FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

TACKLING THREATS

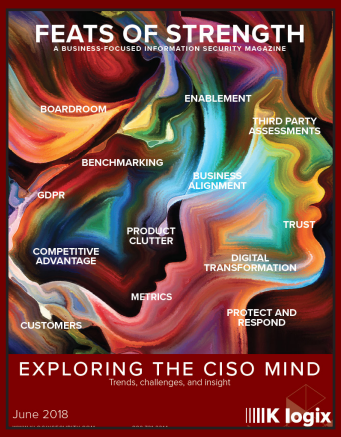
THE IMPORTANCE OF WORKING TOGETHER TO REDUCE RISK

SEPTEMBER 2018

KLOGIXSECURITY.COM 617.731.2314

K logix

TABLE OF CONTENTS



To view past issues, visit:
www.klogixsecurity.com/feats-of-strength

Magazine Created By:

K logix

Magazine Contributors Include:

Kevin West
CEO, K logix

Katie Haug
Director of Marketing, K logix

Kevin Pouche
COO, K logix

Marcela Lima
Marketing Coordinator, K logix

Contact Us:
marketing@klogixsecurity.com
617.731.2314

We provide information security strategic offerings, threat and incident capabilities, education/awareness, and technology services. We craft our services to address specific customer and industry challenges. One of the ways we do this is through our thought leadership, business-focused publication Feats of Strength. Through 100+ CISO interviews, we extract trends in order to provide services that align business to information security.

LETTER FROM

KEVIN WEST

CEO

TACKLING THREATS: WHAT IT MEANS FOR CISO LEADERS

After speaking in-depth to our CISO community and the leaders we featured in this issue of the magazine, it became apparent that tackling threats isn't as much about having the right technology in place, but more about CISOs leading their organizations by instilling a strong security culture.

Leaders who establish strong security cultures are more protected, smarter, and result in an entire organization's strength against any potential threats. CISOs who establish these strong cultures do not work in silos, they instead protect their organization in a stable, assertive manner. Many CISOs we speak to, both those we feature in the magazine and those who advise us, continue to share why and how building a security culture is at the forefront of their strategy.

Second to a strong security culture is having the right talent to support your goals, from both a strategic and tactical perspective. Time and again, CISOs tell us they are only as strong as their team member's strengths – both as an individual and as a productive team working together on common goals.

We went deep with the CISOs interviewed and asked them a range of questions about their approaches to tackling threats. They shared with us how they organize their program in a strategic, yet enabling way, all while ensuring they continue to protect against the continued influx of threats. Many CISOs shared similar opinions about the top threats impacting their organizations, and the industry as a whole. We learned how many security leaders communicate the threat landscape to their executives in a business-minded way.

To recap some of the conversations we had with CISOs who helped put this issue together, here are some of the highlights from questions we asked them:

How do you stay on top of new threats?

Most CISOs rely on a few sources including their peers, industry threat sharing sites, and products.

What is the biggest threat impacting your organization?

The majority of CISOs we spoke with said phishing, and the more targeted spear phishing.

What is the biggest concern for insider threats?

Many responded they are more concerned about the accidental employee versus the malicious employee.

How do you communicate threats to your executives?

Today, security leaders are having proactive conversations about threats due to better alignment between business and security, and heightened awareness of the general public.

We learn even more about threats in our article with Erik Kamerling, lead information security consultant at K logix. Erik shares his extensive experience working with organizations all over the world battling phishing threats. He breaks down Business Email Compromises, phishing attacks with commonly disastrous financial consequences, and provides examples and actionable recommendations.

We always want to hear from our security community about their opinions on the topics we cover in the magazine. Please don't hesitate to let us know what you think about this important issue.

KEVIN WEST is the founder and CEO of K logix, a leading information security company based in Brookline, MA. K logix helps create confident information security programs that align with business objectives.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

MAARTEN VAN HORENBEECK
CISO, ZENDESK

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 2,000+

ANNUAL REVENUE: $500 Million

"There's always ways to deal with the threat of the day, but in the end, you need to build a culture that's agile and open enough to using those technologies and using the different people in the organization to help protect the organization."

- Maarten Van Horenbeeck

Originally from Belgium, Maarten Van Horenbeeck began his career as a security engineer, splitting his talent between his day job and voluntarily helping nonprofits with their security needs during the evenings. Stemming from this early work, Van Horenbeeck gained perspective on how to implement security and realized security was much less about a technical problem, and instead more of a problem of culture. He recognized the importance of building a culture of security within an organization to be effective. He says, "There's always ways to deal with the threat of the day, but in the end, you need to build a culture that's agile and open enough to using those technologies and using the different people in the organization to help protect the organization."

In the late 2000s, Van Horenbeeck worked at Microsoft as a manager who helped release security updates for the Windows platform and protect users of the operating system. The main challenge for him was building security into Microsoft products and creating a culture of security. After other high-level positions in information security, Van Horenbeeck joined a startup company where he built out the security capabilities from the ground up before moving into the CISO role at Zendesk.

GROWING INTO A CISO LEADER

Six months ago, Van Horenbeeck was hired as CISO at Zendesk, a cloud-based help desk solution offering customer service software and support ticketing systems. When discussing the growth into a C-level executive, Van Horenbeeck describes it as a transition of learning to 'let go.' He explains, "For me to transition from being an engineer to a leader has really been about letting go. It's been about identifying the areas where I was no longer the best person to do this job and figure out how to hire, retain, and get those people on board that are the best people to do that specific work. It is something I've personally always had a challenge with. In fact, I like to be in an organization where I can still step in and do something when it's necessary and as you grow into a chief information security officer role, you must accept that you're no longer in that place."

When discussing his role and what it means for handling risk, he believes it to be one of the biggest differences in becoming CISO. He says, "When it comes to assessing the risks, the buck really does stop with me. I have to bring together the views of my team. I have to bring together the views of other executives and identify what risk is appropriate for us as an organization and what isn't and be sure that we communicate very transparently and very openly so the business can actually make the right decisions."

