DIGITAL SECURITY

CHALLENGES AND SOLUTIONS THAT EVERY BUSINESS SHOULD KNOW ABOUT

TOSHIBA

WHY IS SECURITY IMPORTANT TO BUSINESS?

Security is a hot topic for Australian business. At the highest levels of corporate leadership, there is an increasing awareness of the potential threat from cyber-attacks and the massive potential business impact.

A recent CEO study[1] showed that

CYBER ATTACKS CAME IN 2ND ON THE LIST OF THINGS THEY ARE EXTREMELY CONCERNED ABOUT

Second only to global health crises

NOT IF BUT WHEN

MANY SECURITY PROFESSIONALS REALISE THE NEED FOR A COMPREHENSIVE STRATEGY AND A RANGE OF COUNTER-MEASURES TO PROTECT THEMSELVES FROM THE VERY REAL DANGERS OF CYBER-ATTACK.

IT'S NOT JUST ATTACKS THAT KEEP CEOS UP AT NIGHT...

...it's making sure that sensitive data, about employees or customers is appropriately managed.

We have seen tougher regulations in Europe around capture and usage of customer data, and strict rules governing the processing of personally identifiable information of individuals inside the European Union[2].

These rules apply to any organisation doing business with Europe, meaning that many Australian businesses have to be able to show that their processes meet not only local, but international regulations.

Since 2017, there has been Australian Government legislation[3] in place that makes it mandatory for organisations to report data breaches that are 'likely to cause serious harm'. Organisations can no longer keep security problems to themselves, or sweep them under the carpet.

AS WELL AS THE 'STICK' OF REGULATIONS AND MANDATORY REPORTING, BUSINESSES ARE DRIVEN BY THE 'CARROT' OF REPUTATION.

In an age where businesses are in highly competitive markets, a security issue has the potential to do massive reputational damage, with a consequent loss of market share and revenue. On the positive side, an unblemished reputation generates trust, and is a business asset that can

WITH THE FINANCIAL, COMPLIANCE AND REPUTATIONAL RISKS, IT'S NO WONDER THAT SECURITY IS A BOARD AGENDA ITEM IN MANY ORGANISATIONS.

They recognise that security is one of the major risks in their business and that protection, prevention and well-founded action plans are critical to the success of their reputation, customer relationships and the very future viability of the business.

WHERE ARE BUSINESSES VULNERABLE?

EXTERNALLY

Many organisations move critical data outside their perimeter, in the form of data backups held offsite or in cloud, data on portable storage, including laptops, and physical hardcopy documents.

IT GIANT IBM BANNED THE USE OF PORTABLE MEDIA BY ANY EMPLOYEE, WITH THE CHIEF INFORMATION SECURITY OFFICER (CISO) CITING THE RISK OF 'FINANCIAL AND REPUTATIONAL DAMAGE' AS THE REASON FOR THE ACTION[4]

PERIMETER

At the perimeter of their organisation is the security wall against external invasion. These threats can be in digital form - viruses, malware, ransomware, adware, phishing and other forms of malicious software designed to disable, damage or extort money from an organisation. Or it could be physical, through security doors or gates.

FROM WITHIN

Inside the organisation is the third source of vulnerability – data about clients or employees could be accessed by non-authorised staff; details of a sensitive proposal can be seen by those outside the client team or more commonly, a disgruntled employed could have access to information that allows them to do deliberate damage.

WHAT ARE THE BIGGEST THREATS?

DATA THEFT OR LEAKAGE

Many businesses capture information about their employees and customers including credit card details, medical benefits records, drivers licence, address and so on. One piece of information may seem harmless, but to an identity thief these are important pieces of the puzzle.

This information can then be used to fraudulently obtain credit or loans, putting the individual at risk of a crime that takes their money and costs a massive amount of time and mental stress to remedy.

The information might be stolen through spyware and key loggers (which find or record passwords), malware (that can access files), or theft/loss of portable media or physical documents. The victim of these attacks may be a client or an employee, but the responsibility is on

A SIMPLE SWIPE

Think about something most people do daily – swiping a payment card – and how much data it generates. One swipe captures information about the individual's name, location, spending habits, financial health and bank details.

RANSOMWARE

This is the introduction of a program that hijacks and locks down an organisation's systems, even paralysing the recovery process. The locked down systems are typically only released on payment of a ransom. In a recent security survey, 30% of Australian respondents reported experiencing ransomware attacks at least quarterly.[5]

DISGRUNTLED EMPLOYEE

They can steal sensitive information to share with competitors, introduce viruses or leak confidential data.

DIGITAL TRANSFORMATION

More connected devices means more data and therefore a high potential level of exposure. With businesses being forced to accelerate the move to digital during the pandemic with remote working, meaning security of devices is more crucial than ever.

