Proposed Enhancements to the Australian Cyber Security Centre Website: Customised Security Controls for Medium, Small and Micro Businesses

Alicia Eaton,

Aymon Husari,

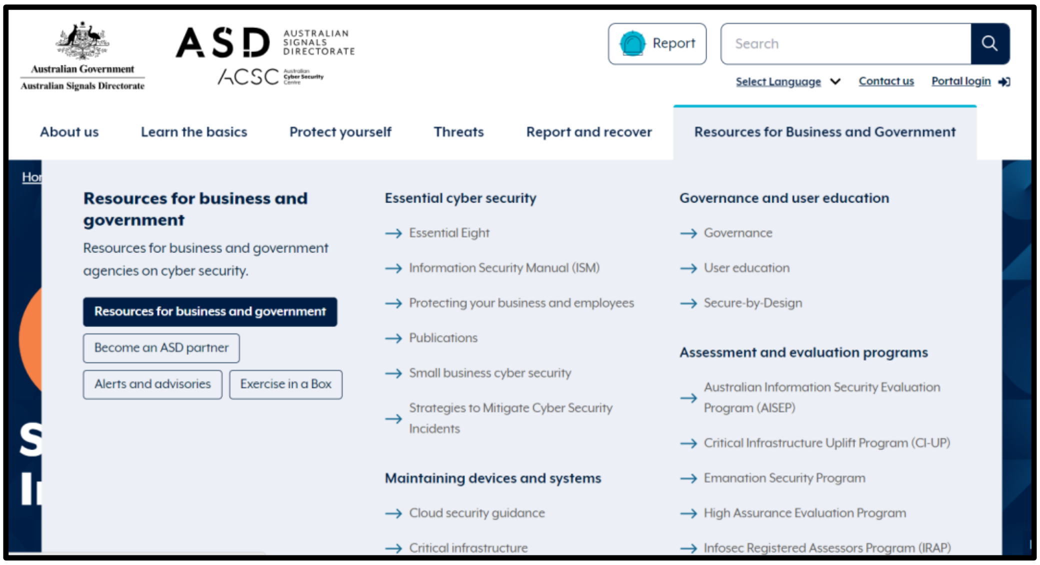
& Callum Macintosh

INTRODUCTION

The Australian Government is invested in protecting the country from cyber threats, rolling out initiatives such as the National Plan to Combat Cybercrime (2022), partnering with tech company Microsoft for investment in protective measures, and conducting annual threat reports through the Australian Cyber Security Centre. The Australian Signals Directorate's Cyber Security Centre (ASD's ACSC) is the lead agency for cyber security and is responsible for monitoring and reporting on global cyber threats (ACSC, n.d.). This organisation manages a popular website, cyber.gov.au, which provides advice and information to individuals and organisations on how to stay protected online. Its content is written for four separate groups: individuals and families, small and medium businesses, large organisations and infrastructure, and government.

The focus of this research project is directed at the content the ACSC has provided for businesses (See Figure 1). Generally, the ACSC has categorised its business relevant information into the following groups:

1. Essential Cyber Security
2. Maintaining Devices and Systems
3. Governance and User Education
4. Assessment and Evaluation Programs



Resources for business and government

Resources for business and government agencies on cyber security.

Resources for business and government

Become an ASD partner

Alerts and advisories Exercise in a Box

Essential cyber security

→ Essential Eight
→ Information Security Manual (ISM)
→ Protecting your business and employees
→ Publications
→ Small business cyber security
→ Strategies to Mitigate Cyber Security Incidents

Maintaining devices and systems

→ Cloud security guidance
→ Critical infrastructure

Governance and user education

→ Governance
→ User education
→ Secure-by-Design

Assessment and evaluation programs

→ Australian Information Security Evaluation Program (AISEP)
→ Critical Infrastructure Uplift Program (CI-UP)
→ Emanation Security Program
→ High Assurance Evaluation Program
→ Infosec Registered Assessors Program (IRAP)

