THOMSON REUTERS

# Five critical points for bank boards' cyber risk agendas

**Jan 30 2017** Rachel Wolcott, Regulatory Intelligence

The risk that cyber criminals pose to banks and financial services infrastructure is not new but if there is a single lesson to be learned from available trends during 2016 it is that complacency is lethal.

Hacks into the Democratic National Committee may have dominated cyber crime coverage, but serious incidents have occurred in the financial services sector. Hacks of the SWIFT payment system led to breaches and losses at emerging markets banks. The $81 million Bangladesh Central Bank heist was the biggest loss related to the SWIFT hack.

In November Tesco Bank, a UK retail bank, saw £2.5 million stolen from 9,000 retail customers, which is said to be the biggest known raid on customer accounts in a developed market. Experts blamed the Tesco hack on anaemic investment in cyber security and a corresponding lack of interest in cyber risk at board level.

The SWIFT-related attacks were blamed on a combination of spear phishing, a well-known technique employed to gain user credentials, and the subsequent deployment of malware used to send fake SWIFT messages.

Emboldened by success and lack of prosecutions, cyber criminals will continue to exploit weaknesses in banks' IT infrastructures and cyber security measures. Earlier this week, Lloyds Banking Group was the latest bank to reveal it had been the victim of a lengthy denial of service (DoS) attack, which locked out some customers from online banking services.

"The rewards for cyber criminals are high and the risks are questionable. There is an elevated level of data in motion that criminals target, where in the past they targeted databases and tried to dig into them. Now they are more like medieval highwaymen holding up travelers," said Viktor Andonov, head of DataArt's Bulgarian operations.

Addressing cyber risk is not simply a case of spending money on security. Banks' boards, especially those at smaller, more vulnerable institutions, must increase their awareness of cyber risks and educate themselves. Following best practice, examining third-party vendor risk, retiring old IT and applications, developing meaningful employee education and setting a risk tolerance for cyber crime are all part of the approach boards ought to be advocating.

**1. Keep best practices, regardless of regulatory requirements**

Regulators, especially the U.S. Securities and Exchange Commission, have sought to promote awareness of cyber threats in the past three years. The SEC, together with the Office of Compliance Inspections and Examinations (OCIE), have sought to promote best practice in cyber crime risk management, making it part of routine inspections. Other regulators include cyber security assessments as part of operational and information technology risk assessments.

In the United States most firms have been following the National Institute of Standards and Technology's Cyber Security Framework.

The Trump administration's anti-regulatory rhetoric has some security experts concerned that U.S. regulators' cyber security programmes will disappear. They have been warning firms to keep up their security programmes and budgets regardless.

"There's a lot of uncertainty right now with regulation. Now regulations are potentially in jeopardy with the new administration, we don't know what's going to happen. Follow best practices regardless of regulation. If we do get regulations you'll be in a good position to meet those requirements. If regulation does go out the window, you'll still be in a good position because you'll probably have better controls than your competitor," said Josh Barons, director of security at Abacus, an IT company catering to the alternative investment sector.

The OCIE's 2015 report underscored the importance of best practice and good security: "A majority of the broker-dealers (88 percent) and the advisers (74 percent) stated that they have experienced cyber attacks directly or through one or more of their vendors."

Andonov estimated that 57 percent of enterprises did not have a consistent cyber security control framework and that attack management and security patches were not deployed properly. Reducing cyber security and failing to follow best practice will only make it easier for cyber criminals.

**2. Third-party risk**

The European Banking Authority's latest Risk Dashboard highlighted operational risk related to IT risk and cyber crime. That included third-party or outsourcing risk:

"As banking operations increase their dependence on IT platforms and telecommunication networks, concerns about connectivity and outsourcing to third-party providers have increased. Operational risks are also negatively affected by fragmented and ageing IT systems. Cyber attacks remain a threat."

"Vendors don't always follow the same security standards firms expect. Be careful and go through security checks with them," Andonov said.

Third-party or vendor risk is potentially a big problem for firms seeking to shield themselves from cyber crime. Firms must ruthlessly evaluate third parties to make sure their systems and controls are up to standard. They should identify their data and its sensitivity, then examine how that data flows from their firm to third parties. That could be an administrator of investor data or a company that destroys documents. Firms must ensure third parties have security controls in place.

"It's also important the firms have contractual controls with third parties. It's not just doing due diligence, it's also important that the third party is contractually obligated to notify you if they have a breach that can impact your data," Barons said.

Firms also need to look at whether software vendors are designing software with security in mind.

"People need to ensure that software is designed with security in mind. There's no use plumbing in security after the fact," said Russell Stern, chief executive at SolarFlare, a New York-based IT security company.

**3. Turn off obsolete IT systems and applications**

The EBA's Risk Dashboard emphasised the risk posed by ageing IT systems. According to experts, that does not just mean a risk of system failure; legacy applications give criminals an entry. Leaving legacy systems running can greatly reduce firewall effectiveness.

"Banks have 8,000-10,000 legacy applications, some of which were developed on visual basic and they'll never touch again. One of the problems with firewalls is there are still legacy applications that use a communication program called Telnet, a low-level protocol to communicate between computers. It's still being used. If I turn it off, the legacy applications don't work. I spend a lot of money of firewalls, but I leave the Telnet ports open," Stern said.

Almost all large, established banks share this particular IT risk. The risk is well-known, but banks put off addressing it regardless. Ignoring it invites cyber criminals and serious system breakdowns.

"The best thing is to get rid of deprecated systems. You don't want to have something that's not running and is a potential vulnerability. It's a big risk. In mergers and acquisitions, firms will inherit an old system. They're told, don't touch it, don't patch it — but if it goes down, the whole infrastructure goes down. There is jeopardy there. They have to look at the code and see what this system is actually doing. Or they take the risk and turn it off to see what is actually impacted," Barons said.

**4. Education and training**

The Bangladesh Central Bank heist and the attack on the DNC both relied on one of the oldest tricks in the hacker's book: phishing. That is when a hacker tricks a target into revealing their security credentials using a spoof email claiming to be from a colleague or a vendor.

Once a hacker gets into the system they can either steal information, such as the DNC emails, or set up malware to infiltrate the system further, which is what happened in the Bangladeshi robbery.

A lot of that, Stern said, could be solved through training, and instilling a culture of good cyber hygiene. People need to get into good habits, such as having two-step login authentication, and generally need to be more suspicious.

"There's another whole classification of human/cyber exposure that's just based on education. Tackle the human behaviour aspect of this and you've got about 80 percent of this problem nailed. It's unbelievable how uneducated

people are," Stern said.

There is almost always a human element to these hacks.

**5. Define risk tolerance**

Firms should think about how much cyber risk they are willing to bear from web-facing systems, smart phone apps and open source software. Stern said it could be time to think about making some trade-offs and scaling back the trend toward web-facing systems.

"There's this trade-off we're making in the world of building networks and data centres. We want to make computing cheaper, easier, open source, open switch, open compute. The irony is the companies that promote open source software secure it and use it in their own proprietary manner. There have been a lot of cyber attacks lately. Guess what? The crooks can read the open source software. They have the ability to determine where the vulnerabilities are," Stern said.

He pointed out that private networks run from data centres under true physical security —infrared, video surveillance, locks and armed guards — were always the most secure. The more infrastructure is built on web-facing interfaces, the less secure it is. Should firms sacrifice convenience and customer service for security?

"There is no one-size-fits-all. It depends on the practitioner. It depends on the firm's risk tolerance. The key there is the firm needs to know what their risk tolerance is," Barons said.

Original article — https://www.complinet.com/editor/article/preview.html?ref=191119