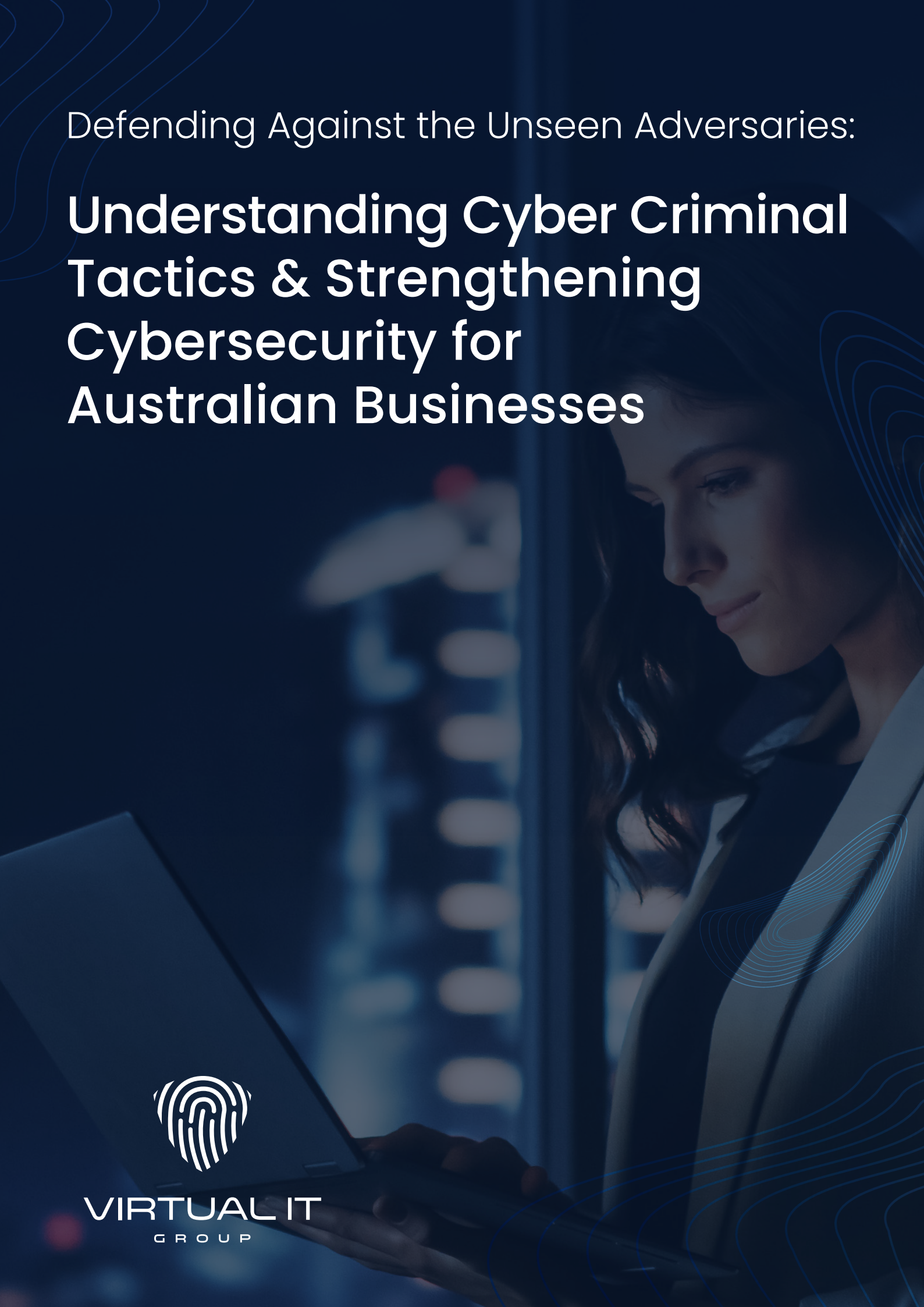
Defending Against the Unseen Adversaries:

Understanding Cyber Criminal Tactics & Strengthening Cybersecurity for Australian Businesses



VIRTUAL IT
GROUP

The current state of cybersecurity globally and its impact on Australia.

When thinking about cybersecurity, it's helpful to take a big-picture view. Zooming out helps us to find our footing in the fast-paced world of technology and gives context to the ever-evolving threats businesses and individuals face.

