Cyber Audit TEAM

Leaders in Cybersecurity Governance

CYBERSECURITY

Is your Business Adequately Protected and Prepared for a Cyber Attack?

April 2018

CYBER SECURITY

Understanding the Challenges, Risks and New

Is your Business Prepared for the New Legislation?

Changes to the Privacy Act 1998 (Cth) now include mandatory Notifiable Data Breach (NDB) legislation, which became law in Australia as of **22 February 2018**. The Act mandates the disclosure of data breaches to the regulator and all affected clients **within 30 days** of discovery of the breach and is designed to enhance and protect individual's privacy, whilst affording greater protection of their Financial Data and Personally Identifiable Information (PII). Businesses will no longer have the option of keeping quiet following an online data breach, with penalties for non-compliance of **$420,000 for each director** and **$2.1 million for businesses**.

Additionally, new EU General Data Protection Regulation (GDPR) becomes globally enforceable as of **25 May 2018**. This regulation demands that security breaches involving EU citizen's data must be reported to the authorities **within 72 hours** of detection. Organisations that fail to comply could face fines of **€20 million Euros or 4% of global turnover** (whichever is greater).

Businesses must now ensure that they have in place appropriate policies and procedures, underpinned by tested Data Breach Response Plans, ensuring that they are adequately prepared to detect, respond and recover from future attacks and breaches.

Cyber Criminals Are Currently Targeting SME Businesses

Recent reports reveal that SMEs are now one of the most targeted sectors by cyber criminals. SMEs of all sizes, accross all industries are viewed by cyber criminals as easy targets and 'Honey Pots', primarily due to their vast amount of highly valuable client information and data they hold or have access to, facilitated through a general lack of understanding of cybersecurity, underpinned by inadequate spending on staff training or basic cybersecurity mechanisms and defences.

Despite all the warnings and awareness campaigns, the Australian Cyber Security Centre (ACSC) found that breaches were up by 22 per cent in 2017 with an estimated cost of $17bn to the Australian economy. An ACSC survey discovered that 90 per cent of businesses surveyed faced some form of attempted or successful breach. More alarmingly, over 50 per cent of businesses admitted that they were alerted by external parties before detecting the breach themselves.

Due to the rapid technology evolution, together with its adoption and acceptance within organisations, digital attack methods have become far more sophisticated, resulting in larger attackable areas that are more difficult to secure. Furthermore, with the advent of the IoT landscape (Internet of Things); internal and external security perimeters are subsequently wider and more vulnerable than ever.

Most companies have traditional IT security, such as firewalls and anti-virus software installed across their systems, often supported by either an internal IT Manager or external third party provider, managing their overall IT environment. Directors are often blindly confident that their business is secure from attack, and may have been reassured (often without any verification) that their company is adequately protected and prepared for cyber attacks. But exactly how confident are you that your digital assets, client sensitive data and your operating systems are all secure from a cyber attack?

The NSA, FBI, CIA, Microsoft, Google, Facebook, Uber, Equifax, Deloitte, Target, QLD Premier's Department, Brisbane Council, Precedent Communications and numerous others all thought that they had adequate systems in place however, all suffered embarrassing, large and costly breaches of their systems and their data. In many cases, this was largely due to a lack of any independent cybersecurity auditing; testing of their cybersecurity systems, policies or procedures, and lack of appropriate staff training.

IT Security and Cybersecurity are very different disciplines, and whilst there is a symbiotic relationship between the two, traditional IT security methods, such as firewalls and anti-virus software, whilst still essential, are no longer enough to keep cyber criminals at bay. Cybersecurity is not an IT or technology issue, it's a whole of business risk. Businesses are rapidly discovering that their internal IT teams or external providers simply do not have the bandwidth, or in-depth cybersecurity expertise or knowledge to protect their businesses and delegating this responsibility (to IT teams) has been catastrophic for many businesses. President Ronald Regan famously repeated on many occasions, "**Trust, but verify**!" After all, your IT Manager or IT provider will not be held accountable following an attack or breach.

The Inescapable Costs of a Breach

The risks of a data breach, or providing sensitive client information or payments to nefarious hackers can be catastrophic for the affected businesses and individuals concerned. The most quantifiable impact on your business is the one which is felt first, and that is the economic cost of incident response and remediation. This involves containing and responding to the attack, investigations into any resulting breach, forensic recovery of data, business interruption, media and public relations, compliance fines, and expenses on the back end to strengthen the company's cybersecurity defences in a way such that the attack can't be easily repeated.

According to a 2017 Webroot report, the **average cost of a successful Cyber attack to Australian SMEs is $1.9m**, whilst research from 'Unisys Security Index Australia' revealed that **85% of Australians would stop dealing with an organisation if their data was breached**.

Broader or less tangible costs could include client attrition, negative publicity, brand & reputational damage, enforced remedial action, senior management resignations, reduced shareholder value, litigation or class actions.

Detecting cybersecurity breaches before the criminals steal or compromise your company's data is a challenge for most businesses. It's common for successful cyber attacks to remain undetected by organisations for 6 months or longer. According to the 2017 Ponemon Institute report, **the average time to identify a breach is 191 days**, with the **average time to contain a breach currently sitting at 66 days**.

