Meeting Australia's **Cyber Security Challenge**

2019

ddls
technology | process | people

Introduction

For as long as the cloud has been discussed as a business opportunity, discussion around how to secure it has not been too far behind. Cloud has served as the catalyst to an array of technology initiatives with ever-evolving security requirements like “bring your own device” (BYOD), remote working and the internet of things (IoT), extending security needs well beyond the traditional data centre. As devices proliferate and more production systems are brought online, the security risks will increase sharply, creating new vulnerabilities.

Damages from cybercrime are projected to hit $US6 trillion annually by 2021, up from $3 trillion in 2015.

In a world of competing cyber-priorities, organisations need to be able to secure their data irrespective of whether it is stored on-premise or in the cloud.

Organisations are introducing new technologies to drive innovation and growth faster than they can be secured. Employees are increasingly targeted as the weakest link in cyber defenses with people-based attacks such as account takeovers, ransomware and phishing scams making it more expensive and difficult for organisations to recover from.

It's little wonder then that the damages from cybercrime are projected to hit $US6 trillion annually by 2021, up from $3 trillion in 2015. At the same time, the demand for cyber security professionals is poised to outstrip supply with the number of unfilled cyber security jobs predicted to reach 3.5 million by 2021.

In this new age of cyber security, what are the challenges that will need to be met by the modern security professional and how can organisations refocus their resources to hedge against that threat?

The number of unfilled cyber security jobs is predicted to reach 3.5 million by 2021.

Section
01 /03

Key challenges in cyber security

As traditionally non-tech companies undergo digital transformation and look to build digital products and services to stay competitive, every company regardless of their industry is becoming a technology company.

From large manufacturers of agriculture machines grappling with onboard sensors and machine-to-machine protection to mining companies automating their supply chain to improve productivity from mine to market, every company is connected through their technology to their employees, partners and customers. As such, the security world has heightened in importance for everyone.

In a recent survey conducted by DDLS, 70 percent of respondents said that they expect data breaches and cyber security concerns to dominate their company's IT agenda.

With this in mind, what are the key cyber security challenges that all organisations irrespective of their size or industry should be wary of in the year ahead?

1.1

Employees are your biggest cyber security risk

The traditional focus of IT security has been on keeping out external threats, but the volume and frequency of security breaches caused by disgruntled, careless or negligent employees has risen significantly in recent times. This is mostly due to moving data off premises and into a growing number of mobile devices and cloud-based applications. As more organisations adopt initiatives such as bring your own device (BYOD) and the cloud, it's becoming much harder for an organisation to spot compromised devices quickly.

According to the 2019 Insider Threat Report, 59 percent of respondents surveyed said that their own organisations experienced at least one insider attack over the past year while more than two-thirds believed insider attacks had become more frequent over the past year.

Authorised employees or contractors use valid credentials to login and have physical access to an organisation's building, making most cyber security tools blunt instruments. However, not all insider threats are malicious with many sparked by careless employees who click on harmful email links or attachments without knowing, reuse the same password across multiple services, use unsecured public Wi-Fi, or accidentally leave their laptops in a public place.

Regardless of users' intentions, any resulting data breach can damage an organisation financially and cause reputational harm.

59% of businesses have experienced an insider attack in the last year.

Section
01 /03

1.2

Cyber criminals do not discriminate by business size

Think your business is too small to attract threats? Big mistake. Cyber criminals don't generally target individuals or businesses - they target vulnerabilities. A business of two is as prone to attack as a large corporation if a vulnerability is detected.

According to data from the Global Economic Crime Survey captured by PWC, 60% of all targeted attacks in Australia struck small and medium sized businesses.

Business is increasingly being done over network connected devices and each one presents a tempting target. A key point is that cyber-attacks are automated and constantly probe for weaknesses 24/7. The rewards of cyber-crime are so great, threats have dramatically increased and cyber criminals have become highly professional. This means that account takeovers, ransomware, phishing and extortion based DDOS attacks are all going to become a lot more targeted, making it more expensive and difficult to recover from.

60% of all targeted attacks in Australia were suffered by SMBs.

1.3 Cyber Security in the IoT age

With the Internet of Things (IoT), security challenges move from a company's traditional IT infrastructure into its connected products in the field. Forecasts peg 30 billion connected devices globally by 2020 as companies look to bring more and more devices, products and production systems online.

