior Vice President at SAIC, and later Vice President at Raytheon, Brown was responsible for profit and loss organizations providing information security services, technologies, products and consulting to federal government, commercial and international customers, particularly in support of CISOs.

After twenty years into his commercial information security career, Brown decided it was time to get back to his cybersecurity roots and work internally as a CISO. Brown wanted to work for a company that was making a difference in the world, and Boston Scientific, with its medical device innovations transforming lives, exemplified a strong fit. With ten months as CISO under his belt, Brown possesses a strong will to expand his program while working closely with other business departments.

DATA PROTECTION AND A TRUSTED SECURITY PARTNER

Shortly after his arrival at Boston Scientific, the company launched a global Data Protection initiative led by the Chief Security Officer, Senior Counsel-Global Privacy & Data Protection, and Brown as the Chief Information Security Officer. The leadership team conducted a cross-functional and stakeholder data review identifying location, owner(s), classification, protection, access, and sharing/collaboration in order to ensure that the company's comprehensive data protection strategy remains robust. As part of its' initiative, the company also established a formal Global Data Protection Council.

The Council is an important partner and channel for Brown's team in many ways. He says, "Through the Council, the security team is more easily connected across the corporation not only for ensuring the protection of Intellectual Property and personal information, but as a way to further enhance our security awareness efforts.

The cybersecurity team and Council have aligned on key initiatives such as threat intelligence, privacy, forensics, and employee education and awareness."

Through coordinated efforts with the Council, Brown and his security team work actively on partnering and engaging various organizations throughout Boston Scientific. "As the CISO and member of the Global Data Protection Council, I meet regularly with the leaders within the businesses as well as key partners such as Legal, Human Resources, R&D, and Finance, for example," Brown relates, adding "but the real partnership comes from the interaction my security team provides with those same organizations at their level." Brown describes this interaction as recruiting "Security Champions" throughout the company which act as primary points-of-contact who the team works regularly with in such areas as awareness and training, alerting, and support. "Top down leadership is a necessary start, but fostering an enterprise-wide culture of awareness and ownership is really the best way to ensure engagement," Brown believes.

MEDICAL DEVICE CYBERSECURITY INTEGRAL TO PATIENT SAFETY

In support of Boston Scientific's Digital Health Initiative, Brown and his security team have focused efforts on ensuring security around the company's products and medical device components and applications, resulting in a clear competitive advantage for the organization. "Digital Health is a strategic priority at Boston Scientific and several things we are doing in security will be differentiators for the company. We always ensure our products meet requirements for medical device security, but we are going further than that. There is so much information that can be housed on medical devices, or accessed through medical devices. It is not just protected health information (PHI) or personally identifiable information (PII). Hackers and cyber criminals will exploit any access point to get to a hospital's data or any other system the device may interconnect with, and if left unsecured, a medical device connected to a hospital network may create an access point. While many are focused on just the devices, we are also looking at what supporting infrastructure and applications can be used to pivot into our devices or a customer's network. We want our customers to be comfortable adopting our entire ecosystem, not just our devices. We want to build upon our trusted partnerships. Those are the types of things we are thinking about with our medical device security program. Ensuring security at those points can be a differentiator for us with the hospitals and healthcare providers."

> "Top down leadership is a necessary start, but fostering an enterprise-wide culture of awareness and ownership is really the best way to ensure engagement."

The medical device initiative requires Brown and his team to work closely with the research and development team, which continues to demonstrate a strong commitment to security. According to Brown, the process has gone smoothly because his own team is working collaboratively and openly. "We don't say 'no you can't do that'. We work to find a secure solution in support of the business. Of course, patient safety and confidentiality is always paramount."

TALKING CYBERSECURITY TO THE BOARD

Brown briefed the Boston Scientific Board of Directors after six months on the job. "It was a fantastic opportunity to give the BOD and several members of the Executive Committee an assessment of the security posture of the company, provide insights into what is happening in the cybersecurity world, discuss the data protection initiative and expound upon the company's strategy," Brown says. He adds, "There is a real importance in working with our executives on security. In today's world many governing bodies, including the SEC, are holding executives and BODs accountable for understanding security threats and risks to their organization."

Brown is researching the best way to leverage current and future tools to clearly communicate with leadership in a concise manner. In support of that, Brown has begun the process of employing solutions that can not only ingest and correlate information and minimize manual processes, but also provide customized dashboards that can present relevant information at the appropriate level. "Whether it is third party vendor management, incident data, training metrics, or compliance information, there is a value in customizing and providing a continuous flow and access of information to the various partners and organizations within the company," Brown states.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JAY LEEK
CISO, BLACKSTONE

HEADQUARTERS: New York City, NY

EMPLOYEES: 2,190

ANNUAL REVENUE: $7.4 Bliion

"I believe that we have a CEO-led information risk and security program," says Jay Leek, CISO at Blackstone, a New York based asset management firm. According to Leek, a CEO-led information risk and security program means Blackstone executives contribute to a strong top-level commitment of protecting company assets and information. Leek became Blackstone's first CISO four years ago due in part to support from senior management in the firm, who were the major drivers in creating the position. During this time, senior management clearly identified security as a priority for the company, something that remains a top priority today.

Leek reports into Blackstone's CTO, who reports to the CFO, yet still possesses ample visibility with other senior leaders throughout the firm. When *Feats of Strength* spoke to Leek he had just come from a regular, standing meeting with Blackstone senior leaders. In that meeting Leek presented the three year security plan for the company. Leek says Blackstone senior management's commitment to security comes from understanding the value of the firm's information. Leek says, "My senior management feels confident in where we are, but remains on guard about the unknown. The key takeaway is that we can never slow down. In fact, it is how can we speed up? We are constantly challenged to push the program as fast as we can without breaking the organization. We have a responsibility to do our best to protect the firm for our shareholders and limited partners."

Since Leek has regular interaction with senior management, he has developed a proven approach to effective communications. "Facts," continues Leek, "We weave in qualitative analysis about our company, and support that information with external data points. Our program is focused on situational awareness, intelligence-led information security and risk management. With regards to threats and incidents, we need to know who, why and how they are attacking us. We need to know their motivations – that requires intelligence gathering and situational analysis. So we educate our senior leadership on this information and approach, and back it up with facts. This approach helps us frame the problem on a continuous basis and helps the executives wrap their heads around it."

Leek states that part of building and maintaining an executive-supported security program requires thinking like business people, specifically your company's business people. "If our senior leaders think of me as just 'the security guy' then I have failed in my mission. I believe that our leadership team views our security team as business leaders who simply happen to know a little more about security than others in the room. This approach allows us to function as

Mentors and a Network of Peers Help Leek Make Tough Decisions

Leek is fortunate that he has access to a large network of security professionals, which he has helped to hire at Blackstone's portfolio companies. Accordingly, Leek serves on the Board of some early stage security companies, so he has multiple opportunities to engage with security leaders. One of Leek's mentors is Jim Routh, the CISO of Aetna who was also featured in *Feats of Strength* last year. Leek says, "I have so much respect for Jim. I have consulted with him, in an advisory way, before I have made big steps in my career. When we see each other, we compare notes and collaborate. I have a lot of senior level security executives like Jim in my network and am both grateful and fortunate for this. We make a concerted effort to get together on a regular basis and compare notes. We are a collaborative community so no one has to reinvent the wheel. We learn from each other's successes, and yes, failures, too."

trusted business advisors in conversations about cyber risk. We must be thoughtful in how we frame that risk in regards to all the other risks across the firm."

