

10 IT Security Essentials

for Australian Business

2020 Edition







Cybersecurity demystified, including:

- ✓ Critical questions to ask of your business
- ✓ Need to know information about Australia's data breach laws
- ✓ Helpful checklists and actionable advice

What is Cybersecurity?

Cybersecurity is the continual pursuit of digital data safety. It aims to ensure only authorised people can gain access to data. However, too often data ends up in the wrong hands.

Imagine
if a hacker...

-  Encrypted your important files or programs and blackmailed you for their release
-  Stole your customers personal contact details, health data, TFN or credit card data for ill use
-  Took your best IP and gave it to your competitors
-  Impersonated a creditor and emailed your accounting team a request to transfer payment to a different (fake) account
-  Hacked your phone and posted malicious content in your name
-  Stole your identity

All these, and more, happen every day to businesses like yours across the globe.

In this eBook, we explore 10 questions to ask of your business regarding IT Security.

In this eBook

	Page
Q1 Why should I care about cybersecurity?	04
Q2 Why is cybersecurity a business-wide responsibility?	05
Q3 What do Australia's Data Breach Laws mean for my business?	06
Q4 What does a good defence strategy look like?	08
Q5 How do I keep my security strategy up to date?	10
Q6 How can I check if my team or outsourced partner is on top of security?	12
Q7 Why are your staff members your weakest link?	13
Q8 Gap analysis: Where does my cybersecurity strategy need improving?	15
Q9 The last stand: would my company survive a breach?	16
Q10 How can Huon IT help my business?	18



Did you know?

During 2019, 65% of Australian businesses were interrupted by a security breach – up 5% since 2018.

Telstra Security Report 2019

Q1. WHY SHOULD I CARE ABOUT CYBERSECURITY?

Cybercrime is big business.

Recent worldwide outbreaks like Wannacry and Petya have very publicly brought cybersecurity in to the spotlight. Companies of all sizes experienced breaches and substantial performance and financial pain.

We hear the topic of cybersecurity on the lips of managers everywhere, however many struggle to know where to start.

- Cybersecurity is an ongoing process, not a destination. The threat landscape changes rapidly and requires regular updating of knowledge, technology, solutions and strategy.
- Technology alone is not enough. Cybersecurity means fostering a culture of awareness throughout an organisation—starting from the top.
- IT experts play a crucial role in IT security, however they can't do it alone. Entire business engagement is crucial.

An effective approach is multilayered and considers people, policy and technology. Many organisations choose to have an experienced partner on board to guide and assist them in this process.

Q2. WHY IS CYBERSECURITY A BUSINESS-WIDE RESPONSIBILITY?

“ANU cyber attack began with email to senior staff member.”

Australian Financial Review, October 2, 2019

Security incidents continue to hit the headlines with alarming regularity. In recent years, companies such as Facebook, UBER, and Marriott have all felt the impact of data breaches.

But the impact isn't just being felt overseas. With local businesses like the **ANU, Canva, Australian Red Cross, Cadbury** and **TNT** impacted, it's no surprise that cybersecurity has transitioned from an IT issue to a 'whole of business' concern.

In the 2019 Telstra Security Report, it was reported that security threats have the attention of executives and boards. “The CEO or board members have a ‘high’ or ‘very high’ formal level of involvement in cyber and electronic security in 48% of respondent organisations.”

Cybersecurity is a business-wide responsibility, and needs to be on the radar of everybody, from the TOP down.

“

The introduction of new regulations ... as well as several high-profile privacy breaches, has driven C-level and senior management interest in security with one-third of Australian respondents saying the frequency of meetings with senior stakeholders has increased.

Telstra Security Report 2019

”

Q3. WHAT DO AUSTRALIA'S DATA BREACH LAWS MEAN FOR MY BUSINESS?

Australia's Notifiable Data Breach Laws came into effect on the 22nd February, 2018. The laws carry the possibility of fines up to \$1.8 million for non-compliance.

The Act means that organisations which fall under the **privacy principles** (and some others) will have to notify affected staff/customers and the Office of the Australian Information Commissioner (OAIC) of eligible data breaches – exposing the company to possible widespread media scrutiny.

Firstly, what is a data breach exactly?