THE IMPORTANCE OF A SECURITY-FOCUSED PURPOSE

"We came up with what our purpose is in the organization, and I like the term purpose over mission because when you have a mission, it implies that there's an end to this. It's important to note that when you have a mission and you fail, people will be very disillusioned. I'll give you an example. If you have a mission to protect the enterprise from a breach and you have a breach, then you effectively fail at your mission and people will feel disappointment with the work that was delivered or what was done. The important thing to acknowledge in security is that you will never get everything perfect," says Van Horenbeeck.

For Van Horenbeeck and his team, having a sense of purpose solidifies their core goals of protecting the company, customers, and employees from threats. Even if an incident occurs, his team still uses their purpose to take the right action items to make sure they protect data or people to the greatest degree they possibly can. The goals supporting his teams' purpose are building a security culture, ensuring effective prioritization, supporting business decisions, and becoming a learning organization.

"My main goal is that we do things that are repeatable. We must be consistent and make sure the teams understand why we do what we do, and that leads to a level of trust that allows them to interact with us more effectively. We also need to understand where we are today, what our gaps are, and how we can reduce risk. We need to understand what that risk is, communicate it effectively across a wide set of individuals, both at a technical level and executive leadership level, and make sure that we can help them drive the right business decisions to balance that risk against growing the organization or doing great things for our customers," states Van Horenbeeck.

When discussing risk with executives, Van Horenbeeck recognizes everyone has a different boundary of how much information they are interested in. As a CISO, he describes the importance of starting higher level and conveying critical facts, but also understanding how deep to go with each individual. He says, "It is a little bit of an individualized approach depending on the leader that you're actually working with. And I think sometimes it's a mistake to start off assuming they all have the exact level of information they require to make a solo decision and feel comfortable with the decisions that you're recommending."

STRATEGICALLY APPROACHING CHALLENGES

In a recent meeting, an employee asked Van Horenbeeck what keeps him up at night as a CISO and the biggest threats facing Zendesk. He replied with an unexpected answer by revealing his greatest concern was being able to hire and retain great people. He explained how everything in security starts with good people who can help move the needle. While hiring in security has become incredibly challenging, especially in the San Francisco area, it is vital to create an environment where people want to work and where they can apply their passion to protecting the company, employees, and customers.

A second threat Van Horenbeeck sees is the different boundaries between where companies inter-operate and where customers inter-operate with those companies. He explains, "As a SaaS provider, one of the big things we do is invest a significant amount of our time building a secure product, and that means addressing software vulnerabilities. There's a boundary there between how customers use the product and it's sometimes less understood these days with how quickly the internet and SaaS services are growing."

Putting Customers First

"When we built out our security program, I tried to take the philosophical approaches we have in place and distill them down into what we do as an organization to be effective. And the single most important one for me was when I joined Zendesk, we always put our customers at the center of what we do. And that's something that we really tried to replicate in the security team, it's something that just intrinsically makes sense to all the employees, so it was a nice framework we could use to tell them how we see security. Some practical ways that we put that into place was by making sure that we push knowledge to our developer and engineering community so that they can actually make security decisions without always having to come to security."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

SELIM AISSI
CISO, ELLIE MAE

HEADQUARTERS: Pleasanton, California
EMPLOYEES: 1,500
ANNUAL REVENUE: $417 Million

About three years ago, Selim Aissi embarked on building a security program from the ground up as CISO of Ellie Mae, the leading cloud-based platform provider for the mortgage finance industry. Leveraging his extensive experience in financial and technology security, along with thought-leadership acumen, Aissi developed a strong security and risk management and worked hard to bridge the gap between Ellie Mae's board of directors, executives, engineers, customers, and partners.

TOP STRATEGIC GOALS AT ELLIE MAE

Aissi leads with four specific, strategic goals to continually ensure he aligns security with the business and makes an impact on the overall organization.

Protecting customer data. For Aissi, this means implementing necessary controls, accessing and understanding risk, and making the right investments to protect customer data.

Automation. Aissi says, "It's key in this space that whatever can be automated, is automated. A lot of the things CISOs do are based on workflows (e.g., incident management, vulnerability management, and patching). All these workflows should be automated. One of my strategic goals has been to automate any security-workflows that could be automated."

Innovation. Pushing limits in terms of detection, monitoring, and remediation are key for Aissi when it comes to innovation. He has deployed many of these innovations and his team continues to be at the cutting edge.

Customer-orientation. "This means continuously talking to customers, understanding their challenges, helping them out when they need help, and learning from them. We have thousands of financial customers and a lot of what they do and what they see is very relevant to us. So, I've started a lot of engagement with our customers' CxOs to share learnings and help them succeed. Since we work in the same space, we're targeted by the same adversaries, and we want to be able to share as much as we can," explains Aissi.

STRATEGY TO COMBAT THREATS

Aissi implements core tenets to continually and proactively combat threats impacting Ellie Mae. The first one is solidifying a strong cyber threat intelligence program. He comments, "The purpose of having a cyber threat intelligence program is to be able to predict most

of the attacks, and to correlate many incidents so that similar attacks can be avoided in the future. This program also helps to quickly collect indicators of compromise and to effectively use them for prevention, monitoring, and forensics."

Aissi also believes that having a strong insider threat program to manage threats is critical. He values building a threat management program based on risk since not all threats are created equal. This type of program enables quick assessment and evaluation of threats, as well as making decisions about the criticality of an incident.

Another important aspect of a threat program is having a strong and effective Security Operations Center (SOC). He says, "When there's a threat, any related alerts should feed into the SOC in real-time. The SOC should analyze it and quickly react to it. Having an effective SOC team and process are key. It's also important to have automation when it comes to threat management. When an incident happens, the whole workflow should be automated including threat hunting, mitigation, investigation, forensics, all the way to the closure of that incident."