Retaining a sturdy business-focused approach permits Leek to consider security through the lens of a financial business leader. He asks, "What is the impact of this security function on the business use. How does the business user feel? Does it impact their work? What is the benefit the business gets from this security control? Is it worth it in the end?"

With security as a central priority for the company, Leek acknowledges the opportunity for security to be considered a competitive advantage for Blackstone, even though the company does not talk about security externally very often. "The alternative asset management community is close knit. There may be eight or nine firms that have CISOs. We are very open in communicating across all these firms and believe this is an important advantage. We also educate our limited partners on what we are doing from a security perspective and why we are doing it. They ask about business continuity and disaster recovery, and we go beyond that to explain information security risk management. It sends a positive message to our limited partners. These limited partners are making 15-20 year financial commitments with us. They want to know our strategy and our culture to make sure their investments and information is safe." Leek believes their security program can be a differentiator in many of those conversations.

A "NO EGO" POLICY MEANS GOOD SECURITY IDEAS CAN COME FROM ANYONE

"I believe that over the last 20 years, as an industry, many of us have done a disservice to our security programs with complex frameworks and too many controls. Security needs to be described simply so that everyone outside of the security and technology teams can also understand it," said Leek.

He continues, "Others [in the organization] can come up with security ideas that can make your business better when they understand security's objectives and necessity. The Blackstone security program is not my team, it is the firm. We support a culture that understands security. Our program is not perfect; we need to get better, but we have been building this culture of education and responsibility for four years. Now we have people from across the company weighing in on how Blackstone can be a safer place."

That collaborative, open environment starts within Leek's team, which includes dedicated internal security personnel, an outsourced SOC and numerous other personnel who help support security functions in other areas of the technology group and in regional offices. "We have a 'no ego' policy," said Leek, "I don't believe in a hierarchy. I do have a deputy CISO to help scale our program, but we maintain a flat organization and a team of equals. There is implicit trust between us. Every now and then someone needs to make a decision and that is what I am here for, but we work openly and collaboratively as a team. Communication is pervasive across our team. Everyone knows what is happening across the program with a few exceptions, for things like sensitive investigations. Everyone is held accountable and empowered to make decisions."

GROWTH AND EDUCATION ARE PRIORITIES FOR THE YEAR

Leek says his team works continuously at educating the most senior level management on the importance of security, but his team must focus the firm as a whole. It is everyone's responsibility to help protect the firm, and it is our job to empower them with the knowledge on how to do it. "We try to train everyone without being a nuisance. We want to make sure everyone understands security's purpose and are following processes not because they were told to do so, but because they understand the value it brings to Blackstone."

Leek's other goal is internally focused on his team. He wants to make his team operate at twice their efficiency scale of physical capacity, while working fewer hours. "I am not talking about Six Sigma, rather just automating manual functions and becoming one thousand times more efficient as a result." They are constantly striving to get closer to this goal.

SPOTLIGHT ON: MICHAEL DECESARE

CEO & PRESIDENT, FORESCOUT

Michael DeCesare shares his thoughts on the Internet of Things, CISO challenges, the current state of IT security solutions, and more.

HE HAS A THING FOR THE INTERNET OF THINGS

"It has taken us 25 years to get to six billion "things" connected on this planet. Gartner predicts there will be at least 25 billion connected things by 2020*, so we're talking about an additional 19 billion more devices connecting to networks within the next four years," says ForeScout CEO and President, Michael DeCesare. As an industry veteran, DeCesare brings passion and a forward-thinking approach to ForeScout, a leading provider of agentless network visibility, control and multi-vendor orchestration solutions that help enterprises prevent and respond to cyberthreats while unifying system-wide security management.

DeCesare knows that managing the Internet of Things (IoT) devices that find their way onto corporate networks may seem like a daunting task. After all, IT security is already extremely challenging. But organizations must ensure that they are not opening themselves up to more attack opportunities. Digital assets must be accounted for and secured at all times. Furthermore, the issue of visibility is key when creating a truly secure network. In a recent Network Visibility Survey of 400 IT and security professionals conducted by research firm Frost & Sullivan, respondents consistently expressed concerns about specialized security solutions working in isolation and creating network blind spots. DeCesare explains how ForeScout addresses this issue with technologies that provide visibility into devices as they access the network, as well as continuous monitoring.

"We are the dominant player in IoT security. Our secret sauce is that we are agentless, which allows our technology to discover and monitor devices—even if those devices don't have security agents," says DeCesare. ForeScout's agentless approach enables its flagship product, ForeScout CounterACT®, to see devices on the network whether they are managed or unmanaged, known or unknown, PC or mobile, and embedded or virtual. CounterACT® can

> "If every time someone stayed at a hotel they were required to download that hotel's own AV client before they could access the network, it would never work. It's the same thing in an IoT world, where it's just not practical. We have to be able to make decisions on what is good and what is bad without requiring a footprint on those devices."

DeCesare Comments on the Current IT Security Solutions Market

"If I'm a CISO in today's society, there's a delicate balance when it comes to choosing technology vendors. The reason organizations tend to be more open to using startups in the security space is the clear advantage of the unknown. Hackers practice over and over again how to break in to the "big names" in the industry, but the chance of them trying this on all 1,000-plus security products is low. However, with this approach comes risk. I walked around the RSA conference floor and realized that many of these startups were not going to be around in two years. CISOs must balance where they want to invest paired with making sure the vendors they invest with are not going to be out of business in a few years. I'm proud to say we did 126 million in revenue last year, grew 77 percent and have proven to be a cash-flow positive company." We are a trustworthy choice for CISOs. In fact, many of the world's largest companies and government organizations now use ForeScout technology."

identify, classify, authenticate and control devices, including IoT endpoints—agent or no agent.

DeCesare goes on to explain how CounterACT® continuously scans the network and monitors the activity of known, company-owned devices as well as unknown devices such as personally owned, rogue and IoT endpoints. And, unlike systems that simply flag violations and send alerts to IT and security staff, ForeScout enables IT staff to automate and enforce policy-based network access control, endpoint compliance and mobile device security.

YOU CAN'T SECURE WHAT YOU CAN'T SEE

"My message to CISOs is that you can't secure what you can't see," says DeCesare. "We go into accounts and ask them how many devices they think are on their networks. Sometimes they can be off by 300 percent and not know about two-thirds of what is on there. The fact is, most CISOs cannot guarantee to their CEO that they know how many devices are on their network, something ForeScout quickly and accurately answers."