Data Breach

According to OAIC "A data breach is when personal information held by an entity is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference." For example, personal information is lost, stolen or hacked.

VS

An Incident

A security incident (different to an ITIL framework incident) is an event that violates an organisation's security or privacy policies and can range from a virus or a lost thumb drive to a malware attack that encrypts (but doesn't steal) sensitive files.

If you experience a breach, do you have a plan in place? Are you ready?

A plan is essential, not only for compliance, but also to ensure that you are both prepared to handle any customer backlash or media coverage fallout and are in the best position to minimise reputational and financial burden.

The Privacy Amendment Act 2017 in a nutshell

Who is subject to the regime?

Australian Privacy Principle (APP) entities, credit reporting bodies, tax file number recipients holding information subject to the information security requirements under the Privacy Act.



When is the requirement to notify triggered?

When an entity is aware that there are reasonable grounds to believe that there has been an 'eligible data breach' of the entity.



Do any exceptions apply to the notification requirements?

Yes, there are a range of exceptions, including where the affected entity takes sufficient remedial action in response to the eligible data breach before it causes serious harm.



What does notification involve?

The entity must notify the OAIC and all individuals affected by the breach. If impractical to notify all affected individuals, the entity must publish a statement on its website and publicise the content of the statement. The notification must set out certain matters about the eligible data breach.



What are the possible sanctions?

Serious or repeated failure to comply could expose the affected entity to the risk of material civil penalties. There is also the risk of reputational and associated commercial damage.

Q4. WHAT DOES A GOOD DEFENCE STRATEGY LOOK LIKE?

The three key points of defence

Cybersecurity and complexity are often seen hand in hand and can be a major barrier for some businesses. However, the crucial elements of cybersecurity can be very approachable, starting with the three key pillars of defence:



People - including contractors, staff, customers and partners, are often classed as the largest vulnerability in a security plan. A strong defence plan has them on board, trained and tested regularly.



Policy development and implementation sets corporate rules that lets people know what is acceptable instead of advisable in and out of office hours. Rules can either be in the form of written guidelines, or preset technology policies such as making some files invisible to certain users, or preventing programs from downloading.



Technology selection, implementation, maintenance, updating and protection. Different technologies provide different capabilities and need different types of protection. Networks need appropriate firewalls, email needs spam filtering, endpoints need antivirus, applications and systems need patching. Requirements change as new vulnerabilities and threats are discovered.



Did you know?

Over 4.1 billion records have been exposed globally in the first six months of 2019.

www.us.norton.com

The Essential Eight

How do you reduce your business' exposure to cyber risk?

It's important to note that no single risk mitigation strategy is guaranteed to prevent a breach. Instead, it's recommended that you take a multi-layered approach.

The Essential Eight guidelines were created by the Australian Signals Directorate (ASD) for businesses and government. It is recommended that these guidelines are implemented in consecutive order for maximum protection.



Mitigation strategies to prevent malware delivery and execution

1. Application whitelisting of approved/trusted programs to prevent unapproved/malicious programs and installers.
2. Configure Microsoft Office macro settings to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
3. Patch applications. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
4. User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office, web browsers and PDF viewers.



Mitigation strategies to limit the extent of cyber security incidents

5. Restrict administrative privileges to operating systems and applications based on user duties. Regularly re-validate the need for privileges. Don't use privileged accounts for reading email and web browsing.
6. Multi-factor identification including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important data repository.
7. Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.



Mitigation strategies to recover data and system availability

8. Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.

Source: www.cyber.gov.au

Q5. HOW DO I KEEP MY SECURITY STRATEGY UP TO DATE?"

Cybersecurity threats come in many forms. Experts say it is not a matter of if you are breached, but **when** and **how serious** the breach will be.

Prevention is better than cure. However cybercrime evolves so quickly it is impossible to 100% protect all fronts, even if you had an endless budget. It is therefore important to continuously review and update your strategy.