We are living squarely in the middle of the 4th Industrial Revolution. Though we're not seeing changes on the same scale as earlier Industrial Revolutions, we are experiencing a faster pace of change. Technology is advancing exponentially, and our lives are more than ever inextricably linked to the digital world.

Think about how you interact with technology daily and how this has changed over the past five years. You will probably be able to identify areas where you previously interacted minimally with technology that is now almost entirely digital. Grasping this shift toward a more digitally connected world helps you understand why ever-increasing cyber threats are now a part of life. As we adopt many new apps, devices, and digital processes, we expose ourselves to cyber threats tailored to that specific technology.

How prevalent are cyber-attacks?

Cyber-attacks and data breaches happen daily to all kinds of businesses. In the 2021-2022 financial year, there were over 76,000 reported incidences of cybercrime. This equates to one cybercrime report roughly every seven minutes, an increase of just under 13% from the previous financial year. Though online fraud was the most frequently reported form of cybercrime, ransomware gets the prize for the most destructive form of cybercrime. Popular methods of attacking in 2021-22 included:

1. Ransomware

Malicious software that encrypts a victim's files or systems, demanding a ransom payment in exchange for restoring access.

2. Phishing Emails

Deceptive emails that attempt to trick recipients into revealing sensitive information, often by impersonating legitimate entities.

3. Viruses

Self-replicating malicious code that attaches to legitimate programs or files and spreads when the infected file is executed.

4. Adware

Software that displays unwanted advertisements or redirects users to promotional content, often bundled with legitimate applications.

5. Spyware

Software designed to secretly gather information from a device or user without their knowledge, often for malicious purposes like data theft or surveillance.

Did you know?

There is one cybercrime targeting Australian businesses every seven minutes.

These figures highlight the multidimensional aspect of cyber-security. There is not one type of attack nor one type of target, so it follows that there can't be an overly simple approach to comprehensive defence. Understanding this reality is key to becoming more fluent in cyber security.

There are as many ways to be attacked as there are ways that we interact with technology - cyber threats are continually changing and evolving as technology is itself.

The cost of cyber-attacks to businesses

As digital threats grow, it's becoming more expensive for businesses to deal with the ramifications of a breach. The average cost of a data break in Australia is climbing 9.8% yearly, currently at $3.35 million per breach.

And while major businesses like Optus might deliver larger volumes and more valuable data to a hacker, smaller businesses are just as likely to be targeted. Fewer security measures and a lower public profile can actually make smaller businesses much easier to take advantage of.

Cybercrime Stats in Australia in 2022

$33 billion
Self-reported losses by Australian businesses due to cybercrime

$276,323 per business
Average cost of a cybercrime

53% of the cost being paid
is detection and recover

23-51 days
Time taken to resolve an attack

60% of all cyber-attacks
Targeted SMBs in Australia

Different categories of cyber criminals and their motivations.

We've touched on the multifaceted nature of cybersecurity threats. Knowing your enemy is a big part of the picture when it comes to defence. Understanding what motivates hackers can help remove the element of surprise and reduce the chances businesses, and individuals will be caught off guard. It's about becoming street-smart in the digital world.

The following descriptions of different types of threats and hackers will help you become better acquainted with the fast-paced world of cybersecurity.

Insider Threat

This is one area where many businesses least expect a threat to come from: inside the business itself. Employee negligence is a major cause of cyber-attacks. Employees unknowingly allow criminals into the business through unauthorised apps. And, on rare occasions, a disgruntled employee could try to bring the business down in revenge.

Individual Attackers

When you think of the stereotypical hacker, most thoughts turn to a hooded youth sitting alone in their room. This is the individual attacker, and their motives are often more one of curiosity and learning. They want to see if they can hack a system rather than attempt anything malicious. This is the most neutral cyber threat.

Industrial Espionage

The most common reason for industrial espionage is to discover the secrets of a rival business, often through spying. However, it could also involve destroying valuable data or, with some IoT devices, physically breaking the technology.

Cyber Criminals

These guys are purely out to make as much money as possible. Using the Internet, they can now easily target everyone in the world with just the push of a button. The list of methods these criminals use to make money from you is almost endless but includes ransomware, crypto-jacking, identity fraud, business email compromise scams, and many more.

Ethical Hackers

As the term ' ethical ' implies, an ethical hacker is the opposite of a cybercriminal. These types of threats are often undertaken for the sake of a company and have been paid for by the business to see if it can hack into its own servers. These hackers test a business's security resilience and locate vulnerable areas before an 'unethical' hacker comes along.