PERSONALLY ACCOUNTABLE CEOS

DeCesare believes the relationship between a CEO and CISO must be airtight. He feels strongly that CEOs must hold themselves personally accountable for confidential customer and employee information that is entrusted to them. Moreover, he's convinced that that accountability begins and ends with strong ties to the CISO and IT department. "By working together with the CISO and having open lines of communication, CEOs and the companies they represent can take on the challenges of the evolving threat landscape," DeCesare says.

* "Predicts 2016: Security for the Internet of Things," Gartner Research Note, December 2015

See. Control. Orchestrate. These three words sum up the foundational intelligence and functionality of ForeScout CounterACT®. By not requiring software agents, CounterACT® lets you see devices the instant they connect to a network. It enables higher levels of control by allowing, denying, or limiting access based on device posture and security policies. And, in tandem with other ForeScout technologies, CounterACT® provides the orchestration and integration for sharing real-time intelligence across security systems and infrastructure, thus creating a unified network security system.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DR. DAVID REIS

INTERIM CIO & CISO, LAHEY HEALTH

HEADQUARTERS: Burlington, MA

EMPLOYEES: 15,000

ANNUAL REVENUE: $2 Billion

APPLYING AN INNOVATION FRAMEWORK TO INFORMATION SECURITY

"Trends in the security industry change so frequently we need strategies that help us deal with the near term while also preparing for the future," says Dr. David Reis, CISO at Lahey Health. "We have to get a step ahead. There are specific frameworks to use to get through that process. The Kellogg [Northwestern School of Business] Innovation Framework resonates really well with me. It helps you develop an innovation engine for reacting to today and preparing for the future."

Many CISOs regularly leverage frameworks and controls such as NIST and the Top 20 Critical Security Controls, however there is a lack of CISOs who implement specific business approaches. Dr. Reis fundamentally aligns with the Kellogg Innovation Framework to cohesively run Lahey's security program. Dr. Reis explains how maintaining an eye to innovation helps enable a strong competitive advantage and makes a lasting impact on organizational revenue.

"The Innovation Framework is qualitative and mathematical in that it can help you track your progress towards creating a security program that brings value to the organization. Through this approach we look at what is going on today, and what happened in history. We review how breaches occurred industry-wide. What has changed over time and what has caused that shift? This allows us to identify future indicators and prepare for them in advance. In security, it is counterproductive to look out more than a year but we can be ahead of this week's malware."

The security program at Lahey facilitates business programs by moving past "blocking and tackling". Dr. Reis accomplished this enablement by demonstrating how information security can drive innovation and evolve to become a high-functioning service. An example of this is the robust role of security in connected health, described as "telemedicine" with patients and other providers, where doctors and patients can interact outside of health care facilities.

Lahey demonstrates a cutting edge technology, delivering healthcare outside of the four walls of treatment rooms and in an easily accessible and secure way, as a direct result

of the information security program. Dr. Reis says, "We are giving patients access to providers who they would not otherwise be able to access. For example, someone may be in the hospital with a chronic illness, and that person would typically have to come back to the hospital for on-going visits. This might be the appropriate treatment plan for some patients, but others would benefit from telemedicine. Our security team is driving the effort to extend the patient portal and video conferencing technology to connect patients to providers for follow-up after discharge without having to come back for an in-office visit. This is novel for healthcare."

Dr. Reis understands the significant role information security plays in an organization and acknowledges a potential for impact on revenue. While he stops short of saying the program is a revenue generator, he does believe security enables revenue. He comments, "I can show you how we have enabled millions of dollars a year in new revenue because we have securely opened up our services and access to populations that we could not reach before."

Dr. Reis also recognizes that revenue impact is strengthened by support from Lahey's business leaders, including the CEO, CFO and Board. Dr. Reis says, "The organization has given IT security a lot of resources and we are able to show our value. It can be hard to show ROI in security, so I focus on value. Kellogg teaches that value is equal to service plus quality divided by cost. At Lahey, our team is relentlessly focused on proving value."

THREE COMPONENTS TO EXTEND SECURITY'S IMPACT

To establish the security practice as a business enabler within Lahey, Dr. Reis focuses on communicating without security jargon, acting as a trusted advisor, and resisting temptations to advocate through Fear, Uncertainty and Doubt (FUD).

• Communication – Dr. Reis believes effective communication is integral to developing a satisfactory relationship with the Board and senior organization leaders. He learned the language of business when he got his MBA, and now easily translates security requirements and needs into financial and business conversations. "You have to speak the same language as the executives," he says.

Communication skills were fundamental in the early 2000s when Dr. Reis got his start in information security. He learned this lesson at a large, regional audit accounting firm where he performed internal and external audits. He says, "That is where I learned how to eliminate security jargon from my presentations because you could not get past the audit partners with security jargon in your report. That became a Rosetta Stone for me. I already knew about security, now I had a new language to communicate it to executives."

• Never Say No – "Executives have their trusted advisors, the people on the team they go to in order to get things done, and you have to do the work to join that circle. "My motto is never say no. Instead we say 'yes, and here is how'." By saying yes when executives or others in the organization want to implement a new tool, or introduce a new process, Dr. Reis engenders collaboration and positions security as a business enabler. To do so he must understand the team's business goals and objectives. Then the necessary controls may be put in place to make the process work in a secure manner.

• Never Promote Fear, Uncertainty and Doubt – Dr. Reis advocates for security by talking about pragmatic approaches and security's impact on positive business outcomes. He focuses on risk management and incidents in the company, and the industry, that can impact revenue. Sometimes, the Board will ask questions related to incidents in the industry, but Dr. Reis works hard to steer the conversation away from FUD. "What you present is as important as the fact that you are in the Boardroom presenting in the first place. You have to establish credibility as a business thinker. This is developed overtime. We can now anticipate the questions our Board will have and proactively address them. This allows us to lead the conversation and helps establish confidence in our program."

The First 100 Days

Dr. Reis has advice for new CISOs and says, "Gartner has a great CISO Framework for the first 100 days. The most important thing is to engage the leadership population and to understand at a general level what is working and what is not within the business. Ask, "What can I influence?" You can gain credibility by delivering on things that address specific pain points, even if they are tangential to security." Dr. Reis suggests that by establishing yourself as a business partner who can get things done you gain flexibility and leeway to implement vital programs.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

BRIAN HAUGLI

VP & CISO, THE HANOVER INSURANCE GROUP

HEADQUARTERS: Worcester, MA

EMPLOYEES: 4,800

ANNUAL REVENUE: $5 Billion

ELEVATING THE CISO ROLE AT THE HANOVER INSURANCE GROUP

"I report to the Chief Administration Officer (CAO), as do the CIOs for all of The Hanover's lines of business. This was really important to me when I took the position," said Brian Haugli, who is ten months into his role as CISO and Vice President at The Hanover. "This reporting structure is incredibly valuable. I participate with the CIOs in discussions around efficiency and operations; my opinion is valued equally. When I speak to CISOs in other companies who report to CIOs they tell me they have the problem of having to defer to their CIOs regarding those kinds of discussions and decisions. I don't have that issue."