The last tenet of Aissi's approach is making sure incident management is proactive and practiced. He believes that security teams should constantly practice this to know whether their workflows work. For him, he says a strong process and meticulous fine-tuning as well as enrichment ensure that incident management is effective.

THE REALITY OF PHISHING THREATS

"The biggest threat we see is phishing. These types of campaigns are massive and they're getting more sophisticated and more targeted. They're coming with new weaponized payloads and new credential-harvesting techniques," explains Aissi.

He continues, "The thing about phishing is that it's a "gateway." It provides an attacker access to many different valuable assets in a very unique approach that leverages human weakness. Social engineering will continue to be an effective method for adversaries. Many years ago, I used to see a lot of targeted attacks where the attacker would go straight to a database. However, today that's not even necessary because if an attacker can launch a very targeted spear-phishing attack that is based on exhaustive reconnaissance, their chances of stealing sensitive information from their specific victim are much higher. They don't need to spend two or three months getting into a database because social engineering is a much easier approach and it's more cost-effective for the attackers."

To combat these types of attacks, Aissi relies on having necessary cybersecurity controls at different levels. While educating and training employees also plays a major role, he says it should be a balanced approach.

For internal education, Aissi focuses on awareness and simulated phishing attacks so employees learn to pay attention to details. In his experience, most phishing emails can be detected visually if employees are well-trained.

When it comes to available commercial security tools, Aissi says many of those can drastically reduce the number of known phishing attacks, however many technologies and processes need to be built internally and continuously fine-tuned and enriched. He comments, "These tools, if they're not self-learning, need to be fine-tuned all the time because you don't want to block good email. The number of false positives needs to be reduced to near-zero, otherwise it's not an effective cybersecurity tool. This is where it's important to be able to have an effective security program and not block the business since legitimate emails still need to go through. Fine-tuning and adding intelligence to these products and solutions is really important when it comes to spear-phishing. I call this ensuring that all cybersecurity controls get the necessary TLC!"

What advice do you have for other CISOs?

"CISOs cannot speak buzzwords, they must understand security technology and innovation trends to make decisions about what solutions to deploy and how to address operational and business risks. They must also be a credible partner to the business and to customers. A CISO should partner with all executives to make decisions together and should aspire to be an enabler to the business. Last, CISOs must be practical but also strategic. They should be able to build an effective security program and describe all of the components of that program in business terms. My last piece of advice for other CISOs: never stop learning!"

Q & A with Erik Kamerling:

Breaking Down Phishing

We asked our CISO community: What is the largest threat impacting your organization?

Not surprisingly, the majority of CISOs said phishing was one of the primary vectors attackers use. We asked ourselves why this well-established threat mechanism continues to retain relevance as a top concern across industry, and what can be done to increase organizational resiliency in a measurable way.

Providing answers to our questions is Erik Kamerling, Lead Information Security Consultant at K logix.

Why do the majority of CISOs say phishing is one of the top threats impacting their organizations?

Erik: It has been some time since the convergence of counterculture old-school hacking and conventional street crime. When the Internet first evolved, the computer attack realm was largely ruled by talented technologists who were motivated by curiosity or cyber espionage. Street level criminals were not initially part of the computer attack game. So, how and why did they emerge as one of the primary syndicates in the threat community?

For one, phishing is easy and very low risk. Willie Sutton was famously quoted as saying that he robbed banks because "that's where the money is", giving us insight into what type of character, what profile of criminal, is attracted to the lowest hanging fruit. Much in the same way that strong arm robbery and menacing is often the simplest method to relieve someone of their money in street crime, phishing may be considered one of the simplest and easily accomplished forms of cyber-attack. However, face-to-face robbery often carries a high risk of physical consequence for the attacker, whereas phishing is equivalently simple, yet carries little to no risk for the perpetrator. This insight into the types of characters who phish us allows us to discuss a proven fix to this social phenomenon that we've seen succeed in other areas of society.

I've never observed a comprehensive off the shelf technical solution to the phishing problem. That's because the core issue is conventional fraud; a targeting of process weaknesses that our organizations natively embody, rather than exploitation of technical exposure alone. That's not to say that enterprises should not invest the time, energy, and money in things like secondary phone verification, a rotating intranet nonce, DMARK, DKIM, antivirus, endpoint security agents, email gateways, and reputation-based services. You should, since the above toolbox tackles about 50% of the phishing threat. But even when you have the tools, you'll still be phished. The question is whether your organization as a socio-technical entity, can thwart the inevitability when your technology fails to inhibit an attack.

What is Business Email Compromise and how does it relate to Phishing?

Erik: One thing I observed is a rising flood of what the FBI calls "Business Email Compromise" or BEC. A Business Email Compromise is a phishing attack with commonly disastrous financial consequences. BEC is typically derived in phishing. According to the FBI: "Since January 2015, there has been a 1,300 percent increase in identified exposed losses, now totaling over $3 billion." In a recent global law enforcement sting, the FBI, DHS, Treasury and Postal Services were able to seize nearly $2.4 million from a worldwide criminal syndicate and disrupt $14 million in BEC related wire transfers.

BECs are often initiated by a first stage phishing attack against a key employee within a company. The person doesn't matter, it's the person's role that is typically targeted. An attacker looks to gain access to a privileged email account allowing them to further habituate through exploitation of inherent privilege, into the email server infrastructure itself. Once account access is gained, attackers often re-route email, change email rules, craft manipulative or access heightening internal communications to other employees, and further compromise additional accounts. The most noteworthy aspect of a BEC attack process is that the attacker will

surveil internal employees' messages to gain insight into the inter office communication process that takes place. They do this because they are staging to "strike when the iron is hot" and use intelligence they've gained to exploit interpersonal or procedural office conditions to pilfer money, databases, PII or trade secrets.

What is an example of Business Email Compromise in action?