As cyber attacks become more sophisticated and targeted, techniques such as 'Caller ID Mobile Phone Spoofing', 'Pretexting' and 'Spear Phishing', are highly convincing and difficult for an untrained person to detect. Staff are increasingly divulging sensitive information, clicking on infected links or engaging with criminals purporting to be a client, colleague or supplier in emails requesting private or sensitive information or requesting financial

"the average cost of a successful cyber attack to Australian SMEs is $1.9m"

"the average time to identify a breach is 191 days, and 66 days to contain it"

“Cybersecurity is everyone’s responsibility and it must be embedded into the culture of your

transfers etc. (also referred to as ‘Social Engineering). Typically, upon infiltrating a company’s network, cyber criminals will probe for, find, and exfiltrate valuable data information. This could include all types of confidential, sensitive and valuable data from your company’s confidential data, your client’s personally identifiable information or financial information, such as TFNs, bank account or credit card details.

Motivation for attacks varies however, the most common are cyber criminals seeking to steal or access your data for financial gain, an unwitting employee being socially engineered, a disgruntled employee seeking to harm the organisation, or unscrupulous competitors seeking to gain a competitive advantage.

Protecting your Business & Digital Assets

Your business is being probed and tested every day by organised, well-funded, sophisticated, highly intelligent, advanced cyber criminals. Many businesses and their staff recognise the dangers of cyber attacks, yet many still do not fully appreciate or understand the enormous implications or serious security risks they pose. Most are simply unaware of how to spot a potential attack, protect themselves from data theft, or identify and prevent an attempted social engineering attack.

Once cyber criminals have gained access to your system, they will often create mechanisms to actively monitor your IT team’s recovery processes (which often consists of IT blindly advising to reinstall company data from an assumed safe point in time), allowing the criminals to reinfect you again at a later date with devastating effect. Therefore, following a digital breach of any type, and during the containment phase of your cybersecurity recovery processes, organisations should conduct an independent and thorough forensic examination of their systems to ensure that the attack has been contained and all threats discovered and removed.

While no single mitigation strategy is guaranteed to prevent cybersecurity incidents, according to the Australian Signal Directorate, at least **85% the adversary techniques used in targeted cyber intrusions could be mitigated** with simple and cost-effective mechanisms and frameworks, underpinned by and supported with robust policies and procedures. Conducting a baseline cybersecurity audit of your business, ‘independent’ of your IT team or provider, will highlight potential areas of exposure or risk. Once the identified risks are addressed, robust policies, procedures and response plans can be developed and tested, underpinned by appropriate board and staff training. As part of your company’s ongoing protection, independent monitoring, followed by penetration testing and of your systems, together with social engineering testing can be deployed to ensure that your cybersecurity resilience is enhanced and your business is secured and prepared for any potential threats or attack.

Conclusion

We are dealing with a rapidly moving and high-impact corporate threat that affects all businesses, regardless of size or industry. Businesses must recognise that Cybersecurity is a ‘whole of business risk’ and not an IT or Technology Issue. Changing the mindset towards cybersecurity and creating a culture that fosters collective awareness, understanding and responsibility must be driven from the top down.

Boards’ must educate themselves on this key area of risk and should communicate the importance of managing cyber risks to every employee in order to strengthen and integrate protocols into daily business operations, which will highlight the importance of shared data security responsibilities and mitigate the overall organisational risk. Adopting a proactive approach can also provide your business with a competitive advantage and contribute to an increased bottom line, whilst delivering you, your board and your stakeholders the peace of mind that your business is operating in a safe, secure and compliant cybersecurity environment.

There is no doubt that progress is being made however, cyber attacks are inevitable, with breaches increasing daily and while we continue employing humans there will never be any such thing as “100 per cent secure”. The good news is that there are many affordable solutions for protecting your business and its digital assets and companies that regard cybersecurity as an integral “cost of doing business” are rapidly discovering that proactive prevention

Cyber Audit TEAM

Leaders in Cybersecurity Governance

Is your Business prepared for the new Mandatory Data Breach Notification Legislation (effective 22nd February 2018) or the EU GDPR (General Data Protection Regulation – effective 25th May 2018)? Contact Cyber Audit Team now to find out more about how both legislations will affect you and your business.

The Cyber Audit Team are leaders in cybersecurity governance and employ a multi-disciplinary team of highly experienced industry experts, providing independent services, support and guidance to various industries.

Adopting global best practice and utilising recommended frameworks such as NIST (National Institute of Standards & Technology) and ISO (International Organisation for Standards), our team can assist your organisation in enhancing your cybersecurity resilience through the following independent services:

- Baseline Assessment & Independent Audit of your current cybersecurity posture
- Cybersecurity policy and procedure development
- Independent ongoing monitoring and threat detection
- Independent Penetration Testing
- Staff training and board guidance
- Social Engineering Testing (testing staff, processes & procedures)
- Chief Information Security Officer 'as a Service'
- Response & Recovery Services (Crisis Management, Legal Support, Computer Forensic Analysis and other related services)

Please engage with us via:

Tel: 1300 028 348
Email: enquiries@cyberauditteam.com
Website: www.cyberauditteam.com

Address: 60 Baxter Street, Fortitude Valley,
Queensland 4006 Australia

Postal: PO Box 1463, Oxenford,
Queensland 4210 Australia

ABN: 43 619 724 506