Haugli's boss, the CAO, was hired just four months before Haugli, and highly values the role of the CISO. This support gives Haugli tremendous confidence in his ability to evolve the security program at the company.

With executive-level responsibility and visibility, Haugli has regular access to the company's leadership. "Information security is critically important at The Hanover. Maintaining security around the data our agent partners and their customers entrust to us is essential. With that in mind, I meet monthly with the CEO to go over operational security areas, security posture, and on-going initiatives," said Haugli. "His interest in security and support around making our security initiatives more effective makes my job much more rewarding."

ASSET OWNERSHIP AND RESPONSIBILITY

"I get really solid questions about The Hanover's security posture from the members of our leadership team. They want to know what we are doing, what is going on in the news, and what the global picture is. They want to talk about business risk and take that into account. It's an open dialogue that is influenced by our strategic business goals," said Haugli.

"We talk a lot about asset ownership, and understanding what is most critical to the business

units. We look at the systems and processes that are revenue generating for each line of business," said Haugli. "They want to make sure our technical investments and capabilities align with business needs."

When Haugli speaks to the business units about security he focuses on two areas – asset ownership and general security awareness. "I am a big proponent of establishing asset ownership," Haugli reiterated. If I am looking at a network component, I want to know who owns it. That person needs to take responsibility for what is on the system and ensure systems and processes are secure. If no one takes ownership of a system it is very difficult to make positive changes to it, and it probably should not be in the technology portfolio."

Haugli uses education and awareness training to heighten awareness and change behaviors by employing practical applications of security best practices. "I use a lot of analogies to educate about vulnerabilities and the need for patches and security changes. I say, 'Just like you do not want your kids' friends to be playing computer games on the computer that you do personal finances on, you also want to limit access to your systems at work.' We want to be certain that access privilege is given only to those who need it."

BUILDING A TEAM AND A ROADMAP FOR THE FIRST 18 MONTHS

Just ten months into the job, Haugli has just begun the transition from what he describes as "unboxing the company" to creating a strategic 18-month plan to strengthen the foundational aspects of network security and vulnerability management. While Haugli's background is in the Federal Government, the learning curve has been minimal and he is quickly developing an understanding of the network, people, and organization.

"I am growing my security team internally and I have hired a new Director for Governance, Risk, and Compliance who, like me, came from a government background." He also created and hired a dedicated Manager of Training and Awareness Outreach. "His entire role is focused on the human element of the company. Everything is about the employees, in order to train them and make them more aware."

During the hiring process, Haugli approaches candidate searches by focusing on skill sets and overall ability to adapt. More importantly, he believes there is not a "one-size fits all" in information security. For example, the manager Haugli hired to perform security training was a math teacher with a Masters in Psychology, resulting in an impactful team member with the ability to better understand user actions and teach new behaviors. He is able to take feedback from operations about what they are seeing in terms of security issues and go talk to the employees responsible for the asset and hash the issue out effectively. He is able to understand their process and work with them to make the process more secure."

"Strict hiring specifications can often preclude really solid candidates who would perform well in specific roles. I will look at the person who might not fit into a corporate workspace and see if they are the best person to hunt for malicious activity on our network. You have to understand and evaluate specific skill sets against the job function."

Revenue Impact of Cyber Insurance

"Insurance is one of the few sectors where security has a clear opportunity to impact revenue," said Haugli. "I cannot think of how a manufacturing firm or a retail company can empower a CISO to drive revenue. But in insurance there is a clear need to enhance our cyber security insurance program and that takes insight from Information Security and a solid understanding of risk management practices. At Hanover, I have been working with a specialty line of business on improving risk management and bolstering our capabilities around cyber insurance." Haugli says Hanover has several different cyber security products but what the industry really needs is a uniform national standard to measure risk against in offering these insurance policies. "NIST is one of the best standards to come out over the years, and is a great first step in the right direction."

Getting to Know the CFO

The CISOs Best Friend in the Boardroom?

Much deliberation has been given to the question of where the CISO fits in an organization. Who should the CISO report to, and why? According to a study by Global Risk Advisors, currently 40 percent of CISOs report into the CIO, and 22 percent report into the CEO, so much of the industry debate has focused there. However, 8 percent of CISOs report into the CFO, and that is the relationship we will focus on now. Even if the CISO does not report into the CFO directly, most CISOs have a dotted line into the finance department, and at a minimum most CISOs partner closely with the CFO on issues related to risk mitigation and data protection.

In fact, the CFO can often be the CISO's best friend and biggest cheerleader. After all, Bank of America's security department did not get a blank check for security in 2015 without the CFO being on board with their efforts. The CFO in any company has a unique interest in information security both because of their fiduciary responsibility to protect revenue and their role as a steward of data.

The 2015 Deloitte CFO Signals report states that 25 percent of CFOs feel their organizations are insufficiently prepared for cyber-attacks and malicious threats. So, we know the CFO is worried about information security. But, to be clear, most CFOs do not want to take ownership of the information security function, and that is the most likely reason only 8 percent of CISOs report into the CFO. "I haven't met a CFO who enjoys having information security on their plate," says Nick Araco, CEO of the CFO Alliance. "Most CFOs do not want the CISO to report to them. But they do want to create a collaborative culture across the C-suite to address the flow of data in general and data security in particular."

Focus on Big Impact Risks to Keep the CFO Engaged

Valerie Rainey, CFO of INTTRA told CFO.com that, "It is the CFO's responsibility to keep cybersecurity issues top of mind for the executive team, which is always dealing with other 'fires of the day'. You [the CFO] have to make sure the company doesn't lose sight of the fact that this very strategic enterprise risk needs to be

What Keeps a CFO Up at Night? Economic Volatility, Over Regulation and Cyber Attacks

According to Deloitte, which publishes a quarterly CFO Signals report on CFO opinions and concerns, "cyber-attacks have become a fixture on the list of CFOs' most worrisome risks, which includes perennial macroeconomic factors, such as economic volatility and overregulation."

addressed on an ongoing basis. It's not like you can put a plan in place and you're done. Hackers are becoming more sophisticated all the time."

In other words, the CFO understands, or is beginning to embrace the idea that they have a stake in information security. This reality makes the CFO a good partner for the CISO. But first, CISOs must make certain that they are communicating at the level of the CFO.

When Rainey tells CFO.com that IT executives may not be effective in articulating the impact of business risks, she is repeating a critique that information security executives have heard before. She says the CFO should "focus on risks that have a high likelihood and a big potential impact on the business, whereas IT people will often say that every risk is important."

To get the CFO's buy-in, the CISO has to address this concern. CISOs must make sure the risks they identify and prioritize are in-step with the company's critical business goals. This ensures security can have maximum impact and will help the CFO view CISOs as executive partners, not technical managers.