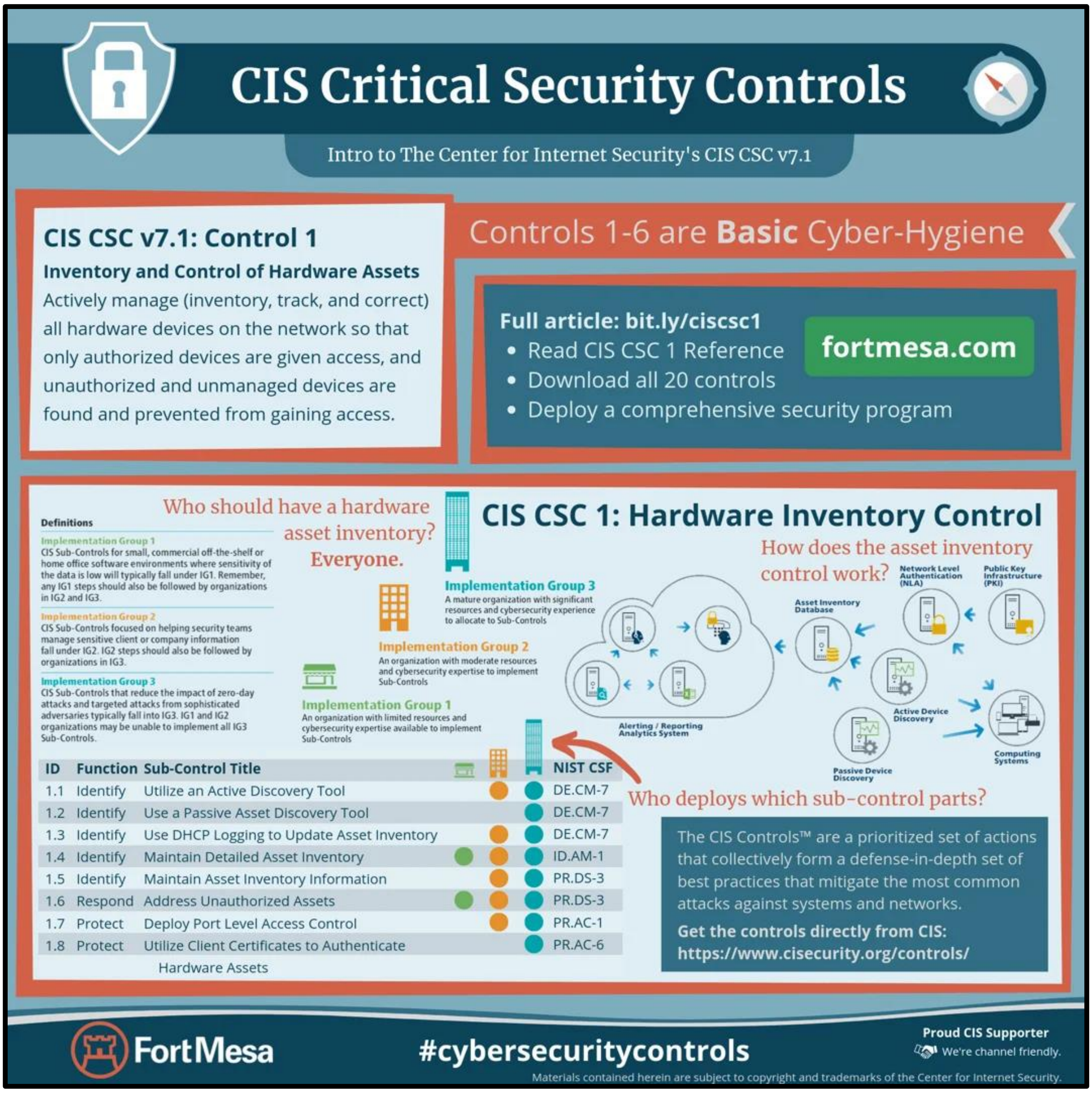
Figure 1: ACSC Business Resources (ACSC, 2023).

Within these categories, information such as mitigation strategies, governance, and the ‘Essential Eight’ are made available, however, there are no categories that exist to provide guidance to medium, small and micro-sized businesses individually. The small business option available is not specifically tailored to small businesses and has written its content for medium and small businesses combined. The lack of distinction between business sizes could easily confuse, overwhelm or even misinform a business operator.

The creation of a list of clear controls targeted to medium, small and micro-sized businesses as individual segments could help create more clarity for business owners. Tailoring each set of controls to align with the estimated capabilities and requirements of each business type will allow business owners to implement and design a more robust cyber security plan. With consideration given to the level of risk and associated impacts of a cyber-attack, the complexity and format of the controls have differed between each category. Medium-sized business controls will be process-driven and more complex. The small business section will provide more tailored, instructional information to operators on how to maintain their online security. Micro business controls will be more focussed on guidance and awareness, considering the increased usage of software as a service (SaaS), limited technical expertise and reliance on outside vendors and companies for business support. A suite of deliverables, including control tables, infographics and checklists, have been created to provide business owners with clear, concise information that is specific to the type of business they manage. While all the recommendations made may not be relevant to the exact specifications of every business, they act as guidance for operators as to the types of controls to consider based on business size.

