Cybersecurity Is Job #1 for Banks. But Whose Job Is It?

Andrew Kim
Director – Technology Risk Management and Cybersecurity, RISC Solutions
A New Reality

In 2016, cybersecurity is on the mind of every corporate executive. And for good reason. Cybercriminals are targeting banks with increasingly sophisticated methods. One U.S. state examiner recently called cybercrime “an existential and immediate threat” to banks both large and small. No wonder cybersecurity is the top concern for banks today, according to Bank Director’s 2016 Risk Practices Survey. Even the FBI is deploying agents, analysts and computer scientists to combat cyberthreats.

Given the potential impact of a breach or powerful, enterprise-paralyzing malware, it’s fair that executives are wondering what role they need to play, asking whose job is cybersecurity anyway? Who in the bank is responsible for understanding the cybersecurity threat, mitigating it and protecting against potential catastrophic losses?

Traditionally, the answer to that question has been the chief information security officer (CISO). CISOs, after all, are the stewards of the networks where cybercrime often occurs. Protecting those networks is their job, which is why CISOs have the budget for information security tools and resources.

But criminals know this better than anyone, which is why they are actively and methodically searching out less-traditional and less-guarded avenues within the bank for their next cyberattack.

The reality is that in today’s hyper-vigilant banking environment, the cybersecurity threat is an enterprisewide concern with significant accountability across the C-suite.

Chief Operating Officer

When we come across chief operating officers (COOs) who still consign cybersecurity to their CISO colleagues, it raises the obvious question: Where will the impact of a successful penetration be experienced first?

That impact is likely to be in operations, where COOs are charged with serving customers and keeping the branches up and running, money in the ATMs, call centers responsive, accounts accessible, payments moving efficiently and so on.

One COO put it this way, “I don’t have to be a cybersecurity expert to be fully aware that an intrusion could be catastrophic for the areas I’m responsible for. Whether it’s a DDoS that knocks our customers offline, or an ATM system penetration that keeps customers from getting their hands on cash, or branch system malware that renders our branch people inoperative – no matter what form it takes, it’s going to be a nightmare for bank operations."

That’s why it’s vital that COOs be prepared by running realistic scenarios of potential cybersecurity attacks and mitigation response plans. If our ATMs are attacked, where would the earliest indications be? If our call centers are suddenly flooded, how do we quickly identify whether it’s a cybersecurity event? Who makes sure that a minor cybersecurity attack isn’t a distraction from a larger intrusion? Our wire system is slow today – what’s going on? Who reacts and how?

Chief Risk and Officer and Chief Compliance Officer

The chief risk officer (CRO) and chief compliance officer (CCO) likewise face a new set of challenges now that cybersecurity has skyrocketed to the top of the bank’s priority list. These officers traditionally delegated cybersecurity worries to the technical types – the CISO or the chief technology officer (CTO) – and focused instead on keeping their banks on the right side of the law and guarding against liquidity and capital risks.

But thanks to the stress tests conducted after Dodd-Frank, regulators already understand your bank’s compliance operations and risk tolerance. They are shifting focus to how well the bank calculates and understands its exposure to potentially devastating cybersecurity risk.
According to *Bank Director*, “Many banks have yet to fully utilize the [Cybersecurity Assessment Tool](#), developed by the Federal Financial Institutions Examination Council and made available to banks in 2015 ‘to help institutions identify their risks and determine their cybersecurity maturity.’"

No longer will regulators be satisfied with assurances that the CISO or CTO is on guard against cybersecurity. They will expect to see cybersecurity risk clearly articulated, evaluated and prioritized within the bank’s overall enterprise risk and compliance profile.

**Chief Executive Officer**

Here’s what tuned-in chief executive officers (CEOs) are saying about cybercrime: "It’s not technology. It’s theft – plain and simple. No matter how it unfolds, it’s stealing the bank’s money or information. Sure, it involves using sophisticated software and the internet, but cybercrime at its most basic involves unauthorized transactions."

Therein lies the CEO’s nightmare: a call from a customer saying, “I didn’t approve that transaction. Why did you execute it?” What’s different about cybercrime is how fast it can happen and how much money can be lost. Consider the S.W.I.F.T. hackers who nearly got away with stealing a billion dollars.

That’s why regulators today are increasingly firm about the CEO mandate. In today’s environment, CEOs can’t delegate away responsibility for any aspect of compliance, whether it’s Sarbanes-Oxley, financial reporting or cybersecurity. The FFIEC explicitly directs bank examiners to assess management awareness, participation and mitigation of cybercrime. That’s why CEOs of leading banks are regularly, routinely and substantively briefed on their banks’ cybersecurity measures.

**Developing a Common, Enterprisewide Playbook**

Clearly, all of these C-officers have a significant stake in preventing cybercrime. No single department within the bank has the resources or the 360-degree perspective needed to anticipate and mitigate threats.

That’s why it’s critical for today’s banks to work from a common playbook – a consistent, enterprisewide view of networks, data and processes needed to detect cybersecurity anomalies and vulnerabilities before losses happen.

If your bank doesn’t have such a playbook, best get started right away in developing one before the criminals – and the regulators – take notice and head in your direction.

**About the Author**

Andrew Kim is director of the Technology Risk Management and Cybersecurity Practice at FIS, where he consults with financial services clients to assess their cybersecurity risks and implement enterprise-class information security programs. Prior to FIS, he was chief information security officer at One West Bank and also served as vice president of information security at Citigroup. He has also held senior IT security roles within the insurance and asset management sectors.