By committing focus to the risks the CFO has identified, the CISO can gain a high-level executive partner advancing the information security program at the Board level. David Rubin, CohnReznick Risk and Business Advisory National Director is quoted in BOSS Magazine saying that, "CFOs are better equipped to respond to the questions and concerns of their Board of Directors and shareholders", once they have a "keen understanding that cybersecurity is more than a set of preventive technologies. It is a comprehensive set of methods, policies, and strategies designed to protect major assets."

Lesson Learned from Finance: Collaborate, Do Not Control

In addition to the shared interest in risk management, there are two other commonalities between the CFO and CISO. The first is organizational. The finance department and the security department are unique in that their programs do not function in silos; by nature finance and security impact all other departments. This means both the CFO and CISO can potentially wield out-sized control over the other departments, which can negatively impact perception and willingness to collaborate. The CFO, of course, has budget control – investment does not happen without the CFO approving it. At the same time, the security department also has the capability to impact productivity, negatively or positively, through security controls.

Araco is speaking about CFOs when he says, "in general we much prefer to collaborate rather than control." He says, "The finance department is responsible for putting processes and standards in place related to how data is used within the company. In this way, the finance department has an impactful role across all departments. Finance brings structure to organizations." Does this sound familiar? The CFO's role is a lot like the CISOs role. There are shared experiences and clear opportunities to align in establishing processes that emphasize collaboration over control.

Lastly, Araco points out that by nature, the CFO and the CISO may be more comfortable with each other as both are likely to be introverted, and more analytical than other members of the C-suite, such as the CEO and head of sales or marketing. While there is no hard data to prove the security professionals and CFOs are introverts by nature, it is true that the CFO appreciates black and white, numbers-focused reporting. While a CISO cannot always show return on investment or impact on profit and loss, the CISO can report on key performance indicators – such as threats detected and remediated. These types of reports, when tied back to risk mitigation can go a long way in proving value to the CFO.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JP SAINI
CTO, TRC COMPANIES, INC.

HEADQUARTERS: Windsor, CT

EMPLOYEES: 3,800

ANNUAL REVENUE: $646 million

JP Saini has held the position of CTO and Head of Information Security at TRC for past 8 years, a national engineering, environmental consulting and construction management firm. In that 8 years he has evolved the Information Security program with commitment from the CEO and the CRO, and with a lot of hard work and effort put into the people-side of security. In fact, Saini says that his biggest challenge in business has been change management. “People tend to dilute the challenge of change management. It takes effort to effectively engage your target audience – employees, partners, clients, or the Board – to embrace changes in behavior.” While Saini lists change management as his biggest challenge, he has found success in the process.

> “You have to invest in the people and prove the value of Information Security”

Success came because Saini put a premium on the human elements of Information Security. He says that it is important to put a few layers of security, including technology and processes around critical assets, but the most important step is securing the human element. “Many of the security organizations spend a lot of money on technology and process, they forget about the people,” says Saini. He believes this is a mistake. “You have to invest in the people and prove the value of Information Security.” This will engender change and make the organization more willing to embrace it. Saini says CISO’s must, “Find a way to continually present the outcomes of security efforts so that the credibility of the program is not lost.”

Showing results includes tracking annual and quarterly progress via reports for the Board, but is better explained to the company as a whole with anecdotes and progress updates. Saini says, “At the employee level we continually highlight any progress and updates that we can in the employee newsletter. Now, we cannot disclose every single detail to our employees because of employee turnover and confidentiality, but we are constantly communicating

at a high-level about the progress being made. We talk about ease-of-use, things to be aware of, and recent successes. The mind does not know what the eye does not see, so we put as much information as we can in front of people."

Saini notes TRC's employees' willing adoption of self-implemented mobile device management as an example of effective change management that improved security. "We allow up to five devices – whether they are TRC provided or not. We put the instructions for enrolling on intranet, and people use it. If you make information meaningful, accessible and visible, your audience will respond to it."

As Saini considers change management one of his biggest challenges, it is notable that he considers empowering TRC's people as his greatest success. Saini says, "Beautiful things happen when you empower people, including your team, your peers, and your board. Empowerment does not mean that they have access to the cruise missile push button, but empowerment does give them access to information, and the authority to make smart decisions. Within the IT department at TRC we have empowered our people to be confident employees and we have seen great results, including high retention rates. People raise their hands to lead new projects and initiatives."

WORKING WITH LEADERSHIP TO IDENTIFY SECURITY CONCERNS

Saini reports into the CFO who is also the Chief Risk Officer. He also works regularly with the company's Senior Management team and Practice Leaders to ensure a security-focus in all projects that impact customers, partners, and employees. Saini reports both the CFO and the CEO are proponents of Information Security. The CEO is very interested in engaging in security discussions. Recently, TRC started a program to evaluate the Information Security strength of TRC's many subcontractors. Leadership came together and decided that as the company strengthens its' own security posture, it must also look at the posture of its' subcontractor eco-system, because anything those companies do as agents of TRC impacts the organization. Saini has a leadership role in helping to evaluate and ensure subcontractor performance as it relates to security.

A FUTURE-FOCUSED APPROACH TO SECURITY

TRC is a company focused on growth and expansion. As a result, Saini spends a lot of his time evaluating and reporting on risks related to acquisitions and effectively combining and acquiring organizations into the company in a secure manner. The company is pursuing an ISO 27001 certification, which will ensure it meets international security standards. "ISO 27001 will allow us to effectively scale as we grow beyond the United States. We will not have to worry about changing our security practices to meet international standards," said Saini.

BUSINESS ACUMEN ENSURES MORE EFFECTIVE SECURITY

Saini believes business expertise and acumen are becoming critical to effectively run Information Security programs. Saini believes business skills can be learned outside of the classroom as well. Saini says, "Business experience is a relative term. I do not think a business school will give you all those skills. You need to have the right level of business experience. You need to have a good mentor. Plus you need to have some formal training in understanding the basics of business. You can become a CISO because you are a great techy; to be a great leader you have to harness a few skills from the business side."

The important thing is that CISOs understand how business functions so they can align security to business priorities. Saini says, "In my view, if you cannot run your own business, you cannot help anyone else run theirs. You have to be able to run any segment of an organization as a business. With a purely technical skill set it can be easy to get stuck in your own world and become too focused on the best technology or best certifications. You have to go beyond technology, process, and people and take a business approach. You have to understand what is happening in the market. What is driving the clients? This is your biggest strategic driver. Within the company you have to be able to sell security to the other stakeholders. That is easier to do when you understand their priorities."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JOHN WHITING
CISO, DDB

HEADQUARTERS: New York City, NY

EMPLOYEES: 15,000

DDB is a large, global advertising network with 15,000 employees at several agencies around the world. DDB is a part of Omnicom Media Corporation, which is among the top two global advertising conglomerates. A mandate from Omnicom's Board put a heightened priority on Information Security, resulting in the hire of John Whiting, their first Global Chief Information Security Officer. The global nature of the role, the fact that it is a new position, and the nature of working in a creative environment presents Whiting with a number of unique challenges.