The controls detailed in this project have been developed through a comparative analysis of the latest information included on the ACSC website against the recommendations of the Centre for Internet Security (CIS). The CIS Critical Security Controls are a set of 18 best practices used to strengthen a business’s security posture (CIS, 2023). This was chosen as a point of reference due to its global popularity and recognition as a source of best practices for businesses. The CIS controls are easy to understand and consider business size, resources and structure, as shown in their divisions of controls into implementation groups (See

Figure 2). The grouping depends on their risk profile and available resources. The structure of the controls in this manner has made it an ideal reference point.



CIS Critical Security Controls

Intro to The Center for Internet Security's CIS CSC v7.1

CIS CSC v7.1: Control 1

Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Controls 1-6 are **Basic** Cyber-Hygiene

Full article: bit.ly/ciscsc1

- Read CIS CSC 1 Reference
- Download all 20 controls
- Deploy a comprehensive security program

fortmesa.com

Definitions

Implementation Group 1
CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. Remember, any IG1 steps should also be followed by organizations in IG2 and IG3.

Implementation Group 2
CIS Sub-Controls focused on helping security teams manage sensitive client or company information fall under IG2. IG2 steps should also be followed by organizations in IG3.

Implementation Group 3
CIS Sub-Controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries typically fall into IG3. IG1 and IG2 organizations may be unable to implement all IG3 Sub-Controls.

Who should have a hardware asset inventory? Everyone.

CIS CSC 1: Hardware Inventory Control

Implementation Group 3
A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

Implementation Group 2
An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

Implementation Group 1
An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

How does the asset inventory control work?

Network Level Authentication (NLA)
Public Key Infrastructure (PKI)
Asset Inventory Database
Active Device Discovery
Computing Systems
Passive Device Discovery
Alerting / Reporting Analytics System

ID	Function	Sub-Control Title				NIST CSF
1.1	Identify	Utilize an Active Discovery Tool		●	●	DE.CM-7
1.2	Identify	Use a Passive Asset Discovery Tool			●	DE.CM-7
1.3	Identify	Use DHCP Logging to Update Asset Inventory		●	●	DE.CM-7
1.4	Identify	Maintain Detailed Asset Inventory	●	●	●	ID.AM-1
1.5	Identify	Maintain Asset Inventory Information		●	●	PR.DS-3
1.6	Respond	Address Unauthorized Assets	●	●	●	PR.DS-3
1.7	Protect	Deploy Port Level Access Control		●	●	PR.AC-1
1.8	Protect	Utilize Client Certificates to Authenticate Hardware Assets			●	PR.AC-6

Who deploys which sub-control parts?

The CIS Controls™ are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks.

