Accountability for a data breach

In March 2013 the US Senate Select Committee on Intelligence named cyber risk as its top global threat. The committee said that the global system was dealing with uncertainty and doubt in the face of new and unpredictable cyber threats. The report pointed out that within the past year, there has been a denial-of-service campaign against the public websites of multiple US banks and stock exchanges, with servers being flooded with traffic, often preventing customers from accessing their accounts via the internet.

IT sabotage was one of Operational Risk & Regulation's top 10 risks for 2013, and in a speech in November 2012 Atlanta Federal Reserve Bank president David Lockhart said the increasing incidence and heightened magnitude of cyber attacks suggests the need to update thinking on cybersecurity. "What was previously classified as an unlikely but very damaging event affecting one or a few institutions should now probably be thought of as a persistent threat with potential systemic implications," he said.

This continued rise in cyber threats only serves to remind financial institutions of their vulnerabilities in this area. And with this comes the question of where accountability should lie within an institution when its cyber infrastructure is breached. In global financial institutions that serve markets across numerous jurisdictions, maintaining sound and secure cybersecurity is a mammoth task. And when that security is breached, someone has to be held accountable.

Forms of attack

There are many ways in which a financial institution can find itself the victim of a cyber breach. The risks can be external or internal, via hardware or software, through people, machines or both – and can threaten customers' private information as well as that held by the bank. The most visible attack is an attack that impacts customers directly. And this can come in different forms, explains Greg Bell, Atlanta-based services leader for information protection at KPMG.

"Attacks specifically impacting your customers may be an attack by a malicious third party seeking to gain personal financial information over your corporate and individual accounts or perhaps fraudulent activity that uses the attack to actually gain access to the funds in an account."

According to Chip Tsantes, a Washington-based principal for information security advisory services at Ernst & Young, the most public type of breach in financial services is one in which personally identifying information is exposed or lost. He points out that in the US, most of the states have reporting laws that require companies to notify customers when their data has been compromised, meaning the public always hears about it. This perhaps makes it the most well-recognised threat, but it is certainly not the only threat banks are facing. "Other types of breach might be the loss of intellectual property, which might be business-level information, acquisition information, software code or other business secrets," he says. "Any intellectual property an institution owns that gives them competitive advantage might fall victim to a cyber breach."

On top of this, Bell points out that there is a new type of attack that is gaining in prominence.

"Attacks against operational information that financial institutions may have are increasing. Examples of that might simply be patterns of trades. They are not necessarily going after the discrete trade itself, but we are seeing big movements going across large sectors of industry or large specific, financial trades that may check off that something may be happening."

Attacks can also come in the form of a targeted attack against the internal general ledger or financial reporting of a bank before it is released to the public, with the aim of making money through insider dealing, says Bell. "If I know a certain bank is going to miss their earnings increase and I can make profit that way, I might target them that way," he says.

Carrying the can

With all these threats on the table, financial institutions have to ask themselves who holds responsibility for their cyber breaches. As the risk increases and more breaches occur, regulators – and the companies themselves – will also be looking for someone to blame. But that is not as simple as it sounds, according to Bell.

"It's a pretty broad set of responsibilities," he says. "We use a term in a lot of cases called 'due care' because often there is a regulatory action or a class action lawsuit that can do the company harm after an incident has happened and people are going back and seeking attribution."

He explains that, in such instances, regulators, plaintiffs and courts will seek to establish whether the organisation demonstrated due care around common controls: while a company

may have firewalls and monitoring in place, for example, questions might also be asked about the training received by the individuals involved.

Bell says: "[They will ask,] did that person receive training from the company on how to differentiate between sources, not to open attachments from untrusted sources? And did the company avail itself of all practical and reasonable approaches to educate that individual?"

If the company did, he points out, then while it is always liable because it is the company's information security that has been breached, its full culpability may be minimised by the fact that it took due care. "They trained their people well and that person still acted on their own cognisance and did not take into consideration the training that he or she had been given. That is where accountability becomes tricky."

Bernard Zelmans is general manager for Europe, the Middle East and Africa at cybersecurity firm FireMon, based in Varbonne in southern France. He says that the key to dealing with such issues is pushing accountability down into the organisation. On top of this, it is critical that cybersecurity is given its due consideration at the beginning of any new project.

"An organisation has to make cybersecurity an inherent part of any new project or any new application when it is started, because if you build an app and then bolt security on later at the end of the process, you have no chance," he points out. "To withstand the onslaught that is coming, being able to push security down into the organisation is key. You need to ensure that people are taking the appropriate steps with the appropriate tools on a daily basis to secure the applications and processes that they are responsible for. It's not enough doing it just once a month if there's an internal report due, or once a quarter if there's an outside compliance audit required, for example."

KPMG's Bell agrees that financial organisations need to be vigilant in implementing new controls when launching new services, in particular those that may be internet or mobile based. He also points out that such firms should be doing continuous assessments of where their vulnerabilities lie. "When you have got a mature organisation that takes these approaches, their culpability is less. The company is always going to be culpable when they have had an issue, even if they have done everything in the world right, but actions like these may be the difference between a $100 million class action lawsuit and a $5 million fine."