INTRODUCING SECURITY PRACTICES AND POLICIES FOR THE FIRST TIME

"It was a mandate from Omnicom that brought me to DDB. In the beginning I was set up to be a sole contributor, running information security as an independent function, but the CFO quickly realized that I could not do this by myself. Now I have budget for help and resources available to me from other infrastructure teams. Those teams each have dedicated people to the security effort. We've quickly gained support for the programs," said Whiting.

Like many CISOs in other organizations, Whiting started with a gap analysis to identify weaknesses and make a strategic three-to-four year plan that sets priorities for the security team's efforts. Those priorities cover all areas of security – Awareness, Cyber and Vulnerability Management, Government, Regulations and Compliance, Configuration Management, Process Optimization and Physical Security Standards. Whiting works with the regional IT Directors who are responsible for the implementation of security efforts across the many agencies within DDB. He says, "Their security program is my program, I push down. If they want to do something different we have a process for exceptions and changes.

> "The push from clients, and the potential impact of security on the bottom line has helped me institute the necessary safeguards"

That process allows them to meet security standards while working within the particulars of their agency requirements."

Whiting runs a global program supporting regional organizations with unique needs. Because of the company's international structure, Whiting reports to the Global CIO, who reports to the Global CFO. The advertising industry is a unique industry that incubates on acquisitions and divestures constantly. This adds an extra level of complexity to a security program as there are no green field opportunities to build out a program. The budget process involves communicating needs and initiatives to the CFO and presenting timelines for implementation. Whiting also benefits from working with his colleagues, four CISOs at the other Omnicom companies. Together, the five CISOs decide on major security initiatives to be implemented across all Omnicom brands. They also rely on each other for best practices and insight as each is in different stages of rolling out their company's first security program.

INTERNATIONAL ORGANIZATIONS REQUIRE GLOBAL THINKING

DDB is international, so Whiting does not adhere to a specific set of standards. He says, "It is a hybrid approach. For the most part we follow ISO, with a little bit of NIST and COBIT. NIST is so US-centric that it does not work well internationally. There is push back from other regions when we try to implement something like NIST."

Whiting says, "The challenges to data protection and information security are standard across the globe, but countries like Germany, Argentina and Singapore have strict data privacy laws, so DDB's agencies in those countries are above the bar. Canada does not allow data to leave the country, so they have tighter standards as well."

SECURITY AND CONTROLS IN A CREATIVE ENVIRONMENT

Whiting says, "I came from AIG, which is in the financial services industry, so a little different in terms of accepting controls and processes. Advertising agencies do not like controls or being locked down. It's a balancing act for sure." Whiting's efforts at DDB have been helped along by client demands for security standards. "Similar to other industries, advertising clients have developed full-fledged governance programs. They are holding us liable with regards to what we do with their information; we are just as liable as if we were a financial services company. The push from clients, and the potential impact of security on the bottom line has helped me institute the necessary safeguards."

Since security does not come innately to advertising executives and art directors, awareness training and advocacy are big priorities for Whiting. "I'm seven months into this job, so I have started with creating awareness at the top level," said Whiting. "I work with all the regional CTOs and regional IT Directors. Since I report into IT I feel like we have to get our act together first, in order to prove security's value. I also talk to all the agency executives. I am asking them to be facilitators. Each agency owns the information they have on clients, and they own the process. As a business unit they take accountability for what happens to that information, and how it is secured."

GROW AND LEARN WITH PEERS

Whiting is fortunate to have four peer CISOs within Omnicom Media Corp, but he also relies on networking and information-sharing at conferences to keep up-to-date and educated on the industry. "I was just at a small conference and I met a CISO from a competing agency who has been doing compliance management in the advertising industry for 20 years. Those are the types of conversations that help me. We talked about the stuff you can't learn in the classroom," said Whiting.

Like many of his peers, Whiting believes the technical knowledge required for Information Security can be learned on the job, or through certification programs and associations. He encourages those interested in Information Security to study business, accounting or risk management in college. Whiting was a pre-law major in college. Early on, that background helped him to understand contracts and security clauses in Service Level Agreements, and his law background helps him to more easily understand compliance requirements and legal mandates.

Q&A WITH RON GULA

CHAIRMAN & FOUNDER, TENABLE

> **What Tenable is trying to do is understand all of the vulnerabilities and defensive controls, such that the business can make an accurate determination of all the cyber risk on their network.**

Q) WHAT KEY COMPONENTS FROM YOUR EXTENSIVE WORK EXPERIENCE HELPED SHAPE THE FOUNDATIONAL ELEMENTS OF TENABLE?

A) When I worked as a penetration tester at the NSA, my job was to go into the networks of other government agencies and report back to them on the security problems I found. Often times, coming back a year later, nothing had been done. The original problems were still there. I thought this was unique to government networks, but after moving into the commercial sector, I found the same thing. I also worked on the Dragon Intrusion Detection System, where we focused on detecting the bad guys. However, after someone asked me if I can stop 100% of attacks, I realized that in reality this is not possible.

All of these things experiences shaped how I started Tenable, with a mission of obtainable and defendable network security. We want people to obtain a high level of security across the entire IT environment and then maintain it. The biggest problem with security today is that people put too much faith in specialized point products that promise to solve cybersecurity for everyone, but the reality is that security for the modern business is an ongoing risk that the world still hasn't come to grips with. What Tenable is trying to do is understand all of the vulnerabilities and defensive controls, such that the business can make an accurate determination of all the cyber risk on their network.

Q) WHAT PLANS FOR GROWTH DOES TENABLE HAVE?

A) There are three ways we are growing. First, we are growing commensurate with demand through great partners and investing in a salesforce that can meet challenges internationally. Second, we are expanding our technology and ensuring we are taking into account cybersecurity for the entire ecosystem. Third is the emergence of a new marketing category, with businesses managing cybersecurity risk the same way they manage sales engagements with Salesforce or finance with NetSuite. Tenable is a platform for people to audit and measure all of their cybersecurity risk in a transparent manner the same way other departments function.

Q) HOW DOES TENABLE SPEAK DIRECTLY TO ADDRESSING CISO CHALLENGES?

A) The discovery of all assets is a huge component. The saying 'know yourself more than you know your enemies' means the importance to discover every asset, every mobile device, every IoT and cloud resource. This is important because if you don't know about something, you can't defend. But, discovering all of this by itself is just raw data, so we have pioneered continuous monitoring of various frameworks. By providing real-time detection of frameworks such as PCI, SANs, and NIST, we can then take all the data and tell you how your organization complies.