The sheer number of cyber security attack vectors increases dramatically as ever more "things" are connected. A corporate network might have somewhere between 50,000 and 500,000 endpoints; with IoT, we are talking about millions or tens of millions of endpoints. Unfortunately, many of these consist of legacy devices with inadequate security, or no security at all.

Forecasts peg 30 billion connected devices globally by 2020.

1.4 Talent Gap

According to recent estimates, there will be as many as 3.5 million unfilled cyber security positions worldwide by 2021. The Asia Pacific region is expected to be the hardest hit with a shortfall of about 2.14 million. The scarcity in qualified security professionals has led to an over reliance on technology at the expense of human expertise, with most organisations lacking the adequate number of security staff internally to do the daily blocking and tackling required of instant response teams.

The data is consistent with trends seen more broadly in the cyber security space.

Section
02 /03

Meeting the challenge: **key solutions**

2.1

Upskilling existing in-house cyber security expertise to fill the talent gap

Filling the skills shortage will require organisations to change their attitude and approach to hiring and training. In order to limit the impact of the shortfall, organisations must have a plan in place to retain and train existing staff. According to a DDLS survey, more than two thirds of respondents said that ensuring their skills and the skills of their team were up to date was the biggest challenge, suggesting not enough is being invested to improve in-house cyber security expertise.

Keeping their skills up-to-date is the main challenge for ⅔ of IT professionals.

2.2

Training all staff on cyber security best practice

Employees are a security risk when they are unaware of what they should and shouldn't be doing. They may be unaware of devices being connected to an insecure Wi-Fi network, the telltale signs to look for in a phishing email, the dangers of installing illegitimate apps or that they shouldn't be storing customer details on a USB.

Cybercrime cost companies in Australia more than $5 billion in 2018 with the most prevalent being people-based attacks such as phishing scams, ransomware and malware. A security-first culture is essential when countering targeted attacks and malicious insiders. This involves ongoing staff training and education that reinforces effective behaviour. While your employees may pose a security risk, with the right training and education you can reduce the risk of falling victim to cyber crime. Ensure all employees undergo regular cyber security content and awareness training and that best practice is communicated to all staff.

A security-first culture is essential when countering targeted attacks and malicious insiders.

2.3 Moving from reactive to preventative security practices

According to a DDLS survey, 54 percent of respondents said that decision makers within their business have given IT a seat at the table while only 13% said that IT is still seen more as a business support function than a business enabling function. The data is consistent with trends seen more broadly in the cyber security space. The elevated status of information security means that more senior security professionals or CSOs now either have a seat at the board level or at least a direct communication path to the leaders of the company which wasn't the case a few years ago.

As such, the challenge for a cyber security professional has shifted from trying to convince the board that cyber security is important, to convincing the board that you have a credible plan. This in turn results in greater investment in cyber security initiatives such as training and resources and means that organisations will be better equipped to tackle those challenges raised in section 3.

So how do security professionals do that?

Firstly, the senior security professional or CSO needs to do a better job in understanding their organisation's wider business before presenting their risk assessment to upper management or at the board level. They need to understand that the board is unlikely to take them seriously if they're not prepared to say why their security recommendations are more important than other priorities within the business.

The senior security professional or CSO needs to ask themselves hard questions such as if they make their organisation spend a certain amount of money to fix a particular security risk, how is it going to impact the business as a whole? Why is it more important than not hiring this person or not rolling out that product feature? If the CSO can't answer questions such as these, then the board will simply assume that they don't really know what the risks are because the risks are inherent to the business and the business includes many facets.

2.3 cont.

Business leaders must also be security leaders. This is crucial if an organisation wishes to move beyond reactionary security practices such as firefighting and disaster recovery to a preventative one. What is integral is an understanding that security breaches have far wider-ranging implications for businesses than the purely technical. The monetary and reputational damage a data breach can have on an organisation has been well documented but it bears repeating. Customer trust may disappear, share prices may suffer and IP and other assets may be lost. In contrast, effective security builds trust with clients, end users and other stakeholders and can create a competitive advantage. Seeing security as a business function and not a sub-department of IT involves executive teams that prioritise and champion security. Without it, a mature security program is going to be hard to achieve.

This may involve the introduction of KPIs and risk indicators so that boards can be kept abreast of the state of cyber security within their organisation. Or rather than the CSO reporting to the CIO, move the reporting line to the COO so that security becomes a direct business consideration that will be risk assessed like any other, rather than an afterthought after an incident occurs.