Get the controls directly from CIS: https://www.cisecurity.org/controls/

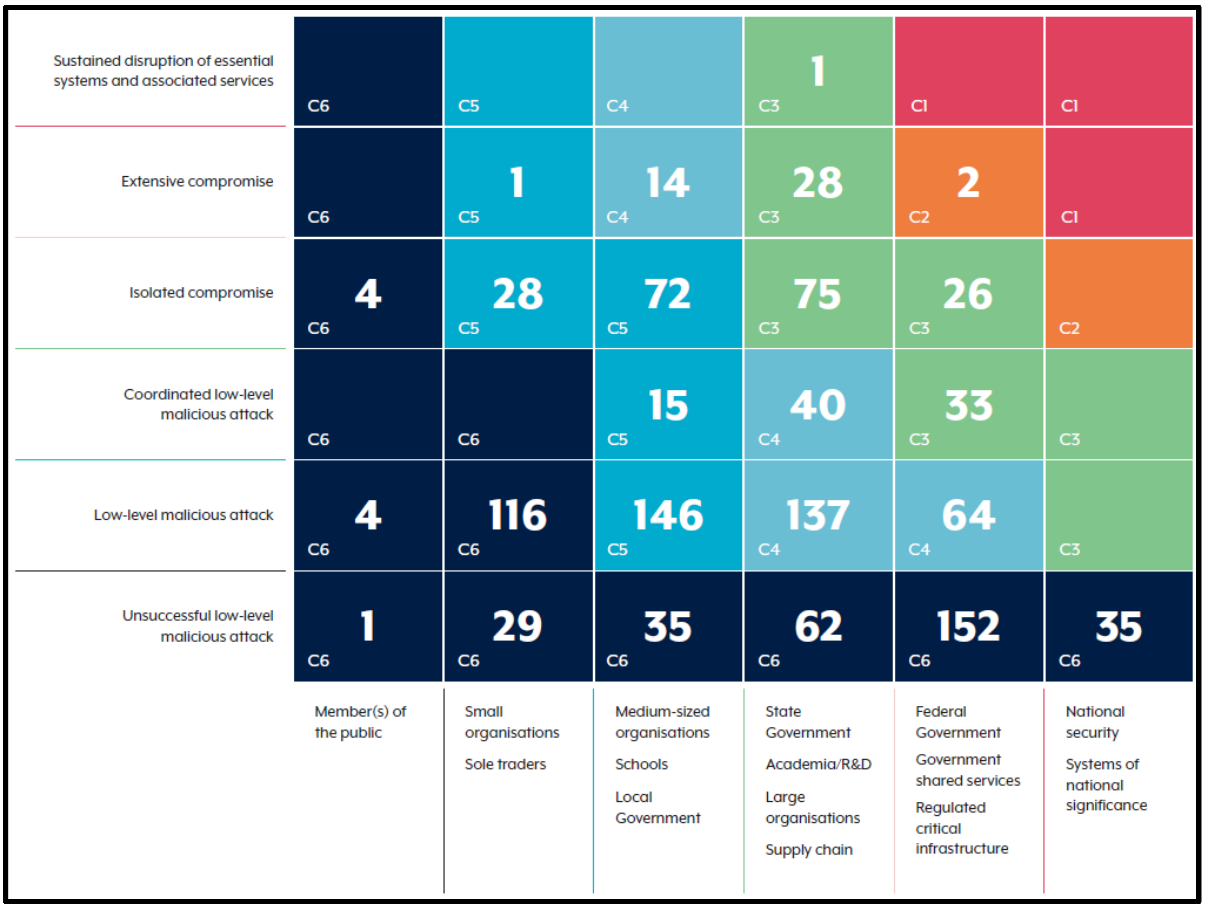
FortMesa #cybersecuritycontrols

Proud CIS Supporter
We're channel friendly.

Materials contained herein are subject to copyright and trademarks of the Center for Internet Security.

Figure 2. CIS Critical Security Control 1 (FortMesa, n.d.).

The ACSC website reports on cyber threats and incidents each financial year. In the 2021-2022 financial year, small and medium businesses were seen as prime targets for low-level malicious attacks (See Figure 3). Incidents were categorised from C1 (highest level of severity) to C6 (least severe). These figures reinforce the need for smaller businesses to ensure they have appropriate security controls in place.



Sustained disruption of essential systems and associated services	C6	C5	C4	1 C3	C1	C1
Extensive compromise	C6	1 C5	14 C4	28 C3	2 C2	C1
Isolated compromise	4 C6	28 C5	72 C5	75 C3	26 C3	C2
Coordinated low-level malicious attack	C6	C6	15 C5	40 C4	33 C3	C3
Low-level malicious attack	4 C6	116 C6	146 C5	137 C4	64 C4	C3
Unsuccessful low-level malicious attack	1 C6	29 C6	35 C6	62 C6	152 C6	35 C6
	Member(s) of the public	Small organisations Sole traders	Medium-sized organisations Schools Local Government	State Government Academia/R&D Large organisations Supply chain	Federal Government Government shared services Regulated critical infrastructure	National security Systems of national significance

Figure 3. Cyber Security incidents by incident category for financial year 2021-22 (ACSC, 2022).

Wider research on the current cyber trends affecting small and medium-sized businesses has also been considered. According to research by KPMG (2023), four cyber trends for small and medium businesses are increased digitisation and connection, evolving threat landscape, adhering to the regulatory environment, and increased business risks. These trends highlight the importance of monitoring the threat landscape as it applies to business owners. New trends potentially mean new opportunities for criminal behaviour and, therefore, reinforce the need to update, manage and/or reconsider current security controls within a business environment. An explanation of these trends and their significance is shown in the below table (Figure 4).

Current Cyber Trends	
Trend	Description
Increased digitisation and connection	Mid-Sized businesses are a ‘way-through’ to higher value targets.
Evolving threat landscape	Mid-Sized businesses are not prepared for emerging threats due to lack of internal resources
Adhering to regulatory environment	Current framework more focussed on larger organisation, so less applicable to SME’s
Increased business risks	Mid markets had the largest average financial loss per cybercrime committed

Figure 4. Current Cyber Trends (KPMG, 2023).

In sum, research on the ACSC website has led to the identification of the need for more business resources specifically designed for medium, small and micro-sized businesses. Through comparisons of the ACSC’s advice with the CIS critical security controls, alongside research of the latest cyber trends and challenges, a list of custom controls have been developed. Each business size is separated into its own section - ‘Medium’, ‘Small’ and ‘Micro’- and includes a clear definition of each business size as per the Australian government standards, with a brief summary of some of the cyber-related risks and challenges. An explanation of each control is offered, as well as possible risks that might result from neglecting the recommendations. The controls link to an appendix table and graphic for further clarification. The deliverables aim to support business owners with more relevant recommendations, supported by evidence, with clear explanations.