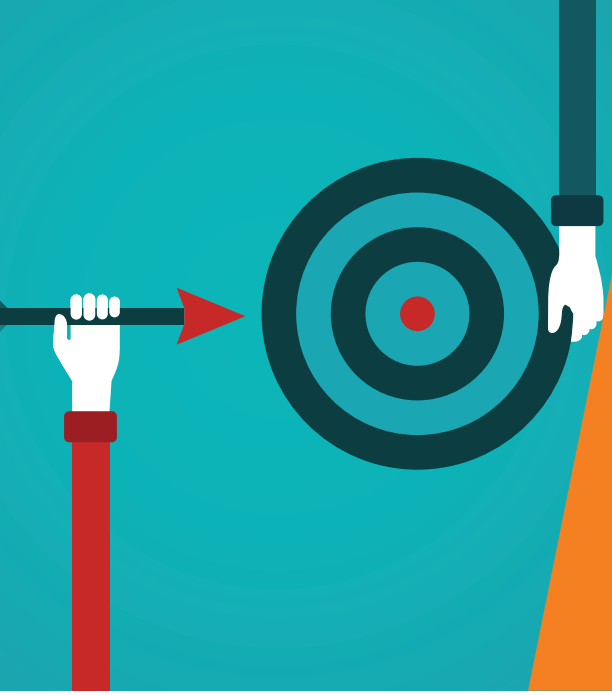
Q) WHAT IS YOUR PERSPECTIVE ON THE IDEAL RELATIONSHIP BETWEEN A CISO AND CEO?

A) For larger organizations, like big banks, they have more resources and big security teams. Their CEOs have excellent relationships with the CISOs. For smaller organizations, like a school, they may run into a lack of awareness from the board and CEO, resulting in lack of budget and a need to beg for policy changes. I always tell these CISOs to understand what they are doing. If they don't have resources or buy-in from the CEO, then they need to spend their time identifying risk and educating up. Another thing I tell them is to get in front of their peers through one of the many organizations out there that brings CISOs together. These help CISOs get ahead by the sharing of information.

I always tell younger CISOS at smaller organizations they are better off outsourcing something rather than defending poorly internally. If your organization can tolerate the cloud, simplify your network and focus on security policy and decisions that will impact your business.

Q) HOW DO YOU SEE THE RELATIONSHIPS BETWEEN CISOS AND THE C-SUITE CHANGING IN THE FUTURE?

A) In the next decade, everything is going to be virtualized, 'cloudified', and 'SaaSified'; CISOs are going to make policy decisions reinforced by the needs of the business. In the future, we will be mostly centralized cloud based applications with simple policy and access control decisions. I realize this is not going to happen overnight because we still have long, complex internal networks, but in the next ten years we will see a shift.



CASB MARKETSPACE ANALYSIS

Understand Solutions & Overcome Challanges

BY RICK GRIMALDI
DIRECTOR OF INFORMATION SECURITY SERVICES

PART TWO

ARE YOU AMONG THE 85% OF ENTERPRISE COMPANIES EVALUATING CASB?

K logix's marketspace analysis of CASB can help

According to Gartner, by 2020 85% of large enterprises will use a Cloud Access Security Broker (CASB) with their cloud services, up from about 5% today. Gartner lists the top three concerns with cloud security as governance, cloud computing environments, and security and privacy. These concerns are prevalent due to the unchartered nature of the current cloud security posture within organizations, which results in a lack of control and oversight, along with a multitude of visibility challenges. Based on conversations with our enterprise clients, it is clear to K logix that there is significant confusion and anxiety regarding upcoming CASB decisions. As a result, K logix is making our CASB Marketspace Analysis, a subset of our Data Protection Framework advisory service, available in the upcoming weeks.

The K logix CASB Marketspace Analysis will help clients distinguish the various approaches from each CASB vendor and help determine the appropriate solution that correlates best to solve their specific challenges related to cloud application visibility, data security, compliance, and threat prevention. Research indicates that these are the top four use cases among our client base.

COMPLETE K LOGIX DATA PROTECTION PROJECT ADVISORY SERVICE AVAILABLE SOON

Within our methodical process, the K logix Data Protection Framework identifies specific requirements our clients need to address, related to Data Discovery and Classification, Data Access Governance and Data Loss Prevention. Ultimately, our Project Advisory Service will help clients categorize use cases and understand which CASB solutions are the best fit based on their specific requirements and unique business needs.

K logix helps clients work effectively with business leaders to identify sensitive data, determine data ownership and classification, understand how data is managed and used, implement data handling processes, determine the requirements for technology to support the process and policies and evaluate specific technologies. Upon completion of the service, clients will be able to answer important questions, like:

1. Where (and what) is our sensitive data?

2. What do we do with unstructured, non-sensitive data and how can we reduce the noise?

3. Where does our data go, and how do I understand data flow and usage patterns?

4. Who has access to our data and how are permissions assigned?

5. What is the best solution or set of solutions for our specific needs?

Contact K logix today to learn more about our ongoing CASB Marketspace Analysis.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

PAT DARIENZO
CISO, CATHOLIC HEALTH SERVICES OF LONG ISLAND

HEADQUARTERS: Long Island, NY

EMPLOYEES: 17,500

REVENUE: $2.3 Billion

"The healthcare industry is at a crossroads," says Pat Darienzo, the CISO of Catholic Health Services of Long Island (CHSLI). Darienzo continues, "There is an industry-wide priority on the sharing of patient data to make information available in order to enable the best care possible for patients. We strive to give access to those who might need it, while at the same time HIPAA requirements limit who can have access to data and place strict requirements for identity and access management." The current landscape creates a challenging balancing act for a multitude of security leaders at hospitals and healthcare networks, especially for streamlined, distributed healthcare services organizations like CHSLI.

Darienzo emphasizes the productive approach to information security at CHSLI, solidified by the CIO and CEO, who also both recognize this important focus. "This past year was very sensitive in healthcare. In the past, information security projects declined based on budget restrictions, now it seems that sometimes the only programs that do not get cut are security programs." This movement toward sufficient budget along with the corresponding elevated concerns is evident at CHSLI, with Darienzo being a major advocate behind this shift.

When Darienzo took the CISO role, the security staff was small with a primary focus on tickets and access management. Darienzo coordinated a full policy rewrite soon after he arrived and helped restructure the organization to enable his team to spend their time on other priorities. This fundamental change not only resulted in a high performing team but also boosted morale and quality of results.

A core goal for Darienzo's team is implementing a new access and identity management tool that will help the provisioning team grant and manage role-based access. He says, "CHSLI's current process is good but it could always be better. It requires human intervention to trigger it, which can be a problem if a manager is busy or forgets to update us. If a person leaves the company the manager must send a note, otherwise the person's access may not be removed. Our new IAM solution will integrate with

the Human Resource system so all access is revoked automatically on the employee's last day. Also, many non-employees work at CHSLI, and with this system we can run a check on their status every 90 days in order to ensure we keep access rights current."