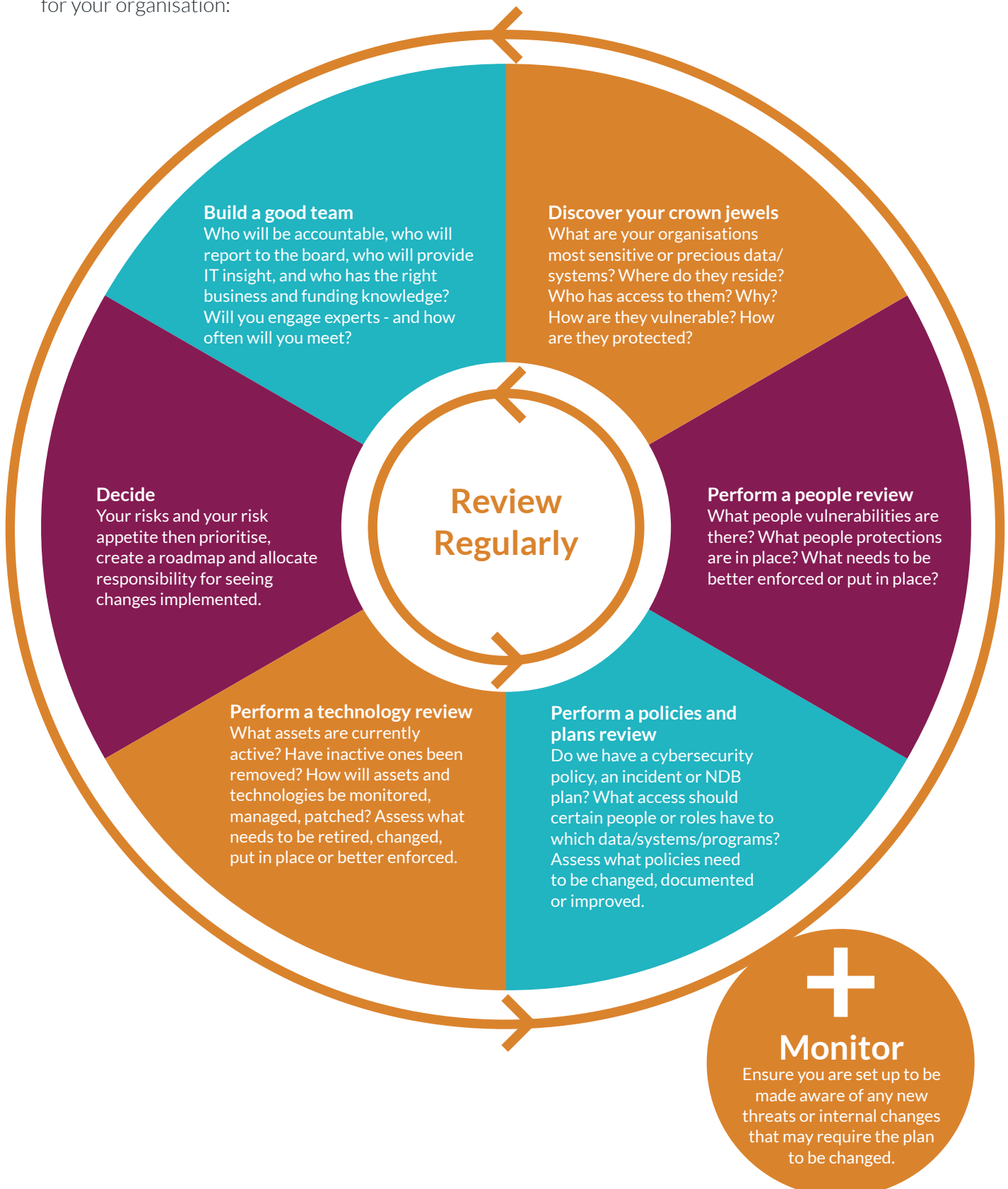


Did you know?

In the 2nd quarter of 2019, 62% of the notifiable data breaches reported in Australia were due to malicious or criminal attacks, 34% were due to human error, and 4% were due to system faults.

www.oaic.gov.au

The following items assist the creation of a well informed cybersecurity defence strategy for your organisation:



Q6.

HOW CAN I CHECK IF MY TEAM OR OUTSOURCED PARTNER IS ON TOP OF SECURITY?

Whether you, your IT department, or an outsourced partner is managing your cybersecurity defence system, it is critical to regularly check in on the status.

Often overwhelmed with a long list of competing demands it is easy for essential items to be delayed or overlooked, therefore it is useful to be able to ask some basic questions.

We have listed some questions here to get you started.