And accountability for such a breach needs to be considered at various levels within the institution – including the individual, the departmental head, the risk team, the security team and the chief executive, points out Joram Borenstein, vice president at US software vendor Nice Actimize.

But trying to assign accountability within a financial institution is not a straightforward finger-pointing exercise, Borenstein says. "To really understand accountability, all the bodies and groups within an organisation need to be collaborating, interacting and communicating. If they are not doing that then it is almost not fair to assign accountability to any one individual or one team," he says.

Ernst & Young's Tsantes agrees. "We don't typically do witch-hunts looking for who should be persecuted. We look at what things are obvious that need to be changed to get the most value to improve the security posture of the organisation in the short term and then make
recommendations in the medium term. Those always go across technology, people and processes – it is never just one thing."

But Denis Beau, director general of operations at Banque de France, says there are recognised risk owners within financial institutions where cyber risk is concerned. "With the development of automated processes and more open information systems, financial institutions face increasing risks related to internal or external malicious acts such as fraud or cyber attacks. Against this background, two main categories of risk owners are usually identified when it comes to information security and the associated risk acceptance: the chief information officer (CIO) and the business areas owning IT systems."

He points out that the CIO is usually in charge of all risks related to IT horizontal processes, such as patch management or change management. The CIO will also have responsibility for shared infrastructures, such as firewalls and anti-virus software, which are used by multiple business users.

For business areas that own IT systems, Beau says the treatment of IT security risks is part of the system owner's responsibilities. "Business unit managers are accountable for their own staff's actions and should make sure that the access rights granted to their staff are valid, that all documents managed in their unit are appropriately classified and handled accordingly."

**At the top of the tree**

There is a broad consensus about cyber breach accountability at board level. Though cyber issues have not been a traditional area of focus for board members, they now find themselves staring it in the face and wondering how to deal with it. And this is not always easy.

"The board in general is struggling to understand what their role is and how to have relevance here," says KPMG's Bell. "They are asking questions of management to make sure management have thought things through in this area and unfortunately the answers they are getting are very technical in nature. For example, the board might ask 'have we considered what the risk of our organisation would be from a cybersecurity impact', and the answer they will get in the next board meeting will be the chief information officer walking in and presenting 45 pages on the technical configuration controls."

He says the board has traditionally looked at areas such as operational risk, investment risk in the case of new financial organisations, regulatory risk and other more traditional risks – but may not have really focused on or evaluated the company's vulnerability to cyber attack or IT security risk. "This is a new set of conversations," he says.

Banque de France's Beau has no doubt that boards need to accept responsibility. "Of course the board of directors has to be deeply involved," he says. "IT risk – for example business disruption and system failures – is one of the specific risk event categories defined by the Basel Committee on Banking Supervision and one for which compliant institutions are required to demonstrate management competence."

He adds that it is also up to the board to ensure that both IT organisation and operational risk management comply with standard requirements and are in a position to address disruption and system failures. "The board, as the relevant body for the overall risk tolerance strategy and policy, has to confirm the risk acceptance and mitigation plans proposed by the business,
IT and risk managers. The board must ensure that critical business functions can be maintained or restored as quickly as possible in the event of internal or external incidents.

The board – both directly and through the risk or audit committee – receives regular reports on the most important IT risks as part of broader risk reports, Beau says.

According to Nice Actimize's Borenstein, cybersecurity breaches have become a regular board topic over the past 18 months in a way that few would have expected years earlier: "People on boards who want to understand these issues are bringing in consultants and experts and technical people to explain to them what might happen, what did happen or what could happen. Obviously the board is also concerned about compliance issues."

The board should also be working with the chief executive to set the tone from the top, according to Ernst & Young's Tsantes: as with other aspects of operational risk management, this will help embed the right mentality throughout the bank in understanding the significance of the cyber threat. "An organisation should be looking at it as though everybody in the organisation is on the security team, everybody each day has the ability to improve or destroy or erode the level of security at the company, and that really starts at the top."

The board should also be monitoring how quickly significant security issues are identified within their organisation and whether the incident has been repeated. "In this day and age you are going to have issues, you are going to have security problems and security incidents and what you want to do is catch them early and put in the remediation steps so that particular type of incident doesn't happen again," Tsantes says.

Bell points out, though, that it is important to remember that it is not the job of the board to govern the process of cybersecurity. Instead of risking being bogged down in the details of security, boards should be concentrating on ensuring that management within the institution is effectively covering the process of security and working to prevent cyber breaches.

"The board should be able to ask executive management questions about their view of their organisational risk for a cybersecurity incident," he says. "What they would do if that type of cybersecurity occurred, what the response might be for that organisation. Have they thought that through, have they planned it, have they exercised that?"

But the board must be absolutely clear on the value of the IT security implemented within the organisation, says FireMon's Zelmans. It is vital that the board understands the layers of complexity that go into these security measures in order to ensure they are happy to make the investment.

"The IT security team needs to articulate the value [of the defences] to their management and their management needs to get back to the board and explain the reasons for all of these different layers of defence and then the reasons for implementing them. It's after that the board will basically decide about the investment; so ultimately, it is the board that decides what to do."