PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

NICHOLAS SHEVELYOV
CSO, SILICON VALLEY BANK

HEADQUARTERS: Santa Clara, CA

EMPLOYEES: 2400+

TOTAL ASSETS: $51 Billion

EXPERIENCING THE EVOLUTION OF CYBERSECURITY FIRST HAND

Nicholas Shevelyov, the Chief Security Officer of Silicon Valley Bank says the bank's mission is to improve the probability of success for entrepreneurs all over the world. He explains how his security organization is directly aligned with that mission, "The bank cultivates an ecosystem for innovation. Part of providing that ecosystem is protecting the interests of the bank and our clients in a rapidly evolving digital world."

In his ten years as CSO at Silicon Valley Bank, Shevelyov's role and the role of cybersecurity in general have evolved to be more vital to that mission. He comments, "Technology used to be just a cool innovation, but now technology permeates every aspect of our lives and business. The technology that empowers us simultaneously may imperil us, so cybersecurity is now a fully-integrated aspect contributing to the success of our business."

With a decade of experience to call upon, Shevelyov recalls when cybersecurity's ability to impact business was not as acute. He says, "Ten years ago, or maybe going back twenty plus years when I started in technology consulting at Deloitte, IT security was seen as an offshoot of technology. It was a nuisance for the business. But now the discipline has evolved so much that it is just a matter of good business practice to have a complete cybersecurity program. We are no longer an offshoot of IT. We are integral to the success of the business."

He continues, "Cybersecurity used to be a topic only for industry periodicals, now it is front-page in the Wall Street Journal. The discussion has evolved from the IT conference room to the executive board room."

The industry shift Shevelyov notes has played out within Silicon Valley Bank. He comments, "Our executives and our board are highly engaged. They want to know, 'What are we doing? How do we compare to others? Are we making the right investments of people, process and technology?' We are reporting that information to executives and the board on an on-going basis."

Shevelyov reports that heightened executive awareness is driving cybersecurity's larger role in business strategy. He explains, "I think there is a lot more investment in security-related learning by executives. They are interested in understanding the information we share and often seek out education on their own. They have realized that cybersecurity is something the entire business needs to think about. They understand that we all need to be good security stewards for the ultimate benefit of the organization."

When sharing information with other executives, Shevelyov is careful to consider their perspective. He clarifies, “When speaking with the CEO, I share a quantitative analysis with a qualitative perspective. We talk about our opinions of the assessment but also talk about accurate ranges of hard dollar impact as well.”

Shevelyov’s standing and visibility within the bank has increased over the years, signaling to the entire organization that cybersecurity is a top priority. “Increasingly, I am seen as a peer to other C-level executives at the bank, and that has a big impact on the overall traction and awareness for the security program,” he says.

BUILDING A STRONG RELATIONSHIP WITH THE BOARD THROUGH EDUCATION

Shevelyov describes a “healthy relationship” with the bank’s Board of Directors. His team provides quarterly updates to the audit committee and deeper dive presentations to the whole board as needed. He encourages an open dialogue between his team and the board about industry-wide cybersecurity concerns, and threats. He says, “Typical presentations are only 15-20 minutes but we have also conducted a half-day offsite meeting where we went into all the rules and regulations impacting our program. In the meeting, we examined industry threats and facilitated a more robust discussion.”

More standard presentations to the Board focus on near and long-term security strategy. He continues, “We discuss how we are engaging across the organization and where we are headed over the next few years. We have a first horizon, highlighting where we are today and a second horizon, which projects two or three years out. We also report on a third horizon that is a little more speculative and considers cutting-edge technologies that could impact our world in the future.”

With years of experience in the role of CSO at Silicon Valley Bank, Shevelyov shares a veteran perspective on Board meetings and communicating with executives. He jokes that new CISOs preparing for their first Board meeting should, “fundamentally know thyself and know thy enemy and you will survive 100 board meetings. That of course is tongue and cheek, but you really need to have a technical grasp of the field and be able to analogize, empathize and translate security’s impact on the business. Remember the security team is here to serve the success of the business, so you need to have a multi-disciplinary perspective on the issues. Explain how cybersecurity issues impact the business’ mission and critical objectives. We need to evolve from a technology discussion to a business and operational risk conversation. This is business resilience for the 21st century.”

.

BUILDING A TEAM WITH DIVERSE SKILLS

Shevelyov’s team recognizes that change is a constant in cybersecurity. His organization is structured to ensure changes in risk and threats are addressed with appropriate people, processes and technology. He explains, “I have a traditional cybersecurity operations group and a security engineering team. We also have a Security Analytics and Assurance group which is perpetually measuring and evaluating our programs and identifying where we need to make course corrections.”

Finding and securing the right talent to staff his teams is a priority for Shevelyov. He comments, “According to reports, there were one million unfilled cybersecurity jobs in 2016. I have heard this number will grow to as much as 3.5 million next year. Finding the right talent and the right expertise for our team is a challenge. To address that, we are exploring alternative methods of recruiting. We are widening the net and thinking outside of the box so that we recruit from backgrounds beyond the traditional technology and law enforcement fields.”

He explains, “We are trying to cultivate a network of professionals. We are exploring ways to contact people in other industries and explain how cybersecurity fits into their career paths. Cybersecurity is a broad business problem, so there are many roles that do not require a technology background. For example, governance and information assurance often do not require deep technical expertise. We are doing a lot of measurement in our analytics group, so a classic data scientist can be a good fit for that team.”

Shevelyov is focused on cultivating what he calls “T-shaped professionals.” These are security professionals who may have very deep expertise in a specific technology or area, but also broader knowledge and awareness across the many different aspects of cyber security.

To build out the expertise of his team and to recruit and retain more employees Shevelyov emphasizes education. “Education is essential and fundamental to being a successful professional in the field. We make a very deliberate effort to get employees the right training. We encourage them to network and learn from peers, and add hard skills to their skill set.”