Erik: An attacker has gained access to a Director of Finance's email account through a sophisticated phishing attack. The attacker then surveils day-to-day email communications and determined the company CFO demands last minute financial requests, no questions asked, near the end of day every other Friday. In anticipation of this flurry of emails, the Director stays later every other Friday to quickly process these requests. The attacker lies in wait and spoofs an email from the CFO to the Director at 5 PM Friday, requesting a large payment to an offshore account. Since the Director is acclimatized to this frenzied process, they comply with the request without secondary authentication or second guessing. It will be Monday before the transaction is discovered, and the company loses a large sum of money.

BUSINESS EMAIL COMPROMISE:

Phishing attack with commonly disastrous financial consequences.

This can only be accomplished through surveillance and intelligence gathering, and careful scheduling of fictitious communication streams. A phishing attack provided the first inroad to the organization, but phishing is not the only thing that could have been combatted. This scenario is largely a con, or what would be more accurately describes as a sting, the touch, a big store, or "big con" (David Maurer), which uses trickery and timing to exploit human procedural weaknesses to relieve a target organization of money and resources. This attack's success was largely due to the exploitation of a flawed human to human process within the organization.

How do we build defenses against Business Email Compromise/Phishing?

Erik: If we are interested in building defenses against this phenomenon, then our solution partially lies in changing the authority structure of organizations. Just as important is to build a sense of skepticism, critical thinking amongst employees, non-deference to authority without secondary authentication, and the fostering of a "trust but verify" milieu to effectively combat this threat. The threat is the attacker, the exposure is where our technology fails, AS WELL as the propensity of employees to execute orders expeditiously for fear of consequences handed down by their superiors.

If we think of phishing and BECs as a natural evolution of classical conning, we must ask ourselves what led to the eventual disappearance of common street grifters? It's a rare occurrence these days to be approached by a con man or "roper" on the street. According to David Maurer, the author of the study *The Big Con* on the language of con men; "Confidence games are cyclic phenomenon. They appear, rise to a peak of effectiveness, then drop into obscurity". He also cites the "booming campaign of Federal and Postal propaganda designed to rob the criminal of the sympathetic public opinion" as the primary mechanism in the reduction of street grifting and roping methodologies and often their forced disappearance or extinction. What this means is the more jaded a populace becomes, the more homogeneously skeptical to the methods of the conman, the more a specific con (BEC in this case) loses effectiveness.

The more an organization has a culture of transparent, honest authority in furtherance of the shared company mission, and the more skeptical employees carry the shared mission no matter what their role, the more reluctant they are to blindly execute orders and transactions on behalf of their cohorts or their cohort's respective authoritative procedures. A willingness to authenticate orders face to face with coworkers and managers results in a more phishing resilient organization. I'm quite sure that if we couple simple psychological changes within an organization with the technical toolbox outlined above, that we can all perhaps live through an era where we saw phishing arise as a new form of the Con, and we also saw it fade back into obscurity as yet another grift that's seen better days.

Erik Kamerling is a Lead Information Security Consultant at K logix with twenty years of experience in the fields of program maturity consulting, network security assessment, penetration testing, incident response, and vulnerability research. His work in Cyber Security has taken him around the world where he's provided program leadership and strategic and tactical consulting to clients throughout industry and government.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR TACKLING THREATS

EUGENE DAVYDOV
CISO, LINCOLN INVESTMENT

HEADQUARTERS: Greater Philadelphia, PA

EMPLOYEES: 1600 (including contractors)

TOTAL ASSETS: $35 Billion

With eighteen years of experience in information security and risk management, Eugene Davydov has worked in multiple roles across many industries, helping to strengthen his well-rounded skillset. Davydov began his career as a security consultant during the industry's infancy in the early 2000s, then transitioned to working for Cigna, a Fortune 100 firm. After experiencing the 'heyday' of HIPAA and everything related to privacy, security, and regulations surrounding healthcare, he moved on to Dow Jones, where his CISO leader exposed him to business-focused, executive-minded decision making, with an eye on risk management and regulatory compliance. Building on this previous experience, Davydov then worked for NRG Energy doing cybersecurity team-lead work, before beginning a position at SunGard, a Fortune 500 technology services organization.

Currently the CISO of Lincoln Investment, a Philadelphia-area financial services wealth management firm, Davydov oversees the cybersecurity risk management and governance programs. Leveraging his robust experience, Davydov was able to confidently accept the CISO role and responsibilities at Lincoln Investment.

He says, "I had the opportunity to significantly build upon a greenfield program in order to demonstrate value to the firm in a way that is unique, by leveraging existing resources, infrastructure, and talent, in a cost-efficient manner. That's the biggest value. We have a matrix reporting structure, where the talent that works on cybersecurity-related matters is also, in some cases, the talent that works on infrastructure and regulatory compliance matters. I believe this close partnership between information security, compliance, and infrastructure is a competitive advantage for us all. We're all here to support and serve the business."

He continues, "What we have done is built credibility and trust surrounding our security and risk management program, in order to make sure we're engaging our front-level staff as much as our senior-level decision makers, all the while meeting business needs and regulatory objectives."

HOW DO YOU UNDERSTAND YOUR RISK POSTURE AND TRANSLATE THIS TO THE BUSINESS?

For Davydov, tackling risk begins with comparing his security posture to the CIS Critical Security Controls (former SANS Top 20 Controls). He explains, "We can get a fairly robust understanding of where our strengths are, as well as where our opportunities are, by using the SANS Top 20 model, we're able to articulate the risk and subsequently relate the risk, from a very technical perspective to a high-level perspective, which resonates with the seasoned C-suite executives."

When asked how he communicates these risks to executives and the board, Davydov institutes a strategy to aid in translating technical terms to business language. He says, "The strategy I

use is to engage real world analogies. Let's say I'm building resilience for a company's infrastructure. I would relate it to building a burglar alarm for your home, adding several levels of protection for your home in a way that's relatable and palatable to a high level non-technical audience. When explaining compliance and regulatory requirements, I present them as baselines and guardrails. Using soft skills and analogies in order to articulate the opportunities for innovation is essential for gaining buy-in."