Hacktivists

A hacktivist is a subset of cybercriminals whose motives are more ideological. As the name references, a hacktivist is essentially a cyber activist. They are using hacking purely to push an agenda, whether political, religious, or otherwise, rather than a financial motive. A hacktivist attack can be as simple as changing the text on a company website to a more nefarious act that interferes with the business's day-to-day running.

Cyberterrorism

While hacktivists don't always cause damage, a cyber-terrorist will; like real terrorism, cyber terrorism exists to bring terror to your business, country and customers.

Nation-State

This kind of hacking is often government versus government. It is functionally indistinguishable from cyber terrorism, but the defining trait is that a country's government officially sanctions the attack. These attacks can involve not only hacking but the use of more traditional spying as well.

Top 5 Cyber Threats

Targeting small to medium businesses (SMBs) in the last 2 years	% or SMBs reported to have been attacked
1. Ransomware	64%
2. Phishing Emails	43%
3. Viruses	33%
4. Adware	30%
5. Spyware	29%

The evolution of cyber threats in 2023 and emerging trends.

Over the past few years, global events have exposed increased business vulnerabilities. The evolution of cyber threats has seen a progression from simple viruses to highly sophisticated attacks. In 2023, emerging trends include:

1. Advanced Ransomware:

Ransomware attacks are becoming more targeted and destructive, targeting critical infrastructure and data with high extortion demands.

2. Supply Chain Attacks:

Cybercriminals exploit vulnerabilities in third-party vendors to infiltrate target organisations, amplifying the impact of breaches.

3. Zero-Day Exploits:

Attackers leverage undisclosed vulnerabilities to infiltrate systems before they can be patched, posing significant challenges to defence.

4. Nation-State Attacks:

State-sponsored threat actors engage in cyber espionage, intellectual property theft, and disruptive attacks, elevating geopolitical risks.

5. AI-Powered Attacks:

Attackers use artificial intelligence for more sophisticated phishing, deepfake attacks, and evasion techniques, challenging traditional defences.

6. IoT Vulnerabilities:

As IoT devices proliferate, they introduce new entry points for attackers to compromise networks and data.

7. Rise of Insider Threats:

Insider attacks, either malicious or unintentional, continue to pose risks due to employee access to sensitive information.

8. Cloud Security Challenges:

Misconfigured cloud settings and inadequate security practices lead to data exposures and breaches in cloud environments.

9. Digital Currency Exploitation:

Cryptocurrency platforms and transactions are increasingly targeted by hackers for financial gain

To address these trends, organisations focus on threat intelligence, zero-trust architecture, AI-driven defences, employee training, and robust incident response plans. We'll walk you through the best cybersecurity practices in the second half of this eBook.

Consequences of Cyber Vulnerability

You've probably heard about several high-profile data breaches in recent news. These attacks are scary for impacted customers and worst-case scenarios for affected businesses, with fallout that extends far beyond what might be expected.

