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."