These soft skills are also utilized during his monthly meetings with the Risk Committee. Davydov says they consist of dynamic conversations in conjunction with his own presentation and agenda. One of the key challenges is helping the Risk Committee understand the relevant information security risks to the organization. He accomplishes this by distilling complex jargon into unambiguous and concise actionable intelligence.

He continues, "We have a number of policies that include reporting on actionable intelligence, when it comes to threats against the firm. If we gauge the threats to be broad enough, we often communicate that to the Risk Committee. Primarily it stays within the purview of myself, the CIO, the CCO, and the General Counsel."

HOW DO YOU STAY ON TOP OF THREATS?

Davydov subscribes to several third-party publications and data sources to stay well-informed to current and future threats impacting his organization. He explains, "We are members of FS-ISAC which provides financial services cyber-intel for our industry. In addition, I'm also a member of a public-private alliance group between the FBI and the private sector, an organization called InfraGard. We share near real-time cyber threat data. That's always very helpful. Primarily, it is third-party data sources I am using to help me stay on top of external threats." Concurrently, Davydov's strategy for internal threats relies primarily on Big Data and correlating events via a centralized intelligence repository.

To filter through the noise and ensure he stays in front of threat alerts, Davydov says the primary gate is whether the threats are relevant to the financial services industry. Many alerts are filtered before they get to him, however he continues to have his finger on the pulse to ensure he remains plugged in to actionable threats.

WHAT IS THE TOP THREAT IMPACTING THE FINANCIAL SERVICES INDUSTRY?

Currently, Davydov says well-researched and highly-orchestrated phishing attacks are the highest threats impacting the financial services industry. He comments, "In these attacks, the adversary will spend a lot of time doing analysis, understanding the individual they are targeting, and understanding what they're interested in. The modus operandi is surveilling and then carefully tailoring the fraudulent communication. The communication is so specific to the individual, that there's a good likelihood the recipient will act upon it. Across all financial services firms, that's been a growing trend, as of 2018."

To prepare and combat these types of attacks, Davydov institutes strong security awareness through simulated phishing campaigns, something he believes has been crucial in driving the message across the firm.

HOW DO YOU LEAD AND EMPOWER YOUR TEAM?

Davydov describes his leadership style as empowering individuals for success by articulating how their contribution helps to drive the broader mission of the firm. To that end, he strongly believes in finding team members who possess passionate curiosity. These types of individuals are often easily teachable and adaptable, and Davydov says they typically stay focused on the agenda despite the dynamics of business and continue to move the program in the right direction. He states, "A lot of it also comes down to being able to learn from the inevitable mistakes we all make. It's only natural, we're going to make some blunders. We're going to learn important lessons from them. And then we're going to move on, stronger and wiser than before. That approach has worked reasonably well in order to keep folks engaged, in an industry where great talent is often scarce."

When looking to the future of his career, Davydov says his primary value proposition is in the risk management and cybersecurity compliance world. He comments, "Perhaps the biggest takeaway is that risk management truly is a team sport. The aptitude to build credibility and trust, not only with your own team but also with other department heads across the organization is paramount. As the cybersecurity program matures, one of the greatest challenges is identifying the 'point of diminishing returns' on our security investments. In order to be perceived as a business enabler through the lens of senior management, we make every effort to strike the right balance, thereby paving the way for business, rather than standing in the business's way. To that end, we're careful to articulate not just the how, but also the why surrounding risk management decisions, in order to win over the hearts and minds of our leadership team and the board of directors."

We Asked Our Partners: **How Do You Differentiate in a Cluttered Marketspace?**

K logix

Partner

Spotlight

We asked some of our top partners an important question:

In such a cluttered market, how do you differentiate?

In their responses below, hear from:

Bitglass: Next-gen Cloud Access Security Broker delivering agentless Zero-Day data & threat protection for any app, any device, anywhere.

ObservelT: Leading insider threat management solution including employee monitoring, user activity monitoring, behavioral analytics, policy enforcement, and digital forensics.

Forcepoint: Transforming cybersecurity by focusing on understanding people's intent as they interact with critical data wherever it resides.

NEXT GEN CLOUD ACCESS SECURITY BROKER WITH BITGLASS

RICH CAMPAGNA
CMO, BITGLASS

bitglass
Next-Gen CASB

Cloud Access Security Broker (CASBs) have quickly emerged as the de facto standard for enterprise cloud security, protecting a wide range of applications. As enterprise use cases evolve, it is our job as a vendor to stay ahead of the competition in that regard.

For Bitglass, our sustained differentiation comes from our strategic, architectural choices. These include:

• Deployability - A CASB solution is useless if it never gets deployed. Most CASB vendors have chosen to take shortcuts in their architecture that cause significant deployment challenges. The core of the Bitglass architecture are agentless proxies which allow transparent access from any device, anywhere, with no software or agent installation.
• Flexibility - Most CASBs have architectures that rely on hand-coded connectors for each new application, slowing down your move to the cloud. Only Bitglass' architecture is built to automatically learn and adapt to any application, which means no holding back your business - simple configuration is all that is required for any application, even internally developed applications.
• Real-time Data Protection - many CASB vendors have made the easy choice of providing only out-of-band API-based integration with cloud apps, eschewing the much more difficult to build inline proxy architecture. Unfortunately, this comes at the cost of losing real-time data & threat protection. Bitglass protects data in real-time and from end-to-end (cloud to device).
• Support - Every Bitglass employee is part of our extended support team. We assign a deployment lead the day of contract signature, and people in every functional team continue to engage throughout the customer lifecycle.

Currently, there are **over 2,500 security technology organizations**, and **CISOs often struggle to differentiate and understand value** between them.

Read how these companies **stand out**.