Key questions to ask your gurus (or yourself!)

1. Can you please explain the layers of cybersecurity defense that you have in place?
What could you improve or add?
2. What are your current key threats?
3. How many breaches have you had in the last year and how were they handled?
4. Do you have incident and response plans in place, and are they current?
5. How do you monitor for potential intrusions to your systems, applications and network?
6. What is the current patch management strategy?
7. Who has administrative privileges and are they appropriate? Why?
Have they been trained in how to use these safely, and what not to do?
8. Have you worked with HR to help provide training to staff and contractors,
set up IT use policies and onboarding tools?
9. How do you assess your organisation, vendors and the security of third parties that have access
to your environment?
10. Are you providing regular cybersecurity reports to management?
Is there anything you think needs to be added to these?

Q7. WHY ARE YOUR STAFF MEMBERS YOUR WEAKEST LINK?



Did you know?

While malicious breaches were the most common, inadvertent breaches from human error and system glitches were still the root cause for nearly half (49%) of the data breaches.

IBM Security Cost of a Data Breach Report 2019

Respondents in Telstra's Security Report 2019 identified the greatest risk to IT security as human error.

More than half of the "bad guys" are insiders*

* anyone who has physical or remote access to a company's assets



25%
accidental insider

11%
targeted insider

8%
malicious insider

Telstra's Security Report 2019

- "A major source of risk to IT security is human error, which is often caused by inadequate business processes and by employees not understanding their organisation's security policies. Human error or a targeted attack on an employee were cited as the highest risks to IT security by 36% of respondents."
Telstra Security Report 2019
- "80% of hacking-related breaches involve compromised and weak credentials. 29% of all breaches, regardless of attack type, involved the use of stolen credentials."
Verizon 2019 Data Breach Investigations Report
- "More than half (51%) of data breaches are caused by malicious attacks."
IBM Security: Cost of a Data Breach Report 2019

How to turn staff from security liabilities into human firewalls:

Do you provide IT capabilities that enable staff to do their jobs well? Simple things like allowing the use of personal devices and remote access capabilities can unfortunately, open a raft of potential access points for criminals to access your company's prized data.

That is why every organisation needs a human firewall—where every staff member takes pride in filtering their actions to protect the organisations data.

Establishing a “cybersecurity first”, human firewall culture from the top down is one of the strongest cybersecurity steps you can take—and it starts with education.

Education:

- Teach your employees how to recognise a risk. These include foreign executable file types, a misleading website, a phishing email attack and a targeted whaling attack.
- Establish policies that ensure any unusual requests for transfer of money or information are identifiable—be it through a policy that this will never be requested remotely, a special code or training staff to query and double confirm using a secondary channel.
- Encourage a “speak up” culture, where peers expect and teach one another cybersecure practices and can identify and report anomalies.
- Work with your HR team to deliver this education in both inductions for new hires, and regular refreshes for existing staff.

Phishing Awareness Training & Simulation

Safe phishing tools exist to help you understand your organisation's phishing risk, educate your staff, nurture awareness and prove success across your organisation.

A ‘fake’ spam email, which is convincing but safe, will be sent to your staff, and their responses monitoring – including who opened a suspicious attachment and/or clicked on malicious links.

This helps you then identify which staff in your team need security awareness training.

Q8.

GAP ANALYSIS: WHERE DOES MY CYBERSECURITY STRATEGY NEED IMPROVING?

Cybersecurity is a big task, and so far we have covered a lot.

Once you have had crucial conversations with IT, HR, marketing, partners, and possibly some sample staff members, then it's time for your team to review the gaps and refine your strategy.

A key question that is often overlooked is: Where do we need help?

Help may be in the form of training up existing staff, hiring a Chief Information Security Officer (CISO), or seeking the guidance of a Cybersecurity partner.

It is also often useful to conduct formal assessments to shine a light on dark corners and help you know what you don't know.

Penetration Testing

This service tests any web-exposed elements of your network, including:

- IP addresses,
- Websites,
- Applications, and
- Infrastructure

Discrete methods mimic the methodologies and attack patterns used by cyber criminals to identify any vulnerabilities.

These vulnerabilities will be rated according to severity, and clear recommendations on how to fix these weaknesses will be provided.



Did you know?

