Managing cyber-security - a 'whole of business' approach

Written by Cameron Whittfield, Lisa Fitzgerald and Kirish Kularajah

Decisions about technology investment have always been vexed. While the normal considerations associated with vendor selection, terms of supply and value for money apply, technology purchasing decisions are also made with the additional uncertainty that comes with the speed of technological change. Yesterday's solution may be 'bettered' today or (worse still) made obsolete tomorrow.

In recent times senior company executives have had another layer of complexity added to the mix: the interconnectivity of things. Investors, management and disruptive competitors alike are demanding that companies embrace technology and leverage off the ubiquitous interconnectivity in the 'cloud'. However, the very platforms that create digital opportunities are also creating enterprise vulnerability.

Responding effectively to this vulnerability is critical and responding with technology alone (such as through data encryption or anti-virus software) is unlikely to be enough.

It has now been over 18 months since the World Economic Forum published its report on 'Risk and Responsibility in a Hyper-Connected world'.[1] Over this period, we've seen a marked increase in cyber-security risks but little to no tangible improvement in 'global cyber resiliency'. For instance, *The Economist* recently reported (with sufficient disclaimers around accuracy) that the average time between security breach and discovery was 205 days.[2]

In this paper, we look at some recent trends in cyber-security, consider the options available to improve preparedness for cyber-risks and demonstrate how and why legal protections are just part (and, to be frank, a relatively small part) of a broader 'whole of business' approach to effective cyber-security management.

POWERED BY

GILBERT TOBIN

1 World Economic Forum (in collaboration with McKinsey and Company) – *Risk and Responsibility in a Hyperconnected World*, January 2014.
2 *The Economist*, 'The cost of immaturity', 7 November 2015

What's happening?

As the global economy continues to become more interconnected, the scale and sophistication of cyber-crime is on the rise. The increasing opportunities available through the Internet of Things (IoT) and online commerce come with a trade-off – susceptibility to cyber-crime.

Malicious software is becoming more targeted and harder to detect. It is also becoming far more accessible. We are seeing increasing incidences of fraud, identity and intellectual property theft, cyber-attacks from competitors, individuals and (some have suggested) nation states and 'hacktivists' disrupting for political gain.

In the past 18 months alone, some of the largest corporations in the world have fallen victim to cyber-hackers:

October 2015 – The bank account details of 21,000 customers of TalkTalk (a UK telco), along with 1.2 million customer email addresses, names and phone numbers were accessed and stolen in a data breach orchestrated by teenagers.

August 2015 – Ashley Madison, the infidelity website, was hacked by a group calling itself the Impact Team. The release of data (including potential data on around 460,000 Australian users) has left the site's 'users' nervous and its owners Avid Life Media, facing unquantifiable legal exposure.

December 2014 – The US Office of Personnel Management was hacked, resulting in the theft of thousands of US government employee data.

November 2014 – Hackers stole and subsequently leaked over 100 terabytes of data (including confidential information) from Sony Pictures Entertainment.

November 2014 – JPMorgan Chase was the victim of a cyber-attack that is believed to have compromised data associated with over 83 million accounts. In November 2015, US prosecutors finally laid charges against two Israeli nationals and an American thought to be responsible for the attack.

September 2014 – Cyber-criminals compromised Home Depot's network and installed malware on the home-supply company's point-of-sale systems and stole information on approximately 56 million payment cards.

August 2014 – Individual accounts of celebrity users of Apple's iCloud were hacked and photographs spread across the internet. Apple maintained that while individual accounts were breached, its systems were not.

It's not just the big names that are under threat. Every day, millions of individuals and businesses fall victim to cyber-attacks. In Australia alone, the number of serious cyber incidents that were detected and reported in the 12 months to October 2015 increased to nearly 10,000 – a 109% rise from incidents reported in the previous year.[3] While improvements in detection and reporting have skewed these statistics somewhat, the undeniable trend is that the quantum and severity of cyber incidents is on the rise. *The Economist* (again), quoting a Merrill Lynch report, estimates that the annual cost of dealing with cyber-security issues is approximately US $575 billion which in turn has spurned a US$75 billion global cyber-security industry. The industry is expected to grow in value to US$170 billion by 2020. It's little wonder cyber-security solutions and advice is the flavour of the month.

3 PwC, *Global State of Information Security Survey 2016*, 21 October 2015

What does all this mean?

Not only do businesses face potentially significant losses resulting from 'downtime' caused by an attack and the time taken to manage the fallout, cyber-attacks invariably compromise commercially and personally sensitive information. The direct impacts can include the loss of customer data, product designs and other digitally stored intellectual property, company strategies and secrets as well as employee information.

