Op risk experts question banks' cyber strategy

Cyber attacks are associated in the public imagination with high-tech data breaches and denial of service attacks, perpetrated by organised rings utilising sophisticated techniques. The reality of cyber risk is much more mundane, though no less serious

Cyber crime generally conjures up images of organised criminals and foreign spies operating out of secret underground lairs, or basement-dwelling teenage hackers.

"The danger is people think of the funky, James Bond-type hacking when they talk about cyber," says Sam Lee, the UK-based head of operational risk at Sumitomo Mitsui Banking Corporation (SMBC). "I think it's dangerous to do that."

Things as simple as an unattended desktop or an unprotected password are the most likely causes of cyber breaches – and can wreak as much havoc as a targeted attack by cyber criminals. The problem, operational risk experts say, is that firms spend all their time and energy locking the front door to their vital data, systems and infrastructure – spending huge sums on the latest firewalls and encryption systems – only to leave the back door wide open.

"Stupid hurts just as much as malicious," says Mark Clancy, chief information security officer at the Depository Trust & Clearing Corporation (DTCC) in New York. "Employees are trying to do the right thing, but they make mistakes."

Clancy recalls an incident at a company he used to work for when a client who asked for a copy of their tax information was mistakenly sent a spreadsheet containing data on all the company's clients. "Mistakes can cause problems because data is sensitive," says Clancy. "It needs to be protected and occasionally it's mishandled."

Most operational risk professionals understand that human error – rather than malicious attacks – is often the single biggest cause of cyber security breaches. "The human risk is always present and can create significant risk for companies," says Rich Baich, North Carolina-based chief information security officer at Wells Fargo. "Whether it is human error on the technology side or a lapse in judgment by an employee on the front line, we must continue to have strong education and awareness programmes."

But many financial institutions "still haven't understood the full ramifications of what cyber risk is, and they think about it as just hacking and are spending a huge amount of money", says SMBC's Lee. "In that regard, sometimes the investment does not match the likelihood of it occurring or the damage it could cause."

Banks often talk themselves into "throwing heaps of money against the possibility that someone who is extremely clever is targeting you, and preventing that" instead of "looking at expenditures to close down the easy routes for data loss and data theft", says Lee. "Do you throw all of your millions of budget to prevent that one-in-a-hundred-year event from happening, or do you say, ‘let's be a little bit more sensible'."

On high alert

In some respects, financial firms are responding to calls from regulators to shore up their cyber defences. Some have gone so far as to suggest a cyber attack might be the most likely cause of the next financial crisis.

"When I think about the risks that might cause the next crisis, cyber security is one that concerns me the most," Sarah Dahlgren, the then-head of the Financial Institution Supervision Group at the Federal Reserve Bank of New York, said at the OpRisk North America conference in New York on March 24.

Dahlgren urged financial institutions to secure their data and IT infrastructure and made it clear that regulators would be watching closely. "There is still a great degree of clean-up to do to fix long-standing data and technology issues that have built up over the years," she said. "Cyber security is the new normal. It will become part of our vocabulary in almost every exam that we conduct, every conversation with senior management and every conversation about the future of financial services."

Regulators are not the only ones pushing banks to think more carefully about cyber security. Although cyber breaches have not led to any downgrades to date, rating agency Standard & Poor's warned in a report published on September 28 that it regards cyber security as an emerging risk that has the potential to result in negative ratings action.

This could happen in two ways, S&P said: a bank could be downgraded before an actual attack if the rating agency believes it is ill-prepared to withstand a cyber attack; or it may downgrade a bank after the event if a security breach causes significant reputational damage and a major loss of customers.

Chief among risks

Despite these constant warnings, there is little evidence to suggest that financial firms are behind the curve when it comes to cyber security.

A survey of cyber security governance published on October 2 by the Information Security Center at the Georgia Institute of Technology found the financial sector has the highest percentage of chief information security officers of any industry at 88%, with IT and telecoms coming in second with 86%. The survey also found 79% of boards of directors in the financial sector have oversight of computer and information security – up from 44% in 2012 when the survey was last conducted.

Financial sector boards are paying close attention to the governance of cyber security, such as reviewing security programme assessments and top-level policies, assigning roles and responsibilities for privacy and security, and receiving regular reports on breaches and IT risks, according to the survey.

