Padlocking the safe in a digital world

Cyber security is a constant and evolving threat across all sectors of the global economy. No bank is immune.

Given the impact that a cyber incident can have on brand reputation, customer confidence and business interruption, it's unsurprising cyber security has risen rapidly up the agenda for executives, with boards increasingly involved in key decisions around cyber risk. Yet in a recent global banking risk management survey, less than half of respondents considered cyber security to be a "top-three" concern.

Cyber security is bigger than an IT issue

With increasing frequency and sophistication around cyber security attacks and hacks, banks are appreciating that it is not an IT issue but a business continuity, financial and reputational issue which requires multi-disciplinary responses.

With organised criminals increasingly using cyber to "go after the money", banks will continue to be targeted. The former director of global technology production at Deutsche Bank, John Baird, is reported as having said that while all banks are constantly being scanned for cyber weaknesses, "more serious" incursions happen around once a month.

Speaking earlier this year at a cyber security event in Sydney, the ASX's head of technology governance Daryn Wedd emphasised the importance of companies coming together to manage the risk:

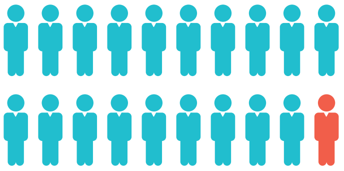
> "There is no point having an IT or tech team that is sitting buried in a room with technology, with all of the equipment and all of the gadgets and all of the kit you could possibly imagine, if that [security] information does not get used to inform the organisation as to what the threats are, and potentially what you need to do to combat them."

A new cyber mindset

Increasingly, compliance obligations are being imposed by legislators and regulators in relation to data breaches and other cyber incidents, and directors face growing threats of individual liability and shareholder class action. Despite this, only 10% of FTSE 100 companies currently deliver cyber-risk training to their board and just 5% of boards have any cyber security experience.

In Australia, mandatory notification of data breaches will come into effect in early 2018. In Europe, the General Data Protection Regulation (GDPR); coming into effect in May 2018 will require mandatory reporting of data breaches within 72 hours, and the Network and Information Security Directive will mandate minimum cyber security standards for providers of critical national infrastructure. Banks supervised by the European Central Bank are set to face breach notification rules similar to the GDPR.

BOARDS OF FTSE 100 COMPANIES



5% have cyber security experience

Fortifying the defences

Banks are investing in scenario planning and communications training to ensure the response team knows how to deal with the unexpected and has sufficient "flex" to respond to what is often an urgent unfolding cyber crisis situation.

Strengthening internal protections

The good news is many financial institutions are recognising the importance of treating cyber security as a "team sport". Focus is turning towards building cyber resilience through effective training and partnerships from board level down.

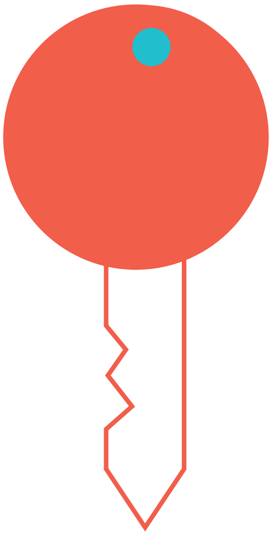
When cracks appear in the safe

One of the biggest data breaches in history was the exposure of names, phone numbers and email addresses of 83 million account holders when a bank's systems were compromised by hackers in 2014.

The recent Wannacry and NotPetya malware outbreaks disrupted industry supply chains, shut down hospitals and affected several banks. The Russian central bank was one institution hit by those attacks.

A hack of the Bangladesh Bank last year resulted in the theft of US$80 million (£63 million) via the SWIFT interbank payments system. The criminals had attempted to place SWIFT transactions totalling almost US$1 billion – the damage was only limited when a typo was spotted in one of the intended transactions. This breach led to urgent upgrades of the SWIFT system.

COMPANIES NOT ACTIVELY ENGAGING WITH **INVESTORS OR CUSTOMERS** ABOUT CYBER SECURITY



FTSE 350 companies

3%

ASX100 companies

32%

Contrary to common perceptions, careless or unaware employees are said to be the most likely contributor to cyber incidents, and therefore are one of the best lines of defence. After that, the most likely perpetrators are criminal syndicates, malicious employees and hacktivists, in order of decreasing likeliness.

Staff are being educated on how to avoid common scams, including the risks of opening unknown attachments or responding to "phishing" emails, leading to infiltrations of the corporate network or the introduction of malware causing a ransomware incident or another form of vulnerability.

Employee awareness is being improved though the "gamification of the process". For example, engaging third parties to send, with increasing levels of sophistication, fake phishing emails to employees, keep track of those who fall for them and then offer retraining and retesting to improve employees' ability to identify malicious emails in a "no-blame" culture.

Bolstering external safeguards

Supply chain outsourcing arrangements are also critical to effective cyber response capability.

Engendering the right behaviours both preventatively and when incidents occur is crucial. Without that, companies that experience cyber incidents originating from a third party supplier will discover that containment is more difficult because the supplier is uncooperative in attempts to contain the effect of the breach or determine its cause – including because of the prospect of subsequent litigation or further reputational risk.

As an example, banks should ensure their contracts spell out how they expect third party contractors to act in the event of a cyber incident. This might include provisions addressing information sharing (such as notification obligations and updates at defined intervals), incident response and mutual support in relation to containing any incident, and requirements that subcontractors sign up to similar provisions downstream.

Supply chain security (and vetting of suppliers) is vital as data processing and other critical business functions are increasingly outsourced or hosted in the cloud. Yet a recent ASX 100 cyber report found that 30% of the ASX 100 have still not assessed the security of third parties and 32% are not actively engaging with investors or customers about cyber security – vastly different to 3% for the UK's FTSE350.

It will be interesting to see how this evolves in the next 6–12 months when Australia's new mandatory data breach laws come into effect.

Andrew Moir
Partner, London
T +44 20 7466 2773
M +44 7809 200434
andrew.moir@hsf.com

Anna Sutherland
Partner, Sydney
T +61 2 9225 5280
M +61 404 035 280
anna.sutherland@hsf.com