WHAT ACTIONS CAN COMPANIES TAKE TO REDUCE

THERE ARE SOME BASIC STRATEGIES THAT ORGANISATIONS CAN TAKE TO MINIMISE THEIR VULNERABILITY. AS A BARE MINIMUM THEY SHOULD ALWAYS HAVE UP TO DATE MALWARE PROTECTION AND ANTIVIRUS SOFTWARE ON

While there is a lot of crossover between these tools, many security experts advise using both together in order to maximise protection.[6]

ANTIVIRUS

focuses on prevention, protecting a machine by stopping it from becoming infected in the first place.

ANTIMALWARE,

however, is geared towards rooting out and destroying malicious programs that have already been downloaded

> AntiMalware looks for things that don’t match its algorithms. It will look at email and other applications, and flag suspicious behaviour. For example, if your computer tries to start up multiple programs that either don’t normally work together, or behave in ways they shouldn’t, it flags. If programs report back to parts of the network not normally communicated with, it flags.

HOWEVER, EVEN THE BEST ANTIVIRUS OR MALWARE PROTECTION WON'T NECESSARILY PREVENT LOSS OF DATA. COMPANIES MUST HAVE PROVEN BACKUP AND RESTORE POLICIES AND PROCEDURES. THESE PROCESSES MUST ALSO BE TESTED ROUTINELY TO ENSURE EFFECTIVE DISASTER RECOVERY.

Finally, we cannot underestimate the value of educating staff on security processes and procedures. Most importantly, these need to be tested. For example, staff could be sent fake emails, and if anyone clicks on them, your security officer is notified. Staff could then be redirected to a training website to re-enforce policy, with the aim of changing behaviour.

Awareness is the first step in preventing or addressing an issue. A holistic enterprise Security Risk Assessment will identify key areas of weaknesses, provide a full report of any exposure and make recommendations for remediation.

SOME ORGANISATIONS EMPLOY 'WHITE HAT HACKERS' OR 'ETHICAL HACKERS' WHO WILL TRY TO BREAK INTO THEIR CLIENTS' SYSTEMS, AND REPORT ON WEAKNESSES AND VULNERABILITIES.

They may also engage in a cyber-attack simulation (or sometimes called penetration testing) that tests the strength of current protective measures, and the processes that they would run in the event of an attack. These services can offer valuable pointers on where an organisations biggest vulnerabilities are - and

Security is best managed with a strategic approach. It requires a strong overarching governance framework, and a security design to meet the needs of your business, which can be deployed, managed, reviewed and updated.

PROTECTION

OUTSIDE

ENCRYPTION - It makes sense to have offsite backups. This could be via a managed data centre, or in the cloud, or in physical document archives. For electronic backup it is important to understand the levels of encryption provided by any organisation that transfers and/or stores your data. Choosing a managed service reduces your workload and skills needed, so it is vital that you do your due diligence on the provider.

TESTED BACKUP AND RESTORE - all organisations understand the need for backup, and many do so to an offsite location. But what is sometimes forgotten is the need to test the restore process. After all the only point of a backup is to have it in case of the need to restore. A full and regular operational test of the backup and restore process is an important security measure.

PHYSICAL SECURITY - It is important to validate the physical security measures of any location where your hard copies or digital data is stored. Consider protection against intrusion, fire, flood and earthquake and select only suppliers who follow industry best practices.

58% OF AUSTRALIAN BUSINESSES ARE LOOKING AT BIOMETRICS AND OTHER PHYSICAL

PORTABLE STORAGE – Establish a policy on whether portable storage devices (including memory sticks and laptops) will be allowed and if so, the rules for their use.

SECURE LOGIN – Ensure that mobile workers needing to access internal systems log in securely.

PERIMETER

FIREWALL - an enterprise standard firewall is a hardware device that sits on the perimeter of the network between the internet connection and an organisation's internal infrastructure. The firewall uses its own proprietary software to scan for malicious attacks and blocks them. For example, a message coming in on an email port that does not have the characteristics of an email will be blocked.

NETWORK PORT PROTECTION prevents a wireless network from being attached to your network. The third largest cause of breaches is network security, and in particular wireless networks.

ANTIVIRUS SOFTWARE – Malware is the single biggest cause of security breaches, so it is essential to have antivirus software to protect all endpoints.

PATCH MANAGEMENT – Installing vulnerability patches is one of the most straightforward security measures, and yet it is estimated that over one fifth of all businesses are six months or more behind with updates. Accordingly, it is the second largest cause of security breaches.

NODE PROTECTION – Desktops, laptops, printers, MFPs, IoT devices, faxes and phones are all nodes on your network. They are all intelligent devices with their own software operating environments and the capability to be compromised. Consider all nodes within your protection plan, as any single one of them could be a point of risk for the business.