But not everyone thinks this attention is warranted. At the OpRisk North America conference on March 24, Craig Spielmann, former head of operational risk in the Americas for Royal Bank of Scotland, challenged Dahlgren's claim that a cyber attack could cause the next financial crisis.

"We just lost $2 trillion to $3 trillion because of the way banks conduct their business, so when I hear that [cyber risk] is the top risk, I think it is a distraction. The way businesses make money is the biggest risk to the financial system, and my proof is 2008, where banks that have been around for all these years disappeared overnight. That is not going to happen as a result of a cyber security problem, it's just not," he said.

So are financial firms wasting time and money trying to thwart the cyber bogey man?

Not necessarily, says Baich at Wells Fargo. The investments in resources needed to deter attacks by hackers, cyber terrorists and organised criminals are justified by the potential losses that could accrue should these attacks succeed, he says. "Yes, it is warranted and it has never been more important. Even if you have not had an occurrence or breach, you must prepare and be ready for potential attacks. The scope and severity of attacks have increased in recent years, thus driving the need for all responsible parties to be prepared."

Cyber criminals are using sophisticated attack methods with speed and stealth, Baich adds. "The time from breach to breach can be seconds. Investing on the front end and focusing efforts on the evolving risk landscape, new technologies and business processes can help companies be prepared for possible attacks."

"It's rightfully a very hot topic," agrees Luke Moranda, chief information officer at the Chicago-based Options Clearing Corporation (OCC). "It's something our board is very sensitive to. We supply monthly cyber risk updates to our board. So it is definitely an important topic that has gotten a lot of exposure."

Although there haven't been any successful hacking incidents at OCC, that does not mean the threats do not exist. "We track the metrics every month," says Moranda. "We can tell people are probing our firewalls, looking for vulnerabilities. We know we get malware targeting us. Nobody has gotten close to getting through our defences, but we can see the probing happening."

Damage limitation

In addition to keeping potential attackers from breaching a company's network or data, firms also need to figure out what to do to contain the damage should they succeed, Moranda says.

"As much as we try to prevent people from getting in, we know a sophisticated attacker with enough time and money will find a way in," he says. "We focus on prevention, but we also focus on containment, so if somebody does get in, how do we keep them from moving laterally through our systems to find more information?"

As a systemically important financial market utility, or Sifmu, OCC works closely with its primary regulator, the US Securities and Exchange Commission (SEC), which annually reviews its cyber security as well as its overall operational controls and technology environment. OCC also works with other federal agencies such as the Department of Homeland Security and the Treasury Department to share information on cyber threats, says Moranda.

Still, operational risk experts say many of the risks that are labelled as cyber risks are in fact weaknesses in internal controls – an issue that Clancy of the DTCC refers to as the "hygiene" of the environment. "A lot of the breaches occur when there is a breakdown in a control process that was designed to maintain the hygiene of the environment, that is, making sure that all the windows are closed and locked," he says. "The basic axiom is if it's important enough to the attacker, they'll invest the time and money to go after the target. But attackers will only work as hard as they need to in order to succeed.

In Clancy's view, an analogy can be drawn between a cyber attack and a burglar attempting to enter a home, where the burglar can employ either a brute-force method to break in, such as using a crowbar, or simply jiggle the handle of a door to see if it opens. "It's very difficult in media reporting to tell the difference between those two events," he says. "The challenge is you read, particularly in mainstream media, that those are the same story, and you have no idea which of those scenarios just happened. To me, they're very different."

Part of the problem may be a tendency to view cyber risk as a proxy for other forms of information security risks. Isaca, a professional association for IT governance, has enumerated three forms of IT risk: IT benefit/value enablement risk (associated with missed opportunities to use technology to improve business processes); IT programme and project delivery risk (associated with the contribution of IT to new or improved business initiatives); and IT operations and service delivery risk (associated with keeping systems operationally available, stable, protected and recoverable).

"Headline-grabbing hacking incidents are just a fraction of broader IT-related business risks," says Brian Barnier, risk adviser at Isaca. "When people overemphasise a specific slice of protection and they miss all those other risks, they end up in huge trouble. All these things have nothing to do with what is narrowly defined by the screaming bells and ringing of the latest hacking incident, but all are things that cripple companies."