INSIDER THREAT MANAGEMENT WITH OBSERVEIT

MIKE MCKEE
CEO, OBSERVEIT

observe it

The cybersecurity space is certainly crowded, but ObserveIT is in a unique position as the only true insider threat management solution out there that's capable of detecting, investigating, and preventing incidents caused by the people you know – such as your employees, vendors, or contractors.

There are some factors outside of our control - such as shifting industry priorities – that have helped us stand out. Until recently, organizations have been primarily focused on external cybersecurity threats. But we've seen a dramatic shift in companies shifting their attention to insider threats with the increase in news coverage for insider threat incidents like those faced by Google, Tesla, Suntrust, and others, and the high costs associated with incidents – Ponemon Institute research shows the average cost per incident over a 12 month period is a staggering $8.76 million!

We can control how well our customers achieve their insider threat-related objectives and how satisfied they are. We pride ourselves on ensuring our customer are successful and on providing world-class support, and we're confident it shows – we've achieved an NPS score of 75 for the past two years! Knowing you're getting the best product to ensure you can identify and eliminate insider threats and knowing you'll receive the best service is huge. Happy, successful customers is the biggest differentiator and best way I know to stand out in a crowded space!

TRANSFORMING CYBERSECURITY WITH FORCEPOINT

DR. RICHARD FORD
CHIEF SCIENTIST,
FORCEPOINT

FORCEPOINT

Cybersecurity is a horribly crowded market – there's no question about it. However, we've tried really hard to be clear about how we view the problem differently. To that end, we do two things to demonstrate that we are a different kind of cybersecurity partner.

First, marketing in cybersecurity has suffered from a terrible "snake oil" problem for years. With buyers often running around searching for a "magic bullet", proliferation of point products, and what can only be described (kindly) as a highly "abundant" startup ecosystem, it seems like all of us have, at one time or another, taken "the sky is falling and only we can help you" approach to positioning. We're very aware of that pitfall, and so we spend a lot of cycles making sure that our products do what we say they do and that you can hold us to it. Cybersecurity is far too important to take based on feel, it's a science, and we try and treat it that way.

Second, while Forcepoint is highly adept at detecting threats (such as malware and phishing), we recognize that this is a necessary but not sufficient skill set. To that end, we have spent significant effort on understanding the "how" and "why" of users and their access to corporate resources, in order to better secure that which matters: your data and your people. We then take it one step further: we don't just say "Hey you have a problem", we automatically allow customers to change their defensive stance based on these observations. In essence, we're not just a monitor, we're a guard who gets involved in dealing with risks to your data. At our core, we're very focused on the fact that cybersecurity is a means to an end, and not an end in and of itself. It's all about protecting what really matters.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

RICK ORLOFF
CISO, ADDEPAR

HEADQUARTERS: Mountain View, California

MEMBERSHIP: 325

ASSETS ON PLATFORM: >$1 Trillion

As an extensively seasoned information security leader, Rick Orloff ensures he delivers actionable results focused on aligning security with real business opportunities that enable the business to achieve goals and objectives. Orloff's notable security leadership positions include leading part of the security program at Apple Inc. around stopping and managing information leaks including protecting Apple's prototype devices and unannounced products and services. His work at Apple Inc. expanded into other security program areas during his 6+ year tenure before moving on as the CISO of eBay where he helped navigate the splitting of eBay and PayPal, among other key initiatives. He then worked as CSO for Code42, a backup and recovery organization, before taking the Chief Security Officer and Chief Privacy Officer position at Addepar, a cloud-based investment management technology startup company.

Among his many accomplishments, Orloff's experience includes business process improvement, structured problem-solving skills, operations leadership, and budget responsibility of $100M. Utilizing process and metrics orientation to build and lead high-performing teams delivering creative world-class solutions, Orloff demonstrates strategic traits including strong analytical, decisive, and technical skills.

STRENGTHENING CISO AND BOARD ALIGNMENT

In his many years of practice, Orloff experienced the continuing evolution of CISO relationships with their executives and board members. "There needs to be meaningful connective tissue between the CISO and the board. Typically, a CISO has 15 or 20 minutes to run through a deck and provide a snapshot in time. What's also needed is the connective tissue where these CISOs are also talking to one another with the different board companies," says Orloff.

He continues, "Many boards are looking to add security expertise and I'm seeing more CSOs/CISOs being asked to sit on other boards. By including security expertise on the board, there's an opportunity for the board to ask meaningful questions and ensure the company has a reasonable security posture. Companies that also have security experts participating on their boards seem to embrace security as part of the corporate DNA."

Orloff advises other security leaders to focus board room presentations around a holistic view of what the security program looks like, highlighting core areas of focus. He notes the high value of prioritizing how the program addresses, or

mitigates, threats that can affect the "valuation or reputation" of the company. Furthermore, he values the ability to walk board members through how he measures program maturity, progress, and goals.

He states, "At the end of my presentation, I try to educate the board on a couple of items. Some CISOs conclude a board presentation but the board members may not know what to ask. The question they really need to ask the CSO or CISO is: how do you know if your security program is failing? They just watched a 15 to 20-minute presentation and it looked great, but the CSO/CISO should be prepared to answer difficult questions like this. And if they can't, then it sounds to me like the program is not complete."

When discussing metrics with the board, Orloff believes avoiding generic language, and instead focus on high-level, business impacting specifics. He explains, "The board should be interested in how many critical incidents there were, what the root causes were, and did we fix the root causes. They shouldn't get into vulnerability and patch management or way down in the weeds on the tactics. They should be focusing on the high-level things that are going to indicate the quality of the program."

THE GROWING THREAT LANDSCAPE AND SPEAR PHISHING

Orloff says traditional security programs were focused on inbound threats and mitigating risks. The approach today has shifted, where teams must figure out what the threats are as categories and put their security programs in place upstream in the data flows or downstream in the technology stack to mitigate those threats. He explains, "One of the biggest threats today is spear phishing. There are different techniques to mitigate phishing attacks that are hitting the servers, but other solutions go further upstream and start to mitigate back at the ISP level. Ideally, we take programs and try to go as far upstream as we can, which gives us more data exhaust to correlate as it's touching our own systems."