PORTABLE STORAGE DEVICES – These are just as much of a risk within the office walls as outside, so policies need to specify if and how they will be used to upload and/or download data. Consider not only laptops and desktops, but that many printers now allow scan and print of a document directly to or from portable storage.

PRINT COLLECTION – Sensitive data can very easily fall into the wrong hands within an organisation via the printer. Job release functionality on a printer means that the job is not actually released for printing until the sender authenticates at the device, guarding against inadvertent or deliberate collection by the wrong person.

ACCESS PRIVILEGES AND PASSWORDS – Documents and systems should be accessible only to the staff who need them, not to everyone. This can be controlled by an access privilege system. As part of this system, passwords offer access protection, but only if well managed. A password policy should be implemented – consider the frequency with which they have to be changed, and the level of complexity, to guard against discovery.

PHYSICAL SECURITY –Just as not everyone needs access to all digital resources, the same is true of physical locations. Restricted access to certain departments or parts of the building is an important security measure. For example, not everybody needs access to the IT server room.

DISASTER RECOVERY PLAN – An organisation might have great security measures for its regular location, but be aware of the need to not only protect, but restore data in the case of a flood, fire or other event forcing a move to temporary premises.

EDUCATION, CULTURE AND PROCESSES

SECURITY ISN'T JUST ABOUT THE TOOLS. IT IS ALSO ABOUT HOW PEOPLE BEHAVE, THE CHECKS THEY MAKE AND THEIR AWARENESS.

A key element of any program of security measures is educating staff and building a culture where awareness of security is high and its importance understood. Staff who handle client

SECURITY AWARENESS EDUCATION COULD INCLUDE

- **SECURITY BADGE PROTOCOLS** – Ensuring that employees do not allow unauthorised persons to have physical access. For example, through sharing of badges, or tailgating.
- **DISASTER RECOVERY SCENARIOS** – Training on guidelines and processes to ensure that data remains protected in the case of a disaster, such as a move to temporary premises or a change in working conditions.
- The risks of using **UNSECURED WI-FI** outside the office.
- Understanding and implemented **PASSWORD RULES** – and never using default passwords.
- Security guidelines for the use of **LAPTOPS/PHONES** for accessing email and other office systems.
- Policies about which **PHYSICAL DOCUMENTS** can be taken offsite, if any.
- Having **SECURITY CLASSIFICATIONS** marked on documents.
- Awareness of the risk of **DOWNLOADING** from an App Store.
- Not divulging information over the phone to an unknown or **UNVERIFIED CALLER**.
- Understanding and following the compliance rules around **REPORTING** a security breach.

LOGGING

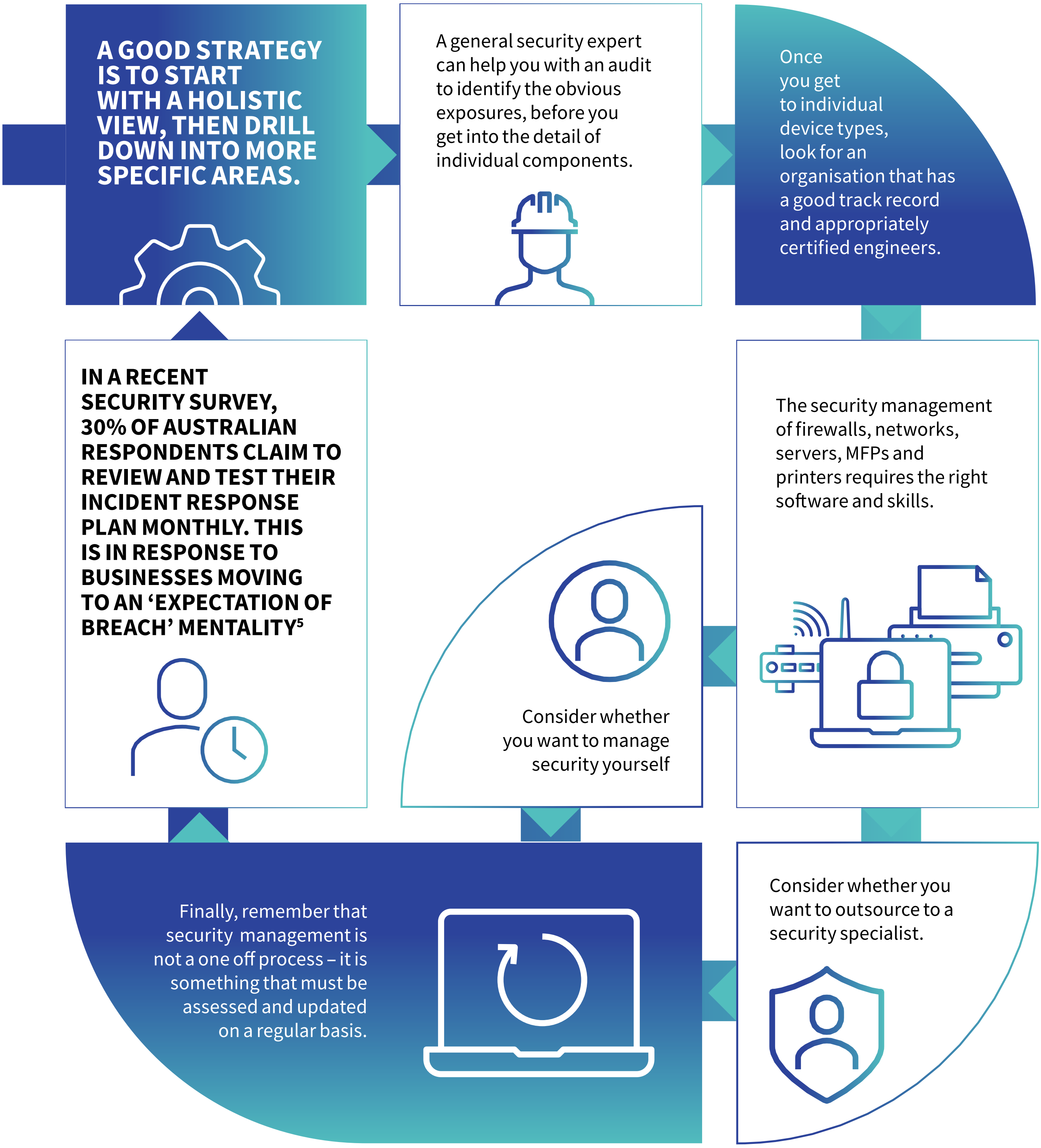
Even the best security measures are susceptible to being breached. Logging is an essential tool to help identify when, where and how those breaches or attempts have taken place.