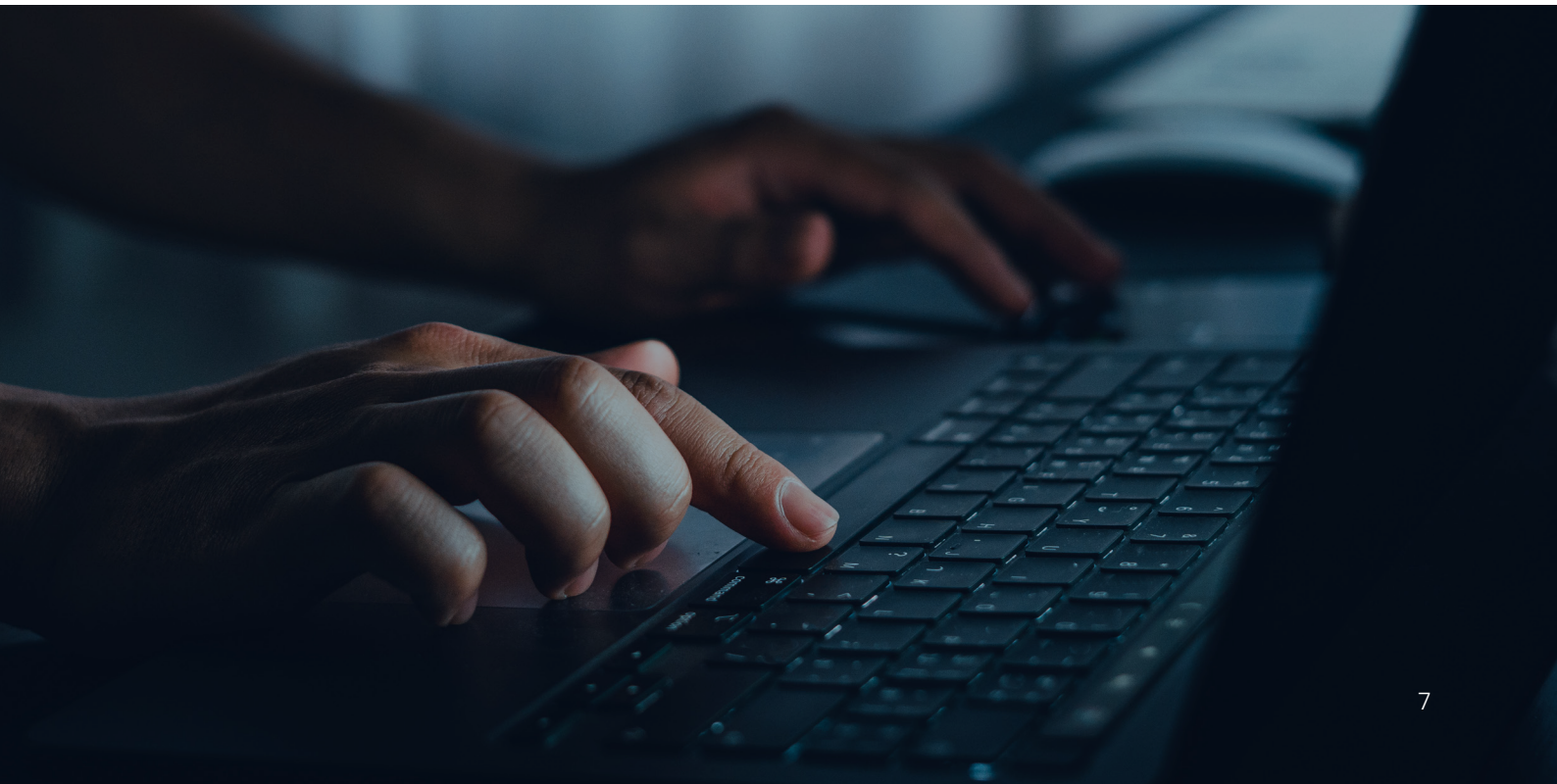
Optus experienced a cyber-attack and subsequent data leak in which the personal information of up to 9.8 million current and former customers was compromised – with approximately 2.8 million severely impacted. This data included full names, dates of birth, Medicare numbers, passport numbers, email addresses, bank details and more. A formal external investigation was conducted to determine the cause of the Optus breach and how other incidents can be prevented. And the fallout didn't stop there!

A class action was filed in the Federal Court of Australia against Optus on 21 April 2023 brought by two lead applicants whose personal information was significantly compromised by the breach.

Close on the heels of this attack, the Australian government announced that they plan to increase fines for companies who fail to protect customer data from $2 million to $50 million.

Another high-profile attack happened to Latitude Financial, who announced they were the victims of hackers in March of this year. The attack occurred after a hacker used privileged credentials bought from a third-party vendor to access Latitude's system and steal the data of 7.9 million customers. After the breach, the company set aside $46 million in customer remediation.

Medibank, Energy Australia and Woolworths were other high-profile targets who lost customer information to hackers. These tend to be the names that get our attention but don't let that influence how you perceive your attractiveness as a target as an SMB. The consequences are just as disastrous for smaller, less conspicuous targets.



The financial, reputational, and operational consequences of a cyber breach.

A cyber breach has severe consequences for all businesses.

Financially, breaches have associated direct and indirect costs.

Direct Costs of Cyber Crime	Indirect Cost of Cyber Crime
Discovering, investigating, containing and recovering from cyberattacks.	Lost revenue, staff productivity, brand and reputational risk.

Direct costs include incident response, legal fees, and fines. Indirect costs encompass customer compensation, lost revenue, and increased insurance premiums. There are also significant operational costs; breaches disrupt normal functions, causing downtime, data loss, and compromised systems. However, one of the most damaging costs to businesses is damage to reputation.