There's also the risk of legal proceedings from customers and employees. For example, the fallout from the 2013 data breach at US retail giant Target (when credit card details of some 40 million customers were lost), is estimated to have cost the company in excess of $100 million mainly in settlement claims from banks and credit card companies who suffered loss as a result of the breach.[4] Similarly, the Ashley Madison cyber-attack has led to at least seven multi-million dollar class actions being filed in courts in the US and Canada, claiming breach of contract, false advertising, negligence in the care of customer data and breach of privacy laws.[5]

Perhaps the most significant yet least quantifiable risks for business is reputational damage that can flow from an attack. The damage to reputation to the likes of Target, Ashley Madison and TalkTalk is likely to be massive. Making matters worse, reputational risk cannot be contractually managed. Even the most robust, 'purchaser friendly' supply arrangements are unlikely to allocate responsibility or liability for reputational damage. What's more, contractual protections are often of limited value once a cyber-security breach has occurred. Much like breaches of confidence, the damage can be instantaneous (social media and the 24 hour news cycle will usually see to this).

What should organisations do?

Legislative and regulatory compliance can force companies to put in place basic protections. Certainly, compliance programs that look to address data protection and privacy laws can drive behaviours that end up protecting the organisation. As the threat of cyber-attacks intensifies, regulators around the world are starting to explore novel and innovative ways to combat the threat. The US and EU have already proposed laws that encourage private and government sector bodies to share information about cyber threats, with the aim of facilitating a collaborative and pro-active approach to cyber-risk. While some (at least historically) have viewed regulation as an unnecessary burden, we have found that (at the very least) they focus senior management on the need to address cyber-vulnerabilities.

There are also clear opportunities to mitigate risks through vendor contracting arrangements. While contractual remedies themselves may be of limited value during catastrophic cyber incidences, supply arrangements that demonstrate (and require) accountability for information and data protection can create the right 'end to end' cyber-risk focus across the entire IoT stack of technology – from cloud servers through to devices.

However, despite the laws and contractual protections, cyber-attacks are an inevitable consequence of embracing digitisation. Businesses must be able to understand, detect and respond to cyber threats at an organisational level rather than simply viewing the threat as an IT issue or one that can be managed through the company's contracts.

---

4 *The Wall Street Journal*, 'Target to Settle Claims over Data Breach', 18 August 2015

5 US Class Actions: *John Doe v Avid Life Media Inc. and Avid Dating Life Inc. dba Ashley Madison (Case No. 2:15-cv-386)*, filed in the US District Court of Virginia on 3 September 2015; *David Poyet v Avid Life Media Inc., and Avid Dating Life Inc. dba Ashley Madison (Case No. 2:15-cv-08456-R-AS)*, filed in the US District Court of California on 29 October 2015; *Christopher Russell v Avid Life Media Inc. (Case No. 8:15-cv-02693-PWG)*, filed in the US District Court of Maryland on 11 September 2015; *John Doe v Avid Life Media Inc. (Case No. 3:15-cv-02750-N)*, filed in the US District Court of Texas on 21 August 2015; *John Doe v Avid Life Media Inc. (Case No. 2:15-cv-06405-PSG-AJW)*, filed in US District Court of California on 21 August 2015; *John Doe v Avid life Media Inc. (Case No. 6:15-cv-01464-LSC)*, filed in the US District Court of Alabama on 25 August 2015; *Jane Doe v Avid life Media Inc. and Avid life Dating Inc.*, filed in the US District Court of New York on 4 September 2015. Canadian cases: Time Magazine, Ashley Madison Faces $578 Million Class Action Lawsuit, 23 August 2015

Before it happens…

Like all organisational crises, concentrating on prevention is always better than the cure. Management of cyber-crime risk requires a coordinated, 'all-of-organisation' approach. Areas to focus on include:

Identification and valuation of data

Not all data has the same value and so implementation of IT solutions and other security measures should be targeted. From firewalls, anti-virus and anti-spam software, intrusion detection, access management and data loss prevention strategies (such as data encryption), measures may vary depending on the data and whether it is critical to business operations.

Data management

Businesses should continually review the sort of data they hold and how and where they store such data. In October 2015, TeleChoice agreed to pay for 12 months of credit monitoring for customers affected by a 2014 data breach after it admitted to storing customer data in shipping containers on Victorian bushland that were easily accessible to members of the public.

Crisis management plan

It is vital that all businesses develop and implement an effective crisis management plan before an attack occurs. The plan should be developed in close consultation with all areas of the business (including Information Technology, Human Resources, Legal, Risk and Compliance). The plan should also be stress-tested regularly to ensure it is fit for purpose. Additionaly, the OAIC's recently published draft "Guide to developing a data breach response plan" may assist organisations in developing such a plan.