MEDIUM BUSINESS

Australian medium businesses are generally defined based on two main categories: their number of employees and annual turnover. According to the Australian Bureau of Statistics (ABS), medium businesses in Australia have a total number of employees between 20 and 199 (ABS, 2009). The Australian Taxation Office (ATO) (n.d.) defines medium businesses by their annual turnover, which is between 10 million and 250 million dollars. According to the Australian Government Treasury, 73% of medium enterprises conduct business online. The ACSC's annual cyber threat report in 2022 indicated that medium-sized businesses had the highest total monetary loss on average per cybercrime compared to their small and large counterparts (See Figure 5). Considering these factors, Australian medium sized businesses face significant challenges in keeping cybercrime under control whilst ensuring their day-to-day operations and sensitive customer data remain safe. While strengthening the security posture and reducing the attack surface should be a top priority, medium businesses must also adhere to legal and regulatory compliance challenges such as the Privacy Act and the Notifiable Data Breach Scheme. In addition, medium businesses operate in a complex network of vendors, suppliers, and third-party service providers, which makes supply chain attacks a potential Achilles heel and a significant risk that must be addressed and prioritised. The recommended controls for medium businesses are described below, along with a risk and impact statement. A table of controls suitable for medium-sized businesses is available for reference in Appendix 1, supported by a checklist for use by operators in Appendix 2.

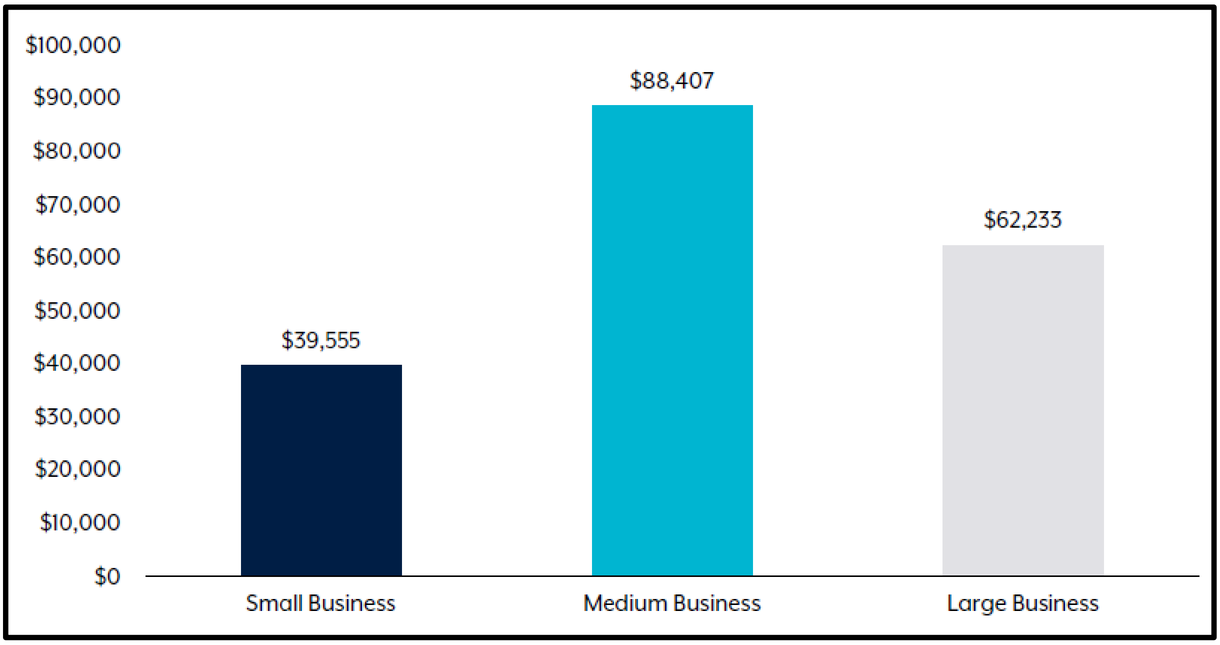


Figure 5. Cybercrime reports and average reported loss by organisation size for financial year 2021–22 (ACSC, 2022).

CONTROLS

1: Governance

1.1: Establish and Maintain Information Security Policies

Create information security policies that align with the business needs and focus to maintain standards and processes. These policies must include documents covering all of the controls in this framework. Regularly update and publish these policies and all updates to them for the company to review, acknowledge, and follow.

Possible Risk: If policies are neglected and not well maintained, there is a high risk in the event of an attack that business operators will be ill-prepared to manage the incident, affecting operations and increasing the chances of a more serious data breach.