Knowing that someone has tried to compromise your systems shows you where your security measures are working and, if the attempt was internal, allows disciplinary or other measures to be taken.

Whilst not being preventative, reports showing that an actual breach has taken place are an invaluable tool for reviewing and updating your security measures.

Logging is also an essential tool to help businesses meet their requirement to report security breaches. As we know, all businesses in Australia have a legal obligation to report security incidents and cannot do this without accurate logging in place.

WHO CAN HELP?



A GOOD STRATEGY IS TO START WITH A HOLISTIC VIEW, THEN DRILL DOWN INTO MORE SPECIFIC AREAS.

A general security expert can help you with an audit to identify the obvious exposures, before you get into the detail of individual components.

Once you get to individual device types, look for an organisation that has a good track record and appropriately certified engineers.

The security management of firewalls, networks, servers, MFPs and printers requires the right software and skills.

Consider whether you want to manage security yourself

Consider whether you want to outsource to a security specialist.

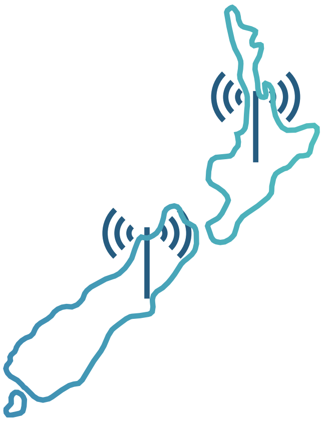
Finally, remember that security management is not a one off process – it is something that must be assessed and updated on a regular basis.

IN A RECENT SECURITY SURVEY, 30% OF AUSTRALIAN RESPONDENTS CLAIM TO REVIEW AND TEST THEIR INCIDENT RESPONSE PLAN MONTHLY. THIS IS IN RESPONSE TO BUSINESSES MOVING TO AN 'EXPECTATION OF BREACH' MENTALITY[5]

IN CONCLUSION

SECURITY IS A VERY REAL CONCERN FOR AUSTRALIAN AND NEW ZEALAND BUSINESSES, WITH BREACHES CARRYING THE RISK OF FINANCIAL, REPUTATIONAL AND COMPLIANCE RISK.

A ROBUST SECURITY STRATEGY coupled with guidance from subject matter experts will go a long way towards protecting information, minimising damage and mitigating risks.



To learn more about how Toshiba can keep you secure, go to: toshiba-business.com.au/support/security

[1] PWC CEO Survey 2021
[2] General Data Protection Regulation (GDPR) (EU) 2016/679
[3] Privacy Amendment (Notifiable Data Breaches) Bill 2016
[4] Simon Sharland, The Register, May 2018
[5] Telstra Security Report June 2018
[6] http://www.itpro.co.uk/malware/28153/whats-the-difference-between-antimalware-and-antivirus-1