PiperAlderman

Article Information

Service: Corporate & Commercial, Cyber Security

Cyber Security: Be Aware. Be Prepared

It's not IF but WHEN – Cyber security encompasses how companies and individuals adopt and implement strategies to deter and minimise the impact of cyber attacks.

Cyber security is not limited to protection against hackers attempting to maliciously gain access through computers in workplaces, but instead requires a multi-disciplinary and holistic approach, having regard to all of the potential exposures that organisations and individuals have at work, at home, and every time that we are connected to the internet. We are now exposed 24/7 through every aspect of our lives, including our computers, laptops, tablets, phones, smart devices, home automation systems, security systems, health and medical devices, and cars.

As we integrate technology further into our lives, through the Internet of Things, smart devices, and social media, the opportunity for innovation and growth increases, but the risks and exposures similarly expand.

Just as technology advances, the breadth, type and complexity of cyber attacks also develop, and we must continue to improve our systems to maximise the protections available to manage the risks and impact of cyber attacks.

Australia at risk

Surveys show that companies in Australia have been affected by more data breaches than any other country in the Asia Pacific region, with ransomware, malware, phishing and social engineering representing the greatest risks.

Aside from financial costs including loss of revenue, drop in share price and remedial costs, other potential consequences of a cyber attack include loss of IP and confidential information, reputational and brand damage, operational and infrastructure impact, loss of consumer and stakeholder confidence, loss of market and competitive advantage, legal and regulatory implications, staff downtime, and opportunity cost. These may lead to the downfall of a successful business.

Be prepared

Driven by board and management

Effective cyber security strategy must be driven from the board and management and requires a complete shift in the organisation's culture. In the same way that boards are expected to have some level of financial acumen, they should also have a basic level of understanding of cyber security and acknowledge that cyber security is not just an IT issue.

Boards should maintain oversight, and may wish to consider:

- having cyber security as a regular item on the agenda;
- having a director with cyber security expertise;
- having a cyber security committee or expanding the existing audit and risk committee to also manage cyber, digital and social security, with such committee providing regular reports to the board;
- engaging cyber security experts, including IT and legal experts; and
- implementing KPIs for directors and management which relate to cyber security, for example, implementing a certain number of policies, or attending seminars presented by experts.

Understand obligations and duties

Organisations need to be aware of their obligations such as:

- those under the *Privacy Act*, including the introduction of mandatory breach obligations which, in short, require organisations to notify the Privacy Commissioner and various individuals if they are aware that there are reasonable

grounds to believe that there is unauthorised access or disclosure of personal information, or loss of personal information where unauthorised access or disclosure is likely to occur and a reasonable person would conclude that access or disclosure would likely result in serious harm to individuals;
- disclosure requirements to shareholders, stakeholders, the market, and regulatory bodies under the *Corporations Act*, the ASX Listing Rules, their constitutions and other contracts; and
- any corporate governance considerations of the organisation, including the ASX's Corporate Governance principles where they have been adopted.

Directors must also be aware of their duties including the duty of care and diligence, and the duty to act in the best interest of the organisation, which encompass having sufficient and appropriate skills, experience and knowledge, acting prudently and responsibly, and having appropriate risk management strategies to address foreseeable risks.

Tailored cyber security action plan

Having a plan that is appropriate and suitable for the organisation:

- taking into account the likely types of digital, physical and social security risks to the organisation, including worst case scenario in terms of costs, downtime, and damage;
- setting out strategies and mechanisms for prevention and protection, and for impact reduction of cyber attacks;
- undertaking a thorough assessment of the equipment, software and processes of the entire infrastructure, including IT resources, data storage and architecture, physical perimeter security, social and media activities, industry specific concerns;
- providing steps to take to manage risks;
- planning what resources will be used to remedy a threat in the event of a breach;
- incorporating a breach response plan setting out key steps and processes to respond to a breach, including relevant contact details, roles and responsibilities, and appropriate ways to respond to cyber threats and breaches such as containment, assessment, evaluation, notification including having pre-drafted statements customised for each stakeholder, and appropriate media releases, and prevention; and
- having regular monitoring and testing to determine whether the processes are effective, whether staff know what to do in the event of a breach, and whether improvements need to be made.