Governance is a crucial component of this control strategy; it helps create and describe a framework of accountability and responsibility. Effective governance will identify which part of the business is responsible for each aspect of its cyber security, ensuring clarity for who and when should act in the event of a security incident. In addition, governance will ensure that the business cyber security strategy is compliant and compatible with the specific laws and regulations within its jurisdiction. The governance control is also responsible for formulating and maintaining comprehensive policies and processes that encompass the entirety of the control strategy. This approach ensures optimal implementation of each control, contributing to the safeguarding of the organisation’s assets and the reduction of its overall attack surface.

2: Inventory and Control of Technology Assets

2.1: Establish and Maintain Detailed Registers of Physical, Virtual, and Information Assets

A separate register should be created for physical, virtual, and information assets. These registers should be maintained upon every change with a checklist for the responsible person to follow. A clear and defined process should be created for maintaining these registers. Physical assets are server infrastructure and devices like laptops, phones, and hard drives owned and managed directly by the business. Virtual assets are infrastructure managed virtually through a third party, such as servers managed by a cloud computing platform. Information assets are your business data, including customer information, trade secrets, and other information held both locally, in the cloud, and with vendors.

Possible Risk: If assets are not tiered and protected as per their criticality, then in the event of an attack, there is greater risk to sensitive data and resources being compromised.

Detailed asset registers will enable medium businesses to manage asset access more efficiently, preventing unauthorised access and potential data breaches. Asset registers also enable improved physical security measures, such as securing network devices and servers where physical damage may lead to business interruptions. Additionally, asset mismanagement can be prevented or reduced by having a detailed asset register where outdated or unpatched software can be remedied and secured against exploitable vulnerabilities (D, 2021).

2.2: Establish and Maintain a Register of All Approved Vendors and Software

A register of all formally approved vendors, service providers, and software should be maintained. This allows employees to have a reference of the vendors, service providers, and software they are allowed to use without needing to proceed with an approval process. All vendors, service providers, and software in the register should be classified or tagged into clearly defined tiers based on the data the vendor receives from the business. For example, Tier 1 vendors may have access to confidential information, Tier 2 vendors may have access to internal information that is not confidential, and Tier 3 vendors may have access to public information.

Possible Risk: If a register of approved vendors is non-existent, then the business may be vulnerable to supply chain attacks and compromised software, leading to data breaches and operational disruptions.

Approved vendor and software registers will help reduce supply chain attacks where only trusted and pre-approved partners are used for procurement, and it will ensure that only vetted software is being used by the business. Furthermore, this will prevent any unauthorised software installation, which could expose the business to new vulnerabilities (Yan et al., 2021).

2.3: Establish and Maintain a Secure and Standardised Device Configuration Process

A device configuration process should be maintained for all physical assets, such as laptops. This process should include vital software such as anti-malware, device tracking, remote device wiping, email clients, and trusted browsers. If possible, a mobile device management (MDM) software should be used to standardise and automate this configuration along with updating the operating systems and software of all deployed devices.

Possible Risk: Unsecure devices can lead to illegitimate executables being run on business assets, resulting in serious data breaches as a result of unauthorised access to systems, compromising the privacy of both customers and employees.

Secure device configuration will ensure confidential data cannot be transferred from insider or outsider threats to external devices. It will only allow for trusted certificates and prevent the injection of illegitimate executables using malicious code (NSA, 2018). Furthermore, secure device configuration can be set to turn off unnecessary features that malware can exploit.

2.4: Enable and Maintain Anti-Malware Software Across All Devices

Anti-Malware software should be installed on all assets. This software should be maintained through regular updates. Utilising MDM software, these updates can be rolled out automatically to all deployed devices.

Possible Risk: If devices aren't protected by anti-malware software, there is increased vulnerability to attacks such as malware infections that may easily infiltrate the IT infrastructure, leading to service disruptions, data loss, and increased operational costs.

Anti-malware software will help detect and remove any malicious spyware that collects sensitive business information that can potentially cause data leaks. It also helps identify any illegitimate programs disguising themselves as legitimate and guard against any computer worms that can quickly replicate and spread across the network.

3. Networking

3.1: Establish and Maintain a Secure Network Infrastructure

Use current recommended best practices for ensuring the network infrastructure is secured with advanced standards. Ensuring a network intrusion detection solution is implemented. Network infrastructure includes any WiFi networks and intranets.

Possible Risk: An insecure network infrastructure increases the risk that an unauthorised user could execute a man-in-the-middle attack, resulting in compromised data integrity, confidentiality breaches, and privacy breaches.

Securing the network infrastructure is a critical security control for medium-sized businesses. The control involves setting up various security measures to mitigate against a wide range of threats. It includes implementing robust access control policies, the use of firewalls, intrusion detection systems and intrusion prevention systems. In addition, this control should specify processes for network segmentation and create user awareness against social engineering techniques to combat keylogging and spoofing attacks.

