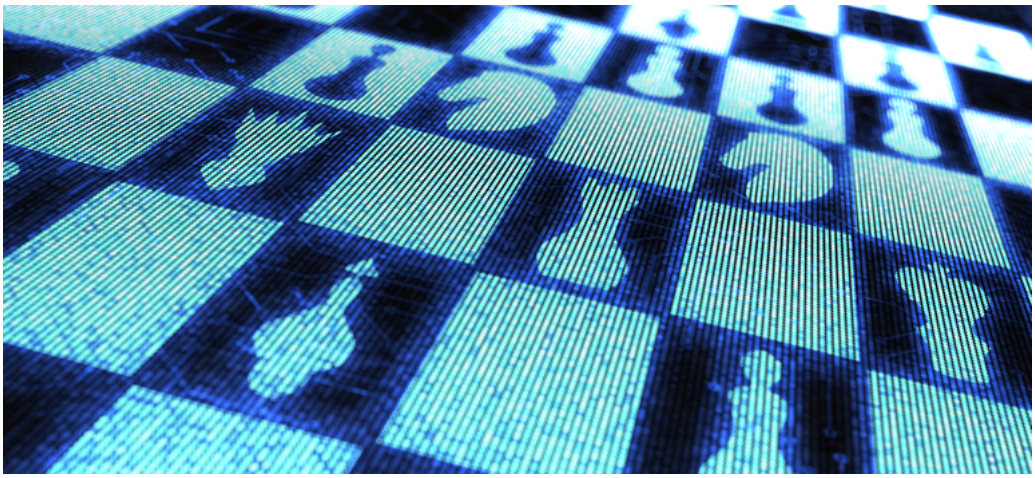
BankDirector.com THE INFORMATION RESOURCE FOR BANKING LEADERS

Needed: CISOs to Play Cyber Chess with Skilled Hackers

By: ***Jack Milligan, editor in chief for Bank Director***
APRIL 13TH, 2017



Help wanted: Highly intelligent and technology savvy professionals who are excited about the challenge of matching wits with equally intelligent and highly motivated digital bank robbers who will always be one step ahead of you.

Allowing for a little bit of creative license, that pretty much describes the challenges facing chief information security officers, or CISOs, a still relatively new position in the banking industry. **As the industry's digital footprint has expanded, so has its risk profile**. There have been a number of highly publicized and not so well publicized incidents in recent years where banks have been hacked. No bank can afford not to have a robust cybersecurity program. Increasingly, bank boards are deciding that they need a cybersecurity specialist to oversee that activity rather than a generalist like the chief information officer (CIO) or chief risk officer (CRO).

In many ways, the nature of a CISO's job reflects the nature of the cyber risks they are trying to contain. "The threats are constantly evolving, so a CISO must take this job with passion and with curiosity," says Sai Huda, senior vice president and general manager at Fidelity National Information Services. "This is a dynamic job, so it has to be someone who is comfortable in a dynamic environment and the demands of keeping up with the latest threats and then trying to understand how all those threats are created and perpetuated. They have to be up on the threats all the time and [understand] how these hackers' minds work."

The role of the CISO is to oversee the bank's cybersecurity program. Huda says the CISO is the organization's "second line of defense" after the day-to-day information technology operational staff, and before the third line of defense, which would include the internal auditing function. The CISO has an enterprise-wide mandate and essentially functions as the chief risk officer for data security. Ideally, he or she will report to the board of directors or the chief executive officer, although other reporting structures could include the CRO or CIO.

The CISO also should be responsible for formulating a cybersecurity strategy, and performing an annual risk assessment like the Federal Financial Institutions Examination Council's Cybersecurity Assessment Tool. He or she also should work with line management to understand what the cyber risks are, and champion security awareness and training throughout the organization—especially since phishing is still the greatest cyber risk that banks face. That's when hackers send an email, usually from a seemingly legitimate source, asking for information or providing a link that compromises the user's computer.

Two of the most important aspects of the CISO's job is, first, to keep senior management and the board appraised of changes in the organization's risk profile. This would include regular and frequent presentations to the board about the bank's risk profile, the cybersecurity threat environment and how that is being addressed.

The other critical aspect of the CISO's job is to oversee incident response and mitigation. **Should a hack take place, the CISO is essentially chief of the bank's cybersecurity fire department**. "It's only a matter of time before a hacker or malicious insider penetrates [the bank's defenses], so the key to success is detection and response to protect the crown jewels," says Huda. "And the CISO's role is to oversee timely detection and effective response. Ideally, operations would use a technology tool to detect possible threats and vulnerabilities, or a breach. And then the CISO would oversee the timely execution of the incident detection and response plan and prevent a cyber disaster."