Reputational damage arises from customer distrust, negative media coverage, and diminished brand value that impact long-term profitability. How readily would you give your personal banking information to a business known to have had recent security breaches? This loss of trust hits businesses where it hurts.

Whether you are an SMB or a high-profile enterprise, the repercussions of cyber-attacks are significant and worth taking targeted measures to avoid. You might be thinking, if this is such a significant issue and companies are no doubt taking measures to prevent them, then why are so many breaches occurring?

Good point! The frequency of attacks comes back to the pace of technological change, cybersecurity illiteracy and highly motivated cyber criminals. So, what's working and what's failing disastrously?

Traditional cybersecurity measures – why they fall short in the current landscape.

Traditional cybersecurity measures, while essential, often fall short in the evolving cyber landscape of 2023. Legacy approaches have the following defining features:

- They rely on perimeter defences like firewalls and signature-based antivirus, which struggle to combat sophisticated, polymorphic threats and targeted attacks.
- They often lack real-time threat intelligence and struggle to adapt to rapidly changing tactics cybercriminals use.
- Traditional models assume a well-defined network perimeter; this approach is outdated in today's cloud-based, remote work environments hampering their ability to protect data and assets effectively.
- The rise of IoT, interconnected systems, and AI-driven attacks demands more dynamic, behaviour-based defences.
- Inadequate user awareness and training also persist as challenges.

The Essential Eight

Common cyber security approaches have evolved around the Essential Eight principles. The Essential Eight is an Australian cybersecurity framework developed by the Australian Cyber Security Centre (ACSC). Many businesses look to this framework to guide their cybersecurity responses. While the Essential Eight forms an important component of a cyber security plan, alone they are not enough to defend against advanced attacks.

The Essential 8 sets the stage, but a comprehensive approach is needed to tackle the complexities of cybersecurity threats.

The Essential Eight consists of:

1. **Application Control**

   allows only approved applications to run, reducing the risk of malicious software execution.

2. **Patch Applications**

   regularly update software and applications to fix vulnerabilities that attackers could exploit.

3. **Configure Microsoft Office Macros**

   turns off macros or ensure they are digitally signed before executing to prevent macro-based malware.

4. **User Application Hardening**

   configures web browsers and email clients to block potentially malicious content, enhancing security.

5. **Restrict Administrative Privileges**

   limit administrative access to only authorised users, reducing the potential impact of unauthorised changes.

6. **Patch Operating Systems**

   regularly updates operating systems to address vulnerabilities and enhance security.

7. **Multi-Factor Authentication (MFA)**

   requires multiple verification forms for user authentication, reducing the risk of unauthorised access.

8. **Daily Backups**

   regularly back up critical data and systems to minimise data loss in case of a cyber incident.

Sophisticated threats often employ advanced techniques, zero-day vulnerabilities, and social engineering tactics that may bypass or circumvent some of these measures.

The need for an updated, comprehensive approach to cybersecurity.

To defend against such advanced threats, organisations should consider implementing additional measures to the Essential Eight. Additional measures include:

1. **Advanced Threat Detection:** Utilise advanced threat detection tools, including behaviour-based analytics and machine learning, to identify abnormal activities and potential threats.

2. **Threat Intelligence:** Stay informed about the latest threat landscape and attacker tactics, techniques, and procedures to adapt defences proactively.

3. **Red Team Testing:** Conduct regular penetration testing and red team exercises to identify vulnerabilities and weaknesses that standard defences might not address.

4. **Security Awareness Training:** Educate employees about sophisticated social engineering tactics and encourage a security-conscious culture to minimise human error.

5. **Endpoint Detection and Response (EDR):** Employ EDR solutions to monitor and respond to suspicious activities at the endpoint level.

6. **Network Segmentation:** Segment networks to contain and isolate potential breaches, limiting lateral movement for attackers.

7. **Disaster Recovery Plan and Business Continuity Plan:** develop and regularly test a comprehensive incident response plan to minimise damage and recover quickly in case of a breach.

8. **Continuous Monitoring:** Implement real-time monitoring of network traffic, logs, and behaviour to detect anomalies and respond promptly.

Remember, cybersecurity is a dynamic field, and threats are constantly evolving. Combining the Essential Eight strategies with advanced measures tailored to the organisation's risk profile, a layered defence approach is crucial to defend against sophisticated threats effectively.