3.2: Apply Zero Trust Network Architecture Concepts

Apply a zero trust approach where every device and user must be continuously authorised and authenticated based on Identity and Access Management (IAM) principles. This includes the use of Virtual Private Networks (VPN), Anti-Malware software, and Firewalls to filter and scan all network traffic and protect against any bad actors.

Possible Risk: Failure to apply zero trust architecture concepts means that there are increased risks, such as network spoofing, leading to impersonation and unauthorised access, potentially causing data breaches and reputational damage.

This control ensures a proactive approach against the key risks identified. Zero trust operates on the principle of treating every device and service as hostile until it can be proven otherwise. Risks such as unauthorised access and man-in-the-middle attacks can be mitigated through zero trust; this includes continuous authentication and authorisation for every identity, location, and device (Microsoft, 2023). This control provides a holistic approach in combining multiple security controls, such as encryption and multi-factor authentication, from protecting endpoints to providing security across the entire network.

3.3: Network Device Hardening

Change default login credentials on all routers and switches. Regularly update network device firmware and install patches where applicable to mitigate risk.

Possible Risk: If the systems are targeted by brute force attacks and the network is not well secured, it may lead to unauthorised access, data exposure, and service disruptions.

Network device hardening will provide protection from various vulnerabilities and attacks, such as unauthorised access, firmware and software vulnerabilities and brute force attacks. This control ensures that network devices such as routers and switches are correctly configured, set up with strong passwords, and have their firmware and software regularly updated. In addition, brute force attacks can be mitigated by limiting login attempts within a specified timeframe.

4: Data Protection

4.1: Establish and Maintain a Data Management Process

Establish a process whereby data management is based on the C.I.A. Triad - Confidentiality, Integrity, Availability. This includes a data classification scheme, access controls, data retention, and encrypting data both in transit and at rest.

Possible Risk: If a data leak occurs and there are not processes in place that ensure minimal impact, sensitive information may be more freely exposed to unauthorised parties, resulting in reputational damage, legal consequences, and financial repercussions.

A robust data management process will help identify situations where data may be transmitted externally without prior authorisation and detect when data is being altered or manipulated. This process also ensures that medium businesses adhere to local and industry-specific data protection laws, avoiding unnecessary financial penalties.

4.2: Enable Email and Browser Protections

Standard email and browser protections should be enabled across the organisation. Utilising a reputable software as a service (SaaS) vendor who specialises in email can manage these protections and any vulnerabilities with greater resources at their disposal.

Possible Risk: A phishing attack is more likely to be successful when email and browser protections are not in place or poorly implemented, potentially exposing login credentials or session tokens, leading to data breaches, financial loss, and reputational damage.

Using a reputable software provider will ensure that email security measures such as spam filtering, malware detection, and Business Email Compromise (BEC) are applied (Garruba & Ghandi, 2023). Enabling browser protection will reduce malicious script injection and protect against various web application attacks through input validation and prepared statements.

5: Account and Access Management

5.1: Establish and Maintain a Register of Users and Accounts

Establish a register of users and accounts to ensure each user's access is noted and updated whenever necessary. This includes for internal role changes and resignations.

Possible Risk: If accounts aren’t maintained and ghost accounts exist within a system, it could lead to unauthorised access and misuse of resources, potentially resulting in data breaches and operational disruptions.

Account and access management will help identify active ex-employee accounts and prevent unauthorised access. Regular updates and reviews of user accounts also ensure that all active accounts are valid and are not subject to impersonation.

5.2: Enforce Access Controls

Limit access to systems and accounts based on the principle of a user's need to know. Utilise role-based access control wherever possible. When a user changes role internally, review their access as per the register and ensure they still need access to the systems they have access to.

Possible Risk: Without access controls in place, in the event of an attack privilege escalation may occur, which may lead to unauthorised access to sensitive resources and data, resulting in data breaches, operational disruptions, and legal consequences.

Account and access management will help identify and correct user access layers to prevent any threat action from gaining unauthorised access to systems or data. It can also prevent any leaked or compromised user credentials from one system from being used on another system within the network (Crowdstrike, 2022).

5.3: Enforce Security Standards for Passwords and Multi-Factor Authentication (MFA)

Wherever possible within systems, enforce minimum security standards for all passwords as well as MFA.

Possible Risk: Poor security standards leave systems more vulnerable to breaches such as pharming attacks that can compromise the system, leading to redirection of legitimate web traffic to malicious sites, resulting in data theft and reputational damage.

Setting MFA for medium business is a crucial control that prevents various attacks, such as brute force and pharming attacks where threat actors can redirect website traffic to a fake website to capture login credentials. MFA also provides a second layer of authentication for employees working remotely under the BYOD model.