Victor Vinogradov joined Western Alliance Bancorp., a $17 billion asset bank holding company headquartered in Phoenix, Arizona, as CISO in 2015, bringing with him 24 years of experience in information technology, 15 of them spent in the security field. Prior to joining Western Alliance, Vinogradov worked as a consultant and was director of network security and services at Charles Schwab. He says his role is to understand the bank, its businesses,

the regulatory environment—and perhaps most importantly, the threat environment it operates in. “I need to have a process to assess those, [develop a plan] and implement ways to mitigate those risks, and then communicate to the [bank] risk committees and the board how that plan is working,” says Vinogradov.

One of the challenges that Vinogradov faces is to work closely with the business units so that Western Alliance has a cybersecurity process in place to protect the bank without interfering with their work. “I need to be flexible to apply the right techniques that fit the business and keep those controls as transparent as possible so that security is behind the scenes but doing its job of protecting the environment,” he says. (Vinogradov also serves as the bank’s chief security officer where he oversees all of its security programs, including physical security.)

Vinogradov delivers a monthly report to the bank’s various risk committees and a quarterly report to its board of directors. He currently reports to Western Alliance’s chief information officer, although some experts believe that a **best practice is to have the CISO report to someone other than the CIO, preferably the CEO or the board itself**. He credits the Western Alliance board with having a good understanding of the complexity of the cybersecurity process and the threat environment that the bank operates in, although he takes advantage of every opportunity to educate them about how those threats are being mitigated because—as he puts it—“the risk is not going to be totally eliminated.” “I go as deep as they want to go into the controls that are available,” he adds. “It’s a combination of a discussion and a presentation of our current status in terms of risk mitigation.”

Vinogradov also credits the board with taking cybersecurity seriously, and communicating its importance throughout the organization. “If the CISO doesn’t have the board’s ear, making progress would be a challenge,” he says. “The tone at the top in our firm is that they have mandated security as a top priority.”

Does every bank need to have a fully dedicated CISO? Huda says that, ideally, yes. **If the bank doesn’t have a CISO, it certainly needs to have a cybersecurity program in place** and regulators expect the board to make sure that is in place, according to the FFIEC’s IT Exam Handbook. “I think the smaller entities, depending on their complexity and risk profile, have some flexibility to use either a consultant or have some other officer wear that hat,” says Huda. There’s no specific asset size where a bank needs to hire a CISO. “But the driver here is the risk profile,” Huda says. “A lot of times smaller entities think, ‘Well because I’m small, I don’t need that specialization or focus.’ That’s a mistake.”

Because the CISO function is still relatively new to the industry, banks that want to hire one can have a difficult time finding qualified candidates. “If you’re going to hire somebody internally for a full-time position it’s going to be a tough ball game because there’s a shortage of qualified CISOs in this country,” says Huda. “However, the military or law enforcement could be a great area to look for well trained, qualified potential CISOs. These are special people who are defending against cyber threats daily,” he says. Huda also suggests that universities that offer advanced degrees in cybersecurity are also possibilities. A third option, says Huda, is to select someone already working at the bank and pay to have that person trained.

One of the challenges that small banks face when they try to establish a cybersecurity program is a general lack of internal expertise when it comes to technology because they are so reliant on their core technology provider for most of that infrastructure, and also the management talent to run it. “What that translates into is that **a lot of times there’s nobody internally who fills the strategic CIO role let alone the CISO role**,” says David Hartley, a principal at UHY Advisors, an accounting and consulting firm. “If you’re a smaller community bank and you’re relatively lean and you don’t have anyone who really understands or deals with technology matters, you’re probably going to rely on a partner.” A third party could come in and help the bank design and implement a cybersecurity program, including a risk assessment. That same entity could help manage the program on an outsourced basis, with either the chief financial officer or chief risk officer overseeing the process internally, Hartley says.

If the bank is in a growth mode, either by acquiring other banks or adding new businesses, it might need to bring the CISO function in-house. This is especially true if the bank is adopting new technology like mobile, which also will alter its risk profile.

“Eventually, cybersecurity becomes such a specialized and such a large issue that I would see the CRO, CIO or CFO not having the skills or time to focus on the problem,” says Vinogradov. “As the bank grows it demands the attention of a full-time, internal CISO because of the scope and complexity of it.”

Jack Milligan is editor in chief of Bank Director, an information resource for directors and officers of financial companies. You can connect with Jack on LinkedIn or follow @BankDirectorEd on Twitter.