Managing Cyber Security

By James North and James Wallace

***James North** is a partner at Corrs Chambers Westgarth specialising in technology, media and communications.*

***James Wallace** is a graduate at Corrs Chambers Westgarth.*

Cyber security is more than just an issue for the IT team. The risks that come with cyber crime and the digitisation of business run through every part of an organisation.

Too often companies only involve their lawyers as a reactive measure to a data breach. However, General Counsel should be an integral part of the proactive plan to prevent, prepare and respond to a cyber attack. The financial and reputational costs of data breaches make it a commercial imperative.

Last year, a US survey of 500 Directors and General Counsel revealed that, after the traditional topic of regulatory compliance, data security topped both Directors' and General Counsel's lists of worries.[1]

It's not hard to see why. In the UK alone there were 5.1 million cases of online fraud and 2.5 million incidents of computer hacking last year.[2] The financial incentive for cyber criminals is substantial. The black market price for stolen personal records on the dark net can be as a high as $1000 per file.

Hackers are acutely aware of organisations' vulnerabilities. Government and company systems are being attacked more frequently every year.

Sony Pictures, Target and UNSW were all the subject of recent high profile attacks. The breach of Target's data centres was perhaps the most damaging with payment information for 40 million customers being publicly exposed.

Cyber Attacks Cost Millions

It is estimated that cyber crime attacks affect 5 million Australians at a total cost of $1 billion every year.[3]

On average a cyber breach will cost a business $2.82 million.[4] The biggest cost is in the release of information that hackers can use for blackmail or fraud. Other costs include loss of business information to competitors, the undermining of customer confidence and reputational damage.

Legal Consequences

Companies also face litigation and legal penalties if the breach reveals non-compliance with privacy obligations.

Companies are required to comply with the Privacy Act and the Corporations Act to protect personal and commercial information from misuse or public disclosure. This can include notifying affected individuals and regulators in event of a breach. There are also other industry specific laws which regulate sectors like telecommunications, finance and health care to consider.

ASIC and the OAIC are taking a close interest in how organisations plan and respond to cyber threats. It is OAIC's primary duty to ensure strict standards on how organisations collect and store their customers' personal and sensitive information.

Failing to comply with legal obligations can result in substantial penalties and potentially a claim or class action suit for breach of duty of care and negligence. Litigation claims in this space are starting to take off.

Risk And Governance Decisions

Cyber attacks expose not only a company's data, but also the systems and practices designed to protect that data.

While the IT team can set up tactical defences and security software in the hope that hackers won't get in, it's impossible to protect every asset.

The executive and Board must decide what matters most to the business and what is most likely to be targeted. The ASIC report (REP 429 Cyber resilience: Health Check) into cyber resilience calls for greater Board involvement in cyber security planning. ASIC recommends the Board oversee the development, testing and implementation of a cyber resilience framework to plan for, protect from and respond to cyber attacks. The framework should involve all parts of the business including legal, marketing, commercial, risk and IT.

General Counsel's Role

Some organisations have a Chief Risk Officer or Risk Committee who can lead on cyber security planning, but for most, the General Counsel is best placed to assess and mitigate risk. This role includes:

- reviewing insurance policies;
- advising Directors of their duties;
- reviewing supply contracts to ensure commercial partners have adequate means of data protection;
- advising on notification requirements in the event of a breach;
- ensuring that post breach investigations are legally privileged; and
- dealing with legal claims.

Cyber security may once have been an IT–only issue, but it is lawyers who now must navigate the myriad legal issues and data protection regulations.

A 2016 priority for General Counsel will be ensuring their organisations are cyber resilient, legally compliant and meeting their duties of care to clients.

Cyber Threat Readiness and Response Checklist

1. Understand what to protect

What are our business critical systems and information assets?

2. Understand your risks

Who is likely to threaten our organisation? Criminals, disgruntled ex-employees, hactivists, rogue states.

Who are the internal stakeholders who need to be engaged (it's not just an IT issue)?

Which of our suppliers have access to our systems and information and need to be engaged?

How might our customers be impacted by our cyber incident and/or threat?

Are we adequately insured for cyber risks?

3. Understand your legal environment

Have we identified and engaged with our key regulators?

What are our statutory obligations?

What is required of directors to prepare and plan?

What are our obligations to notify if a breach occurs?

What are our contractual obligations to keep information confidential and to take steps to recover it if there is a breach?

4. Understand your current defences

Do we conduct regular threat assessments to ensure our defences are adequate? • Are our cyber defences focused on protecting our key information assets and systems?

5. Have a game plan

Do we have a cyber response plan that has board input and approval

Which senior executive will lead a response to a cyber incident and/or threat and who are the other key stakeholders?

Who are the external advisors who will help us manage the crisis? IT forensics, legal, crisis PR.

Is our cyber response plan aligned to our business policies and procedures e.g. business continuity plan and privacy policies?

Have we tested our cyber response plan, e.g. by conducting simulation testing?

6. Activate your cyber response plan and get help immediately

Have we contacted our general counsel and external advisors to avoid mistakes, mitigate risk and establish a privileged environment?

7. Understand the incident and/or threat and the consequences

What is the nature and extent of the incident and/or threat?

Have our information assets been stolen or compromised?

How do we protect the organisation from further damage?

What are consequences of the incident and/or threat for business continuity?

Are we in control of our key systems?

8. Manage communications and notifications

Who do we need to notify about the incident and/or threat - customers, regulators, the market, insurers?

What is our public communications strategy?

Have we notified our insurers?

9. Investigate what and how

Who is behind the incident and/or threat?

Why did our defences fail?

10. Recovery

What steps can be taken immediately to reduce the risk of further intrusions?

Who are the third parties affected by the incident and how do we resolve any issues with them?

Can we claim under our insurance?

Are we prepared for legal claims by customers and other affected third parties?

11. Learn

What can we learn from the incident and/or threat?

How do we incorporate these learnings into the planning process and security posture of the organisation?

[1] 2014 Law in the Boardroom Study

[2] United Kingdom Office of National Statistics, Crime Statistics Year Ending June 2015.

[3] 2013 Norton Report: Total Cost of Cybercrime in Australia.

4 The Ponemon Institute and IBM, 2015 Cost of Data