Executive teams and business leaders must prioritise and champion security.

Seeing security as a business function and not a sub-department of IT involves executive teams that prioritise and champion security. Without it, a mature security program is going to be hard to achieve.

This may involve the introduction of KPIs and risk indicators so that boards can be kept abreast of the state of cyber security within their organisation. Or rather than the CSO reporting to the CIO, move the reporting line to the COO so that security becomes a direct business consideration that will be risk assessed like any other, rather than an afterthought after an incident occurs.

Cyber security awareness: the basics

Implementing good cyber security practices is the responsibility of all staff, not just the IT department. Here's a list of the bare minimum all staff should know.

Choose secure passwords.
Complex passwords are essential to preventing cybercrime. Insist that staff choose different passwords for all of their accounts and ensure they are changed on a regular basis.

Beware of phishing emails.
As cybercriminals become more sophisticated, phishing emails are getting harder to spot. Tell your team to flag anything with an unfamiliar or unorthodox email address, spelling/grammatical errors or improbable requests.

Don't click on popups.
Your team should know never to click on a pop-up or link from an unfamiliar webpage, or provide personal or company information in response to communication they didn't initiate.

Adhere to the company's BYOD policy.
If your staff are using their own devices and accessing your network, make sure they set up automatic security updates and are using secure passwords across those devices.

Section
03 /03

Training for the future

With a wide range of training courses available across multiple vendors, deciding which aspect of cyber security training to prioritise can be a challenge in itself. Here's our summary of the most valuable courses and certifications.

01 **CEH: Certified Ethical Hacker.**
An intermediate-level EC-Council credential (EC-Council) and the most critical certification for IT professionals looking to develop their expertise in countering hacking attacks.

02 **CISSP: Certified Information Systems Security Professional.**
An advanced level certification offered by (ISC)2 for senior IT professionals and the most comprehensive review of information security concepts and industry best practices.

03 **EC-Council Certified Network Defender.**
An intensive course for network administrators and security professionals to level up their cyber security skills set.

04 **CISM: Certified Information Security Manager.**
Aimed at experienced security professionals, the CISM accreditation is a must-have for IT security professionals with enterprise-level security management responsibilities.

05 **CompTIA Security+.**
Technically an entry-level certification, although best suited to IT pros already familiar with network security.

06 **CompTIA Cyber Security Analyst + (CySA+).**
Designed to follow CompTIA Security+ or equivalent experience, CySA+ covers threat and vulnerability management and cyber incident response.

07 **RESILIA Frontline.**
A solid, foundation-level certification from AXELOS designed to equip all levels of staff with the basics on good cyber security practices and

08 **RESILIA Professional.**
Designed to help IT professionals implement effective cyber resilience using their organisation's existing processes and standards, this certification is offered at both Foundation and Practitioner level.

To learn more about these qualifications, visit the DDLS cyber security training page on our website.

References

Threatbusters: Bitglass (2019) Insider Threat Report. Available at: https://pages.bitglass.com/FY19Q2ThreatbustersBitglass2019InsiderThreatReport_LP.html

Cyber Security Ventures (2019) Annual Cybercrime Report. Available at: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

PWC - Global Economic Crime Survey (2014), ABS - Business Use of Information Technology (2014), Ponemon Institute - Cyber Security Report (2014), Synmantec - Internet Security Threat Report (2015). Available at: https://www.staysmartonline.gov.au/sites/default/files/Cost%20of%20cybercrime_INFOGRAPHIC_WEB_published_08102015.pdf

Accenture (2019) Australia at a glance: Ninth Annual Cost of Cybercrime. Available at: https://www.accenture.com/_acnmedia/accenture/redesign-assets/dotcom/documents/local/1/accenture-ninth-annual-cost-cybercrime.pdf#zoom=50

Statista Research Department: Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. Available at: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Mckinsey Insider Threat Report (2018). Available at: https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk

Symantec Internet Security Threat Report (2019). Available at: https://resource.elq.symantec.com/LP=6819?inid=symc_threat-report_istr_to_leadgen_form_LP-6819_ISTR-2019-report-main&cid=70138000001Qv0PAAS

ddls
technology | process | people

Contact
training@ddls.com.au
www.ddls.com.au
1800 853 276