49% of participating C-level executives have cybersecurity issues on their board's agenda once a quarter.

Deloitte. The future of cyber survey 2019

Q9. THE LAST STAND: WOULD MY COMPANY SURVIVE A BREACH?

While every business should do its utmost to prevent a cybersecurity breach, the reality is that it could still happen. Even with state of the art defence technology in place, the bad guys are often a step ahead.

So if all else fails and you get 'locked out' or your system is taken down, ensuring you have an IT continuity plan in place is critical.



Did you know?

According to the National Cyber Security Alliance 60 percent of small and midsize businesses that are hacked go out of business within six months.

www.staysafeonline.org

Back up your files, securely

Cyber-nasties such as Ransomware work by 'locking' (a.k.a encrypting) your files, and demanding payment to unlock them or they will be deleted by a certain date.

Backups can be your saving grace, but only if done right.

Your backups face three risks:

Backing up already locked files

Ransomware can work quietly in the background for some time, so before you know it, your backup system has been backing up already locked files.

Compromised backups

Ransomware can also lock the backup files themselves – preventing you from restoring those, too.

Missing data

Is all of your data actually backed up in the first place? All too often businesses believe they have everything backed up, however when it comes to restoring there can be gaps.

To ensure your backup system can brave such an attack, ensure you are using up to date backup software across ALL devices which securely encrypts your backup files, allows your IT team to 'sandbox' (isolate) breaches, and offers versioning and long term retention so you can restore to a point in time before the attack.

Disaster Recovery (DR) & Business Continuity

While most people think of DR plans for building fires and floods only, a major IT security breach certainly warrants the term 'disaster', too!

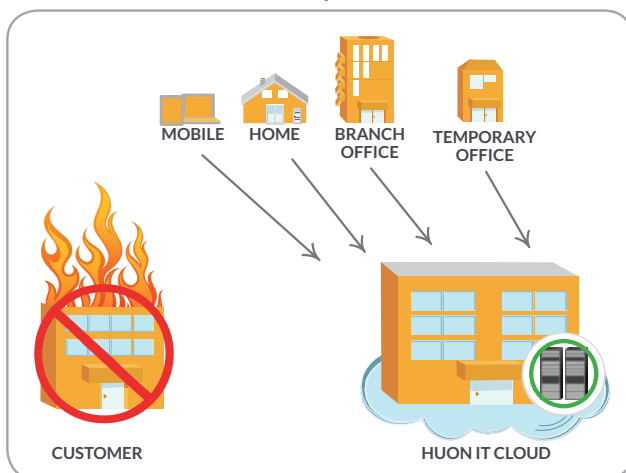
If the worst does occur and your IT systems are taken down, you should have a solid plan in place that will allow staff to swing in to action. This extends far beyond the IT team (who will be busy trying to recover files or even restore your entire environment to your disaster recovery system).

Every single employee has a role in the post-attack process, including communicating with clients, activating workaround plans to keep critical operations running, and dealing with your legal team to address repercussions of such an attack.

Simply writing such a plan isn't enough, either. It needs to be distributed to all staff, trained, and regularly reviewed and updated.

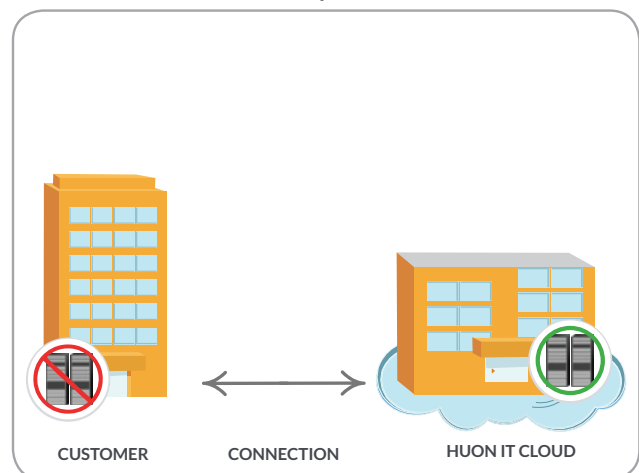
Remember – cybersecurity breaches don't just happen to other people. Be prepared.