The Essential Eight is the 1st line of cyber defence only.

Futureproofing Your Business

A holistic approach involving AI-driven anomaly detection, zero-trust principles, robust user education, and continuous monitoring is critical to address defence shortcomings and bolster cybersecurity in the current threat landscape.

We've mentioned your first line of defence should consist of the Essential Eight guidelines; your **second line of defence** is one of the hardest components to get right - people.

Instilling a culture of cyber security awareness in your business is quite simply crucial. Remember the stats we shared above? An excessive number of attacks each year are caused by human error and cybercriminals using social engineering techniques to exploit some of our most human vulnerabilities: trust, fear, and greed.

Trust	Fear	Greed
Attackers often exploit people's trust by pretending to be someone they are not. For example, they might call or email the victim and pretend to be from a legitimate company, such as a bank or credit card company. They might also use a fake email address that looks like it's from a legitimate company.	Attackers also exploit people's fear by sending them emails or text messages that claim to be from the police or a government agency. The emails or text messages will often say that the victim is in trouble and that they need to provide their personal information or do something else to avoid being arrested or fined.	Attackers also exploit people's greed by offering them something they want in exchange for their personal information or doing something else that will benefit the attacker. For example, the attacker might offer the victim a gift or a discount on a product if they provide their email address or credit card number.

Key components of a business continuity plan

Every robust business continuity plan comprises several critical components:

- **Risk assessment:** This involves identifying potential risks that could disrupt operations and evaluating their potential impact. By understanding these risks, businesses can develop strategies tailored to mitigate them.
- **Recovery strategies:** Once risks are identified, the next step is to develop strategies to recover from these disruptions. This could range from alternative supply chain sources to relocating operations temporarily.
- **Communication plan:** During a disruption, clear communication is paramount. Establishing predefined communication channels ensures that stakeholders, both internal and external, are kept informed, ensuring smooth coordination.
- **Training and awareness:** A plan is only as good as its execution. Regular training programs ensure that staff are aware of the procedures to follow during disruptions, ensuring a swift and coordinated response.

See below a High-Level Business Continuity Plan Template:

1. Introduction

Overview of the business, its operations, and the purpose of the BCP.

2. Risk Assessment

Identification of potential threats and their impact on business operations.

3. Response Strategy

Detailed strategies for responding to identified risks.

4. Communication Plan

Procedures for informing stakeholders about disruption and the company's response.

5. Recovery Strategy

limit administrative access to only authorised users, reducing the potential impact of unauthorised changes.

6. Regular Review

Schedule for reviewing and updating the BCP, incorporating insights from business continuity tests.