A large portion of CHSLI's security focus is on employees and how they interact with patient data, reinforcing the importance of Darienzo's team in keeping employees informed about the value and importance of security efforts. Each employee receives security training during on-boarding and the security team publishes a monthly newsletter on their intranet. He explains to new employees, "Our security processes are the primary defense standing between CHSLI and an incident affecting our patients and business." CHSLI does not evaluate employee security awareness via specific tests, yet Darienzo consistently sees an increase in reports of suspicious emails and messages, a strong sign the organization is evolving to become more security conscious.

MEETING HIPAA REGULATIONS REQUIRES A TEAM APPROACH

CHSLI includes six hospitals, three skilled nursing facilities, a regional home nursing service, hospice and a multiservice, community-based agency for persons with special needs. Darienzo works with a team of appointed privacy and security officers at each entity. "They are our satellite arms and our first point of contact if any security incidents come up. They file incident reports with us and we conduct the analysis." Darienzo balances his time between officers, while maintaining productive ties with each.

For the purpose of reporting HIPAA incidents to the Office of Civil Rights (OCR), each incident is assessed by the CHSLI's HIPAA Executive Steering Committee, which includes Darienzo, the CIO, the CPO, the CMO and representation from the Legal Department. The group reviews all incidents and determines if a breach requires reporting, or if an additional formal risk assessment is needed. All decisions of whether or not an incident meets the definition of a breach are documented, along with the facts upon which the decision was made. In cases where the OCR has reviewed CHSLI's assessment of an incident, Darienzo states they have supported the CHSLI decisions.

BE NIMBLE AND BALANCED TO BE EFFECTIVE WITH A SMALL BUDGET

Darienzo states, "CHSLI is half the size of the Health System I had worked at prior to this position. So, while we do not have as many resources, we are more nimble. You can do a lot with less, if you focus on the right things. Some of the things we accomplish are astounding when you compare it to our annual spend."

Darienzo emphasizes the importance of a team consisting of smart and efficient people, but he is cognizant of not over-working his security team. He says, "I am here to clear hurdles for them and help them get their job done. To some extent I would say I try to be hands off with my team. I just focus on giving them the time and room to get their job done effectively." Darienzo is also trying to see that steps are taken within the security plan to give the team ample support when possible. One project that will help his team this year is a SIEM project, which will provide more comprehensive monitoring; Darienzo is essentially outsourcing that function so his team can focus on higher caliber priorities.

Pulling a Rabbit Out of the Hat

Some days CISOs may feel like security requires a 'magic touch', something with which Darienzo would agree. While his full-time career is a healthcare CISO, he is also financially supporting his magic hobby with regular performances as a magician. To Darienzo, a clear connection exists between magic and information security, a possible reason why many of the CISOs he meets also enjoy partaking in the hobby (coincidentally, the CHSLI CISO before Darienzo was also a magician). Darienzo says, "Magic is about deceiving people. You draw their attention to one spot, while you perform some sleight of hand where they're not looking. Security is the same thing, you have to be aware of what is going on beyond your line of sight. Both security and magic are about deception and it's a skill knowing how to spot that deception."

C-SUITE PLAYERS: WHO ARE THEY?

Information security has only recently been elevated to the C-Suite, and many CISOs are new to the role with an average of almost two years experience. Understandably, many CISOs are still carving out their role in relation to the C-suite and still working to establish relationships with other business leaders.

CISOs are in a unique position. They are one of the few executives whose programs require collaboration and partnership with every other department in the organization because data protection and security initiatives impact people, process, and technology across the whole company. That means, more than any other C-level executive, CISOs must understand the motives and priorities of every other department. To establish the strongest working relationship with their peers, CISOs must understand how each leader thinks about information security.

Chief Executive Officer

2016 Priorities: Growth and digital innovation

Security Check: 44% of US CEOs are extremely concerned about cyber security in 2016 (PWC 2016 US CEO Survey)

In their words: "As technology transforms our company, the risk of intrusion and cybersecurity worries us the most. Now, we've spent serious amounts of money on this, but the reality is you're never done. As much as we used to think about protecting our physical assets, it's the same today with our non-physical assets. They're in the hands of different people, and it's sometimes harder to figure out."
- Brian Moynihan, CEO of Bank of America Corporation quoted in PWC 2016 US CEO survey

Chief Marketing Officer

2016 Priorities: Data driven marketing

Security Check: CMOs top concerns are brand loyalty and consumer confidence after a breach

In their words: "As you might imagine, data security and privacy are extremely important to this company and we've learned a couple of things along the way. There's a simple question that we ask that can guide people really easily, which is, "Are we doing something for our guest or to our guest?" And if we're doing something for our guests it implies that there's a value exchange: In return for information we are giving them something of value. Obviously it's far more complex than that. It means you must have really clear privacy policies, be transparent about opt-in/opt-out and build better preference centers. All those things are super important, but it starts with a pretty simple question."
- Jeff Jones, CMO of Target quoted in Forbes.com

Chief Financial Officer

2016 Priorities: Margin and earnings performance

Security Check: Cyber security risks are the second highest priority for CFOs

In their words: "When you talk about the finance function being involved in IT and information security, it is usually to put in place process, standards and structure related to how data is used and accessed. I don't know a CFO who wants to own the security function. CFOs interact across all departments and can play an impactful role in incorporating security throughout the organization."
- Nick Araco, President of the CFO Alliance

Chief Information Officer

2016 Priorities: Managing the digital transformation

Security Check: Security & privacy are the number two priorities for CIOs (SIM 2016 CIO survey)

In their words: "One thing I'm seeing is that in some companies, when they think about security they see it as a compliance and risk exercise, and I get that there is a place for security there. But, we are doing security wrong and doing it a disservice [when we limit it to risk and compliance] because security should actually be an enabler, customer experience enhancer, revenue enhancer. I would offer that perhaps security should report to the COO or Chief Strategy Officer."
- Theresa Payton, former CIO of the White House (excerpt from Theresa's Profiles in Confidence)

Chief Technology Officer

2016 Priorities: Secure development

Security Check: Cybersecurity risks are the second highest priority for CFOs

In their words: "Building value through technology today requires technical and business knowledge as it always has, but understanding and aligning each system with an effective security program early in the life of that system is now critical as the risks are higher than ever," said Bill Murphy, Blackstone's Chief Technology Officer. "Development and security partnering early on produces better and cheaper solutions. Bolting security on at the end never works as well and usually costs a lot more."
- Bill Murphy, CTO of Blackstone

Chief Legal Officer/General Counsel

2016 Priorities: Ethics, compliance, regulatory issues/challenges

Security Check: 59% of CLOS rated data breaches "very" or "extremely important" in 2016 (ACC CLO Survey 2016)

In their words: "Whether the CISO reports to the CCO or CLO there should be a direct report to in-house legal counsel in the event of a data breach. Short of that, the CLO should be kept apprised of changes in security systems and protocols, since those directly concern questions regarding compliance and legal liability."
- Christopher Hart, Attorney at Foley Hoag

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

DEAR C-SUITE

JUNE 2016

K logix
WWW.KLOGIXSECURITY.COM
888.731.2314