According to Orloff, spear phishing presents one of the biggest threats for all verticals. He says since all companies use email, it creates one of the largest threat vectors. With numerous social networks such as LinkedIn, these often are leveraged to craft well-articulated and unique messages to an individual in order to spear phish.

To combat phishing, Orloff relies on best of breed approaches. He says, "The idea is to identify solutions that have the best effective capability, combined with putting a large value on how you measure effectiveness. Don't tell me how many attacks were blocked by the tool, also tell me how many attacks actually made it through. Tell me how and why they made it through."

For Orloff, another critical aspect to combat spear phishing is internal training and awareness. He explains, "When it comes to humans, carbon matters. You've got these spear phishing attacks coming in and now it's all about human behavior and training people to stop, look, and assess that email. Employees need to question whether or not the email 'attributes' make sense."

"There are anti-phishing training programs out there that are very good. I have seen some corporate programs establish a baseline with a high number of employees getting phished. As that training continues throughout the year, the number of people that were successfully phished dramatically reduces. Results like this validates the importance of an anti-phishing training program."

To stay abreast on the latest threats, Orloff takes a strategic, combination approach. He comments, "It's a combination between reading the newest stuff that's coming out as well as being a member of some key organizations, maybe two or three, so you can speak to your peers to really understand what other people are doing and what risks are manifesting out globally."

Aligning with Executives Through Strategic Communication

"When aligning with executives, CISOs must focus on their communication style and more specifically, what they are going to communicate. What I have found to be the most successful is not necessarily going in there and talking about problems and how you're going to fix them. What works best is if you start off with talking about the framework by which we're going to operate the department and the problem-solving strategies that we're going to embrace to identify the root problems. A CISO doesn't have to be risk adverse. What we need to communicate is that we can accept calculated risk, it's important they understand security leadership isn't going to take a position that says I can't accept any risk. There must be a balance to solving important problems, mitigating the less severe problems, and not to be completely shut off to all risk. There are only three things we can do with risk, i) accept it, ii) transfer it, iii) mitigate it. It's not possible to eliminate all risks."

Q&A WITH MEERAH RAJAVEL

CHIEF INFORMATION OFFICER, FORCEPOINT

As an experienced IT executive, Meerah Rajavel excels at delivering transformation, innovation, profitability, and agility for business through technology. She is a passionate leader who inspires and motivates teams to achieve extraordinary business outcomes through entrepreneurial thinking and collaborative cross-functional partnerships. Currently the CIO of Forcepoint, a global cybersecurity leader, Meerah is responsible for digital and operational transformation with a strong focus on customer centricity, scale for rapid growth, and operational efficiency while minimizing risk.

We interviewed Meerah to learn more about her role as Forcepoint CIO, and how Forcepoint continues to be a market leader.

Q: WHAT ARE THE CORE FUNCTIONS OF THE CIO AND IT AT FORCEPOINT?

My team and I have three main functions:

1. Engine of operational excellence

I look at IT as the engine that provides productivity and scalability with operational excellence. Forcepoint is in a phase of rapid growth and my team and I make sure our company scales in a profitable fashion.

2. Nervous system of the company

If you think about IT today, we are the nervous system of the company because we provide foundational infrastructure, similar to how the brain connects the various parts of the body and allows it to perform. IT must work through a significant amount of reliability, availability, and performance factors in order for us to operate smoothly.

3. Guardian of the galaxy

As CIO, I am responsible for the security of the company. But I must also let the business run at the speed they want to run, just in a safe and secure fashion. My job is to protect, not to be a naysayer.

Q: WITH SO MUCH CLUTTER IN THE MARKET, HOW DOES FORCEPOINT DIFFERENTIATE?

The fundamental crux of Forcepoint's differentiation is our human-centric approach to cybersecurity: when identity compromise is the leading cause of data breaches, only by understanding the typical behavior of every user on a network can you easily spot the abnormalities and the risks. Our Risk-Adaptive Protection solutions automatically enforce security policies depending on the level of risk. This adaptive security allows us to provide the highest levels of user and data protection, while giving people the freedom to do their jobs.

Moving from threat-centric to behavior-centric. You cannot only have dynamic products, you must also enforce constantly. Our unique approach to enforcement is how I believe we differentiate ourselves in the market. Through our risk-adaptive technology, users only receive meaningful events and alerts, and the security response and enforcement can be automated based on the risk threshold rather than relying on human intervention. Instead of chasing thousands of alerts, which is not effective, security teams only take action on fewer, higher quality alerts. It is humanly impossible to deal with all the alerts and events without intelligent automation like we provide in place.

At Forcepoint, we truly believe we are going to change the paradigm by focusing on people and all of their digital identities interacting with critical data and technology. Whether they're humans, accounts, or bots, these entities are controlling how data is moving and who should have access to what data. So, from our point of view, understanding the behavior of people is the most effective way you are going to manage and control the flow of your data.

FORCEPOINT + EAST COAST

"Forcepoint has a significant presence on the east coast. When you are thinking about it from a cyber community point of view, Forcepoint is very invested in the northeast region and the eastern region as a whole, due to the government and financial services organizations that we serve in the area. Our CEO Matt Moynahan has strong ties to his hometown of Boston, and we plan to open a new center of excellence in the area later this year."

- Meerah Rajavel

Creating frictionless security. We really believe in the notion of providing frictionless security, which means security teams maintain control, but the security implemented does not introduce friction to the business. Staying frictionless, maintaining control, and preserving privacy--all three are important.

There are so many security players in the market, and security has been a fragmented market for a long time. Today, if you ask any CIO, CISO, or board member what they are looking for, it all comes down to frictionless security—providing the kind of safety the business needs without compromising productivity. How do you keep control over data without introducing the friction? That is the problem Forcepoint is solving.