Corporate governance

It is also important to consider what procedures and measures could be adopted for good corporate governance. Where the ASX Corporate Governance Principles are adopted, consideration should be given to some of the relevant principles that may be relevant to cyber security such as structuring the board to add value, making timely and balanced disclosures, respecting the rights of stakeholders by providing information, recognising and managing risk, and remunerating fairly and responsibly.

Organisations should consider how their cyber security strategy and plan align with such principles, and whether any of the following measures should be adopted:

- requiring major decisions on cyber security to be made by multiple persons within the organisation, not just one;
- having appropriate levels of accountability;
- having good protocols and screening when attracting and retaining board members and employees, including undertaking background checks and due diligence to minimise the risk of cyber security threats arising from within the organisation;
- being aware of how technology is used by board members, management, and staff at work, at home, and while travelling to identify and manage all potential risks; and
- ensuring that every person within the organisation knows the next steps to take to manage any potential threats or risks.

Technology

Organisations need to implement technologies that are appropriate for their business and industry, including at a minimum, endpoint and gateway controls such as anti-virus and malware protections, email filtering systems, website filtering systems, and internet filtering systems, as well as other processes and systems such as patch management processes, threat and vulnerability scanning, intrusion detection and prevention systems, and privileged account management.

Existing IT departments and service providers may be highly skilled in providing IT services, but may not have the expertise to provide cyber security services. It is therefore necessary to assess the type and level of IT support currently provided to the organisation, and determine if it is necessary to also engage cyber security experts to manage its cyber

security risks.

Policies and procedures

It is important to have appropriate policies and procedures dealing with cyber security which are disseminated throughout the organisation including:

- IT policies dealing with use of technology, access, password and login protocols, information security, internet usage, email usage, social media and networking tools, and remote access;
- data security, storage and breach policies;
- privacy policies including notification requirements;
- third party management policies; and
- HR, finance and accounting policies which may need to be updated to address cyber security risks and threats.

Education and training

Technology is only one piece of the puzzle. For the policies and procedures to be effective, staff at all levels must be made aware of, and understand, the potential cyber security risks and the policies and procedures that are put in place to manage those risks, including what to do in the event of a breach.

This can be done through regular communications, making the above policies readily and easily accessible, and providing training sessions by relevant persons in the organisation and/or external IT and legal experts.

Third parties, contracts and liability

The above recommendations may assist in elevating the security of an organisation to deter cyber attacks, but the organisation may still suffer significant consequences where there are successful attacks on third parties within an organisation's supply chain. As such, consideration should be given to the level of cyber security sophistication required of third party service providers and suppliers.

Contractual obligations could be imposed on third parties requiring them to have a cyber security action plan, take reasonable steps to protect the organisation's information, minimise cyber security risks, comply with various information security standards, and notify the organisation of any breaches regardless of whether they have any legal requirements to notify.

Contracts may also specify the steps that the third party is required to take in the event of a breach, including who is to notify individuals affected where personal information is jointly held.

Consideration should also be given to updating contracts to include terms which allocate risk and liability, and obtain indemnities for any loss or damage suffered as a result of any cyber attacks or breaches of a third party.

Insurance arrangements

General business insurance policies often exclude loss or damage suffered as a result of any cyber attacks or breaches. Consideration should be given to acquiring specific cyber security insurance which is now offered by a number of insurers.

Seek assistance from the experts

Take advantage of all resources that are available, including those that are part of the Federal Government's Cyber Security Strategy, and engage cyber security experts who are skilled and experienced to assist in managing and reducing the impact of cyber security risks.

Legal experts who specialise in cyber security can assist by working with IT experts to raise awareness and educate the board, assist organisations to understand their legal, regulatory and contractual obligations, prepare a cyber security action plan, establish good corporate governance procedures, prepare appropriate policies, provide training, and review contracts and insurance policies.