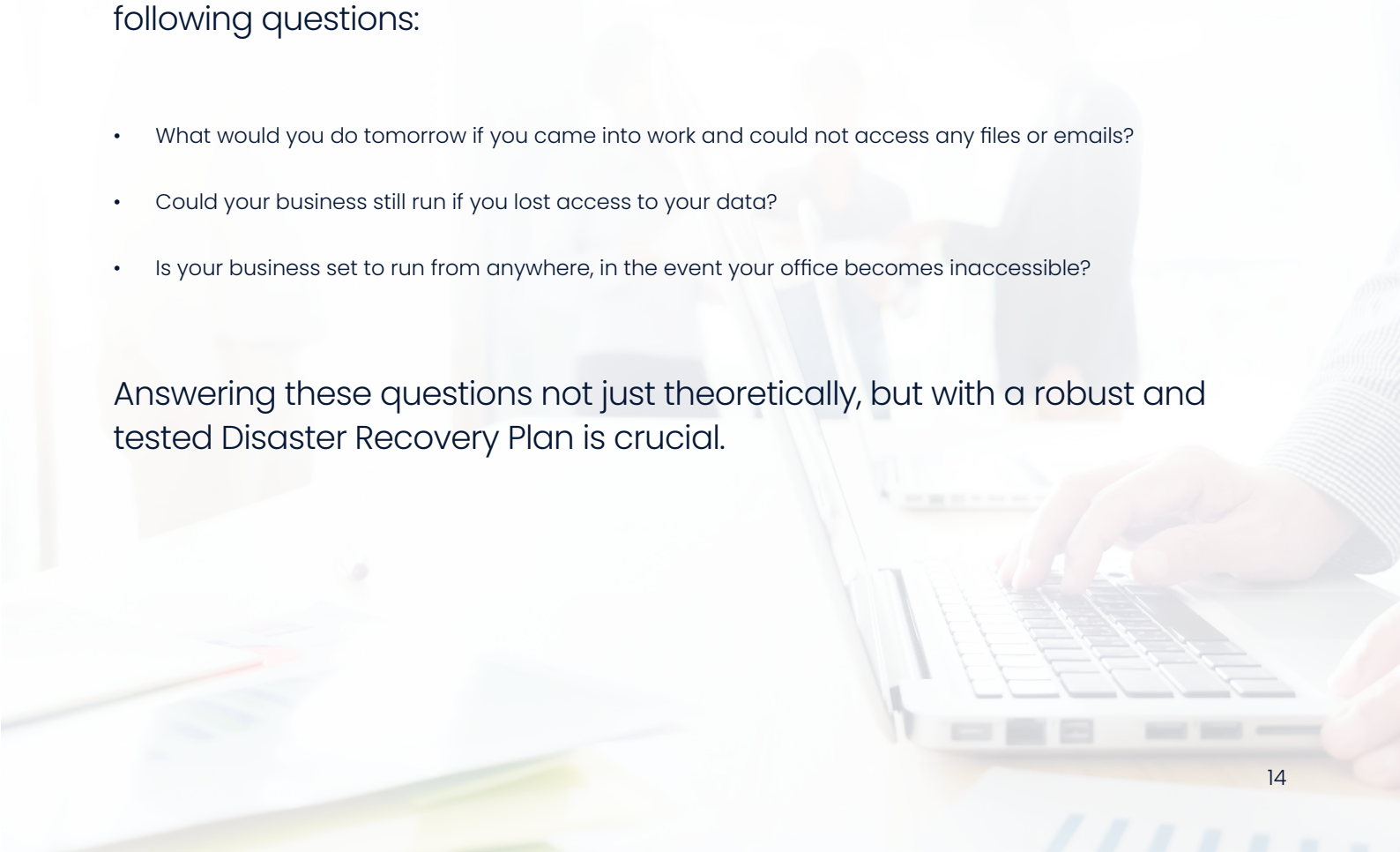
7. Training and Awareness

Plan for training employees and ensuring they are aware of their roles in the BCP.

Your **last line of defence is backup and disaster recovery.** Think about the following questions:

- What would you do tomorrow if you came into work and could not access any files or emails?
- Could your business still run if you lost access to your data?
- Is your business set to run from anywhere, in the event your office becomes inaccessible?

Answering these questions not just theoretically, but with a robust and tested Disaster Recovery Plan is crucial.



The key components of an effective cybersecurity strategy in the modern era.

1. Have you reviewed and adjusted the security settings of your cloud tenant and your organisation's internal network?

2. Have you ensured the security settings and measures for remote users are appropriate for current and foreseeable usage levels?

3. Is your team proficient in the latest security threats, or do they need help?

Time is not on your side:

Get a handle on your security picture. If you haven't had time to perform basic endpoint hygiene and connectivity performance checks on your computers and devices, better late than never. In addition to confirming all your laptops have the necessary endpoint protection configurations for all this new off-LAN activity, ensure your employees are following recommended security practices by asking these three important questions.

Continuous monitoring, threat detection, and fast, effective responses are crucial in cybersecurity.

Continuous monitoring

nvolves real-time observation of network activities, systems, and data to identify unusual behaviour or security anomalies. It provides ongoing visibility into an organisation's digital environment, helping to detect potential threats promptly.

Threat detection

leverages advanced tools, like intrusion detection systems and behaviour analytics, to identify malicious activities and patterns. Early detection allows for swift mitigation before threats escalate, minimising potential damage.

Effective response

involves a well-defined plan to address and mitigate identified threats. Rapid responses increase a business's ability to contain, eradicate, and recover from security incidents, reducing their impact and preventing future occurrences.

Together these advanced cyber security measures create a proactive defence posture, reducing the dwell time of threats, enhancing incident response efficiency, and safeguarding critical assets against a rapidly evolving cyber threat landscape.

The Business Case for Robust Cybersecurity

How cybersecurity resilience supports business continuity and growth.