Scenario 1: Physical Disaster



In the case that an entire building is offline, (e.g. fire or extended power failure), servers will be brought online at the DR site and users given remote access. Users can then work from anywhere that has an internet connection.

Scenario 2: System Failure



In the case that critical system hardware has failed, your servers will be brought online at the DR site and network routing re-adjusted to point users to the servers at the DR site, and users will continue to work at their desk.

Q10. HOW CAN HUON IT HELP MY BUSINESS?

“ The ability to timely detect and effectively respond to incidents is still the number one challenge for Australian companies when managing electronic security. Alarming, 19% of Australian respondents surveyed estimated that more than half of the data breaches impacting their company went undetected altogether in the past year. This is despite 74% of Australian businesses believing they have strong systems in place to verify when an incident has occurred. ”

Telstra Security Report 2019

Technology can have the powerful but polarising ability to either enable, or disable, a business.

Here at Huon IT, we strive to find the perfect balance between productivity and sound cybersecurity. Stopping all attacks may not be possible, but you can put the odds in your favour—from good system design through to training, timely management, proactive monitoring and the establishment of robust incident, back up and IT continuity plans.

Many organisations aren't in a position to have all the knowledge, resources or time to really step back and gain an in depth, unbiased perspective of their cybersecurity posture, nor follow up all the alerts that come through.

Whether you have a complete IT department and are looking for a third party perspective, or to outsource your IT, we are here to help you turn technology in to a key asset that opens opportunity and growth.

Huon IT's Core Security Services

Strategic Services for Executive Teams



Huon IT's Cybersecurity Maturity Program is a 12-month long program for CEOs, Directors, CFOs, COOs, as well as IT & Compliance teams.

The purpose of the program is to guide leadership teams through assessment, planning and continued review of your organisation's cybersecurity strategy. This program is tailored to each business' unique requirements and the engagement typically follows three phases over a 12-month period. These include:

- Discovery & audit
- Planning & recommendations
- Steering & remediation

Audit Services



Security risks can lurk internally and externally. The following security audits should be conducted once every 1-2 years at a minimum (or more depending on your business' risk profile):

Network penetration testing:

Cyber-criminals look for holes in your system – so we want to find them before they do. With a penetration test, you can safely see just how far a real-world attacker can actually get with your current IT security systems & address any holes before it's too late. This service tests any web-exposed elements of your network including:

- IP addresses,
- Websites,
- Applications, and
- Infrastructure

You will be provided with recommendations on how to fix these issues. If you need help to implement the changes, Huon IT's security experts are on-hand to help your team.

Vulnerability assessment:

While penetration testing is an external security check of your web elements, vulnerability assessments identify wider risks within your network setup. They include a review of your:

- Core infrastructure (including switches, routers, firewalls, applications etc.) and
- End-user security (e.g. anti-virus, anti-malware, mobile devices and password policies).

Proactive Monitoring



To defend Australian business networks and devices against malicious threats, abnormal user behaviour and data breaches, Huon IT's Security Operations Centre (SOC) operates 24/7, 365 days a year.

In the Cyber Patrol service you will receive:

- Daily 24x7 monitoring via our world class Security Incident & Event Management (SIEM) system.
- Weekly vulnerability scans & monthly reports to identify any new potential weaknesses.
- Expert analysis by real people reviewing and validating issues, around the clock.
- License per device for an affordable monthly fee.

Defensive Systems



Huon IT has a broad portfolio of best-of-breed defensive security systems including:

- Managed infrastructure
- End-point antivirus
- Email filtering & protection

Managed infrastructure



End-point antivirus



Email filtering & protection



Staff Education



Even with the latest and greatest technology safeguards in place, the “human factor” can still leave you exposed to risk.

To minimise the risk of users inadvertently clicking on suspect links, accidentally releasing their password or unintentionally downloading malware, education is more crucial than ever before.

Huon IT’s Cybersecurity Awareness Training is conducted over a 12-month period. It covers:

- Baseline testing
- Training your users
- Regularly phishing your users
- Reporting and re-training as required.

mimecast

KnowBe4
Human error. Conquered.

To prepare for the worst, only trust the best.

Contact the security experts at Huon IT today for custom advice on how to ensure your business is safe.

P: 1300 HUON IT (4866 48)
E: info@huonit.com.au
www.huonit.com.au