Invest in technology security

An obvious solution to manage cyber-security risks lies in the technology solutions themselves, which need to continuously improve to keep pace with digital changes. There are many technology options available to protect companies and their data. As noted above, however, even the most robust technology protections remain vulnerable to compromise.

Consider going cloud

While cyber-security is often a reason for resisting the move to cloud-based services, some cloud service providers are able to leverage their scale and access to greater intelligence on cyber threats. Combined with effective risk allocations through contract negotiations, cloud options can often be a viable avenue for businesses seeking to mitigate cyber-security risk.

Effective contract negotiation

The importance of effective contract negotiations and drafting in technology related contracts cannot be understated. Risk allocation and service level obligations around cyber-security should be at the forefront of all contract negotiations with third party service providers. Similarly risks can be mitigated through contracts with customers as well as employees.

Mitigate employee risk

Internal threats are often as serious as external ones. Effective cyber-security is about more than just expensive and complex technical systems. Businesses should continually assess the processes it has in place to protect its data (including on employee mobile devices and laptops) and how these are reflected in employment contracts.

Consider cyber-crime insurance

Many insurers now offer policies covering loss of data and crisis communication costs relating to cyber-attacks. However, while cyber-crime insurance might help to recoup some of the financial loss after the fact, no amount of insurance can ever replace lost intellectual property or damage to reputation.

Training and compliance

As cyber-security comes to the forefront of priorities for governments and regulators, the legal and regulatory frameworks surrounding the obligations of business is becoming more and more complicated. Legislation such as the *Privacy Act 1998* (Cth) and its Australian Privacy Principles (APPs), as well as industry based guidelines including ASICs' 'Report 429: Cyber-resilience – Health Check' impose important legal obligations on companies and their directors to take reasonable steps to avoid security breaches. The regulatory framework is also in a constant state of flux, trying to keep up with the pace of technological change. The APPs, for example, were amended last year to achieve a greater degree of consistency in the way privacy principles applied to private and public sector organisations as well as to introduce changes in relation to cross border information disclosures. Organisations should stay on top of these changes and ensure that requirements and obligations are made clear to staff at all levels and across all business lines. Legal and regulatory education is just the beginning. Staff should also be given continuous 'IT fitness training' to equip them with the necessary tools and understanding to allow them to protect themselves and their organisations in the digital age. After all, even the strongest fortress is insecure if those inside are willing to open it for all who come knocking with bogus emails and dodgy software.

After it happens…

While businesses should be pre-emptive in approaching cyber-security, no amount of precaution can guarantee safety. Being prepared to react and respond rapidly if and when there is a security breach is critical. Businesses should focus on ensuring that damage is minimised, controlled and contained. Several strategies may assist:

Rapid response –

The first 24-72 hours after a cyber-incident is critical. Businesses must use this time wisely. A business should be able to put its crisis management plan into action within this time to prevent or dampen the fallout. This can be as basic as knowing who within the organisation is part of the response team, how they can be contacted, including after business hours (via up to date contact details) and pre-defining the roles and responsibilities of each team member.

Immediate engagement of trusted external advisors

This includes engagement with legal advisors, forensic and security advisors as well as public relations consultants who can be briefed immediately to assist in the management of the incident. This is even more important in a continually changing regulatory environment.

Go to market strategy

In an increasingly digital age, news is social and it travels fast. It's important to control as much of the information in the marketplace, and in the hands of customers, as possible. Based on the nature of the cyber-attack, the business (in consultation with its advisors) should swiftly establish a 'go-to-market' strategy – to inform the market and (if required), customers and regulators of the incident.

Where to from here?

Regrettably, cyber vulnerability is inevitable risk for companies who must make cost / benefit decisions in relation to cyber-attack prevention investment. The challenge now, given the increased proliferation of cyber-crime, is how much to invest in prevention and where the tipping point lies between investment and risk.

The next 12 – 24 months will be an interesting period. There is increasing concern that cyber-attacks are impacting on decisions to fully embrace the cloud or take full advantage of the digital revolution (a 'cyber-backlash', as some commentators have observed).

We remain of the view that robust protections that address the risk (rather than treat cyber-security issues as a matter of compliance) and excellent crisis management strategies are critical. It is this combination that will provide the confidence to embrace digitisation, having ascertained and mitigated the risks.

The authors would like to thank Michael Caplan, Michael Williams, Michael Burnett and Jane Kluske for their contributions to this paper