We are living in a era of escalating cyber threats. Businesses that are proactive when it comes to security will not just lower the likelihood of an attack and optimise their response if one does occur, they will attract partners, customers, and investors who value a secure ecosystem. If it's not yet, the robustness of a business's cybersecurity stance will be one of the foundational pillars business stakeholders, including customers, will demand.

Businesses that can demonstrate security resilience are communicating that they can embrace the safe adoption of new technologies, expand into digital markets, and innovate without compromising security and critical business functions. These will be the businesses that are reinforcing their growth trajectory with cybersecurity resilience that guarantees the highest possible level of protection.

The role of cybersecurity in building customer trust and enhancing brand reputation.

Privacy is a word that is thrown around a lot in the consumer space. It used to mean that companies would commit to not selling or sharing your personal information with 3rd parties. Now it relates to the measures they are taking to protect the security and confidentiality of customer information.

When customers perceive that their personal information and sensitive data is well-protected, they are more likely to engage with a brand confidently. This confidence is needed to drive brand loyalty and positive word-of-mouth. How likely would you be to recommend a friend use a particular company's service if your information had been compromised?

In contrast, data breaches erode trust, leading to reputational damage, customer churn, and legal repercussions. By prioritising cybersecurity, brands protect assets and create a foundation of trust that drives customer satisfaction, competitive advantage, and long-term growth.

Two key ways businesses can demonstrate their commitment to security are by creating and implementing Business Continuity and Disaster Recovery plans.

Evaluating Your Cybersecurity Solution

Key questions to ask when considering a cybersecurity solution:

- Do we have a cybersecurity policy?
- What would be the first steps I'd take if we were to have a data breach?
- Do I know what cybersecurity my business has?
- As a company director or business owner, am I personally liable for costs should my employee's data be stolen?
- Would my team members know if they received an email from someone pretending to be someone else?

How to assess the alignment of a cybersecurity solution with business needs.

Assessing the alignment of a cybersecurity solution with business needs involves systematically evaluating how well the solution addresses the organisation's specific security requirements and objectives. The process of evaluating this alignment should include:

1. Requirement Analysis

Understand the organisation's business goals, operations, and critical assets. Identify the specific cybersecurity challenges and risks it faces.

2. Solution Evaluation

Thoroughly assess the features, capabilities, and functionalities of the proposed solution. Ensure it aligns with the identified business requirements.

3. Customisation

Determine if the solution can be tailored to meet the organisation's unique needs without compromising its effectiveness. **Consider whether it can integrate with existing systems.**

4. Scalability

Evaluate whether the solution can scale to accommodate future growth and evolving cybersecurity needs of the organisation.

5. Cost-Benefit Analysis

Analyse the financial implications of the solution. Consider the total cost of ownership (including licensing, implementation, and maintenance) and weigh it against the potential benefits and risk reduction.

6. Compliance and Regulations

Ensure that the solution aligns with relevant industry regulations and compliance requirements that the organisation must adhere to.

7. User Experience

Consider the ease of use and manageability of the solution. It might not fit with business needs if it introduces complexities that get in the way of productivity.

8. Feedback and Collaboration

Involve key stakeholders, including IT, security teams, and business leaders, in the assessment process. Their input is vital to ensure alignment.

9. Pilot Testing

Conduct a pilot test of the solution in a controlled environment to validate its effectiveness and compatibility with business operations.

By carefully considering these factors, organisations can assess the alignment of a cybersecurity solution with their business needs and make informed decisions to enhance their security posture.

Your Next Step: Building Cyber Resilience

Cybersecurity can feel like an overwhelming topic and can lead to businesses inadvertently avoiding looking it square in the face or reverting to an 'it won't happen to me' stance. We hope that you are now more aware of the significant risks posed by cyber threats and how much businesses can do to put themselves in the safest possible position.

If you would like to find out more about the types of cybersecurity support we offer businesses at VITG, you can contact us here or click the links below.

Resources:

https://vitg.com.au/what-cyber-security-lessons-can-australian-businesses-learn-from-the-multiple-recent-data-breaches/

https://www.slatergordon.com.au/class-actions/current-class-actions/optus-data-breach

https://www.9news.com.au/national/latitude-hit-with-1-million-lawsuit-over-data-breach/569fbba9-5b10-47c5-b2a9-36c6b7934960

VIRTUAL IT GROUP

1300 144 984 info@vitg.com.au Virtual IT Group

HEAD OFFICE 1 Lamerton Crescent, Shellharbour City Centre NSW 2529