Alexei Miller, managing director at DataArt, says: "The funny thing is those headline-making incidents are most often caused by some mundane operational lapses. The general public would be amused to know how much of a cyber criminal's success is driven not by some ingenious technical ninja tricks, but rather by exploiting simple human vulnerabilities."

A recent example is the hacking of financial newswires for sensitive unreleased news, in which perpetrators stole approximately 150,000 confidential press releases from the servers of newswire companies, and then traded ahead of more than 800 stolen press releases before their public release. The attackers employed a variety of tactics to gain access to the newswire companies' servers where the press releases were stored, including posing as employees of the newswire companies, the SEC said.

Iain Wright, head of enterprise and operational risk at Sun Life Financial, says that his company's investments in firewalls and incident response mechanisms are justified because the "downside is so great in not being able to protect our customer and employee data".

At the same time, it's also investing in "peripheral protections", he says. "Recently, our focus is much more on things such as ‘Are people aware of an innocuous looking email and why they shouldn't click on that link?' It's an interesting risk because it continues to evolve, it's not one of those risks you put on a heat map and doesn't change."

Is cyber an operational risk?

As cyber threats continue to evolve, financial institutions are seeking to bring cyber risk management into the fold of traditional operational risk management.

Since by definition, operational risk is any risk that is not market or credit risk, cyber risk is an operational risk, says Bill Sweeney, US financial services evangelist for technology and consulting firm BAE Systems Applied Intelligence.

"The traditional goal of operational risk management is to ensure that the enterprise will survive financially from any form of business loss," he says. "Some of the operational risk practices, such as risk control self-assessment, are extremely useful for cyber risk assessment."

Sweeney recommends pairing an operational risk expert with the chief information security officer to review all business vulnerabilities with a view on cyber, and calling it "CRCSA – cyber risk control self-assessment".

At the Options Clearing Corporation, for example, chief information officer Luke Moranda collaborates with chief risk officer John Grace in constructing key risk indicators, or KRIs, so it can quantify its cyber risk exposures to the board of directors, and in tabletop exercises.

Individuals from Moranda's management team sit on the company's enterprise risk management committee, and are also represented on the model governance committee.

"There are several committees that John's team and my team are plugged into together to match the project delivery and the technical delivery to the risks," Moranda says.

Rich Baich, chief information security officer at Wells Fargo, agrees that cyber risk management needs to be viewed holistically by both the operational risk and IT functions. "Security is not just a technology issue, it is an operational and business issue as well," he says. "To operate securely, everyone has to be on board and partner across the organisation to understand the risks present and the remediation needed."

As a risk category, cyber risk, and information security in general, is a subset of operational risk but overlaps with IT, says Sam Lee, head of operational risk at Sumitomo Mitsui Banking Corporation. In some companies, information security exists alongside IT on the organisational chart, and in others it resides within IT. "In many ways, it doesn't matter," says Lee. "It's not about having one department called Info Sec. It's about having a proposition that cuts across all the relevant functions."

A problem shared...

In a 2014 white paper, the US Depository Trust & Clearing Corporation (DTCC) noted that the systemic risks posed by cyber threats can best be mitigated by "a truly co-ordinated approach that includes both private and public sectors across industries and national boundaries".

Critical to these partnerships is collaborative information sharing by industry participants, governments, academics and other private and public sector stakeholders.

In order to counter the threat of cyber attacks, there are a number of sector-led cyber security initiatives which have been forged with the objective of protecting the resilience of critical infrastructure organisations, including financial services firms and others worldwide.

Soltra, a cyber threat information sharing service founded last year by the DTCC in partnership with the Financial Services Information Sharing and Analysis Center, has 2,000 users at 1,600 companies across the financial services and other industry sectors.

"The thesis with Soltra is that I may get a hundred threats I have to deal with as a CISO every day," says Mark Clancy, chief information security officer at the DTCC. "Eighty percent of them are probably not going to hurt me very much, and only 20% deserve my attention. What we're trying to say is, let's expend very little human effort on what we already know, and focus more effort on things that are risky and complicated."

Original article — http://www.risk.net/operational-risk-and-regulation/feature/2430089/op-risk-experts-question-banks-cyber-strategy