Q: WHAT IS THE IMPACT OF DIGITAL TRANSFORMATION ON SECURITY?

Digital transformation comes with significant benefits to the business, and opting-in or opting-out is not an option. Opting-out puts you at a large disadvantage compared to your competition.

Digital is disrupting every single industry, and it does not matter whether you are talking to the CISO, CIO or CTO, they all agree. These executives all say their organization demands innovation and speed from them. They are also concerned about how to manage risk, including security, scalability, and performance.

This changes the role of security. Security used to be the 'fence builders' – saying who is and who is not allowed inside. But today, there is no fence. The world is cloud, mobile and IoT, and these environments are synonymous with digital transformation. Even within your own premises, if you take machine learning into account, all of a sudden you are talking about requiring a different level of security. CIOs and CISOs need to understand that introducing new technology means introducing new vulnerabilities -- and you need to bring in security early on in the conversation.

Q: WHAT IS THE "FORCEPOINT ON FORCEPOINT" PROGRAM?

The objective of our "Forcepoint on Forcepoint" program is to use our own cybersecurity products and make them the core components of how we provide security to our own business. I call it drinking our own champagne – we create quality products that we would use ourselves.

It is important to me to protect Forcepoint with our own technology. I call my team the first and best team of Forcepoint product users. We are the lighthouse customer, which means we tell the product team what the customer's pain is, so they can really steer the boat to address the pain. We are also customer zero, which means before the product is released, we have already implemented it in-house.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JUSTIN BERMAN
CISO, ZENEFITS

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 500

ANNUAL REVENUE: Not disclosed; private company

> "... not only is our company safe, but we're using security to make the company more successful."
>
> **- JUSTIN BERMAN**

Justin Berman re-located from New York to the Bay Area over one year ago to become the new CISO of Zenefits, a provider of cloud-based software-as-a-service for managing human resources, payroll, and benefits. The opportunity and core company mission attracted Berman to make the change and move across the country.

As a leader at Zenefits, Berman embraces the company mission to securely deliver products and services that make it easy for small businesses —the backbone of America's economy—to start, run, grow and thrive.

"We're a payroll, HR, and benefits company," adds Berman. "Therefore, we have a strategic focus and commitment to the kind of controls necessary to protect against both external threats and internal accidents. A testament to that ethos: our executive team determined they needed a CISO with a practical, mature view of risk and security."

He continues, "A bonus to that rigorous approach: not only is our company safe, but we're using security to make the company more successful. The kind of capabilities we want to build here are things that give our customers the confidence that not only are we taking care of their data, we're taking care of them too."

Berman values the commitment Zenefits has to their customers. He says their opportunity is to not just think about being safe enough, but to actually make customers safer by virtue of helping them understand patterns of bad or dangerous behavior. He explains, "People use our tools, and expect we do the job well enough so their data isn't going to get lost. I correlate it to the fact that no one's excited when they turn on their water.

But, they get really upset if their water is off. It's the same thing with security. So, to me, while very important, keeping secure is not enough."

EXECUTIVE ALIGNMENT: LISTEN FIRST, TALK SECOND

When forming and building relationships with executives, Berman believes in listening first and talking second. He says CISOs should come from a place of wanting to help executives do the right thing for the business. By relying on strong listening skills, CISOs should understand the needs of executives, then come up with solutions that move both security and solutions to their challenges forward. This approach resonates with executive advocates and skeptics alike.

For skeptics, Berman's approach is to engage with them more than you would others by pulling them into the decision-making process. He explains, "The skeptics are the ones you should educate by having them be the devil's advocate against your program. They will sharpen your ability to convince other people more effectively. You should actively engage the people that are your biggest doubters and do so consistently. You'll end up converting a meaningful chunk of them over time as they gain more and more confidence in your knowledge and plans through first-hand interaction. If you are sharpening your decisions and your arguments with someone who doubts you, then the people who don't doubt you are going to be convinced very easily."

COMPREHENSIVE APPROACH TO THREATS

"When we talk about insider threat, most people mean the malicious employee. I think it's just as important to consider the employee accident. The latter is a far more likely scenario and worth your focus and time as a CISO, more often than the willfully malicious employee," explains Berman. He says for CISOs who are in the beginning phases of developing insider threat programs, the most important first step is identifying what is most valuable to the organization and which employees have access. Most often, insiders use legitimate access to steal; they typically do not attempt to break systems using complex technological methodologies, according to Berman.

The attention insider threats create is due in part to insiders having so much opportunity, yet Berman does not believe the solution is to create massive monitoring functions for each employee. He continues, "It's about monitoring close to the use or abuse of things that you don't want stolen or manipulated. This is because insiders look very similar to a system that's been compromised by an external adversary. They may be different in the sense that an insider has more awareness of their legitimate access. However, once an insider's device is compromised, that adversary behavior can look very similar. So, really remember the value you're driving from an insider threat program is also protecting against external threats."

"There are going to be a set of threats that you have to plan on defending against, and you can look for the steps within those threat actors' playbooks. Determine if you can defend against the whole playbook by looking at each step and evaluating if you can disrupt it."

Berman believes that planning for and controlling insider threats may vary based on an organization's specific viewpoint and needs. He comments, "Every company has a different view of that problem. It depends on what you're protecting first. What is the value in that? Why would they steal something or what could that do to the company? If they're just trying to steal money, then you're really talking about financial controls, which is a lot different than the security controls you might put in place to prevent data theft."

According to Berman, the biggest risks to any organization are often the adversaries specifically motivated by the organization's business. He says, "There are going to be a set of threats that you have to plan on defending against, and you can look for the steps within those threat actors' playbooks. Determine if you can defend against the whole playbook by looking at each step and evaluating if you can disrupt it. There are just way too many actors with way too many playbooks to laser down which specific threat is the biggest problem. It's not just phishing, it's not just ransomware, it's not just any one thing once you get above a certain scale of organization."

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446