6: Vulnerability and Patch Management

6.1: Establish and Maintain a Vulnerability and Patch Management Process

Utilise a vulnerability and patch management process when managing your own server(s) or system(s). This helps to ensure all steps are regularly taken to assess and mitigate risk caused by existing vulnerabilities.

Possible Risk: If processes for patching and vulnerability management are not followed, systems can be more readily exploited, resulting in unauthorised access, data breaches, and operational disruptions.

A vulnerability and patch management control process will protect against new vulnerabilities that can be exploited on the same day by updating systems with patches as soon as they are released (Sadowsky & Charrier, 2023). This control also ensures that software is always kept up to date, mainly when security updates no longer support previous versions.

6.2: Establish and Maintain a Penetration Testing Program

A penetration testing program should be used in conjunction with a vulnerability and patch management process. This ensures that vulnerabilities found from the penetration testing are resolved in a timely manner.

Possible Risk: Without penetration testing, configuration errors that may exist within the system can go unnoticed, leaving it vulnerable to attacks and consequently unauthorised access, data exposure, and service disruptions.

A Penetration testing program will help medium businesses identify misconfigured security controls for systems and networks, identify any vulnerabilities and ensure fixes are implemented.

7: Audit Log Management

7.1: Establish and Maintain an Audit Log Management Process

Use a standardised and automated audit log process across all systems where it is possible.

Possible Risk: If there is inadequate means for detection of suspicious activity, attacks such as Distributed Denial-of-Service (DDoS) attack can occur, leading to service disruptions and greater downtime, data unavailability, and financial losses.

Medium businesses must have an established audit log management system to detect and identify any unusual patterns or sudden changes in activity for data being accessed, change in location or device. Log management can also detect IDOR vulnerabilities where system identifiers are manipulated to gain unauthorised access (Tidmarsh, 2022).

7.2: Regularly Check, Maintain, and Investigate the Logs

The audit logs must be regularly checked for unusual behaviour, kept updated, and investigated wherever needed.

Possible Risk: If a reconnaissance attack is successful, then bad actors can identify system vulnerabilities and weaknesses, resulting in future cyberattacks as it is more likely to go unnoticed without proper log management.

Regular checks of logs will enable medium-sized businesses to identify any botnet activity when logs show simultaneous login attempts from different geolocations. It can also expose any preliminary or reconnaissance attacks through system event logs and network logs (Kent & Souppaya, 2006).

8: Security Awareness and Skills Training

8.1: Establish and Maintain a Security Awareness Program

Create and maintain a security awareness program including a security induction for all new employees. A record of all training and inductions should be kept on a training register.

Possible Risk: If an employee is uninformed and consequently provides a login to a bad actor through a phishing attack or otherwise, it may lead to accidental data exposure, operational disruptions, and security incidents.

An awareness training program is necessary for medium-sized businesses; cyber threat identification will help reduce human error and educate employees on cyber security best practices.

8.2: Enforce Annual Security Compliance Training

All employees must undertake annual security compliance training. All software engineers must undertake an annual secure code training. A record of all training should be kept on a training register.

Possible Risk: If the overall attack surface is not effectively managed and secured, then there is a higher likelihood of successful cyberattacks, resulting in data breaches and operational disruptions.

Compliance security training for all employees will ensure the latest information and training is provided, significantly improving the business's overall security posture.

9: Incident Response Management

9.1: Establish and Maintain a Security Incident Response Plan

Establish a clear and concise incident response plan that includes all key roles and responsibilities for undertaking the plan.

Possible Risk: If a security incident occurs and the business's response is inadequate, then further security incidents and reputational damage can occur.

An incident response plan must be developed to investigate, contain, remediate, recover, and communicate whenever a security incident or a data breach occurs.

9.2: Conduct Post-Incident Reviews

All relevant senior stakeholders and subject matter experts must conduct a post-incident review after every incident.

Possible Risk: If a weaker overall security infrastructure persists due to lack of insight, then the likelihood of more successful cyberattacks increases, leading to data breaches, service disruptions, financial and reputational damage, and legal liability.

If a security breach occurs, careful analysis and understanding of the breach must be undertaken to understand the full scope of the attack and create prevention measures against evolving and future attacks (Cybereason, 2023).

10. Business Resilience and Disaster Recovery

10.1: Establish and Maintain Automated Backups and a Data Recovery Process

Enable and maintain automated backups of all information assets on a regular schedule, such as weekly. These backups enable data recovery. Establish and maintain a data recovery process with clear guidance and order of procedure.

Possible Risk: If a key business system is disrupted, then operational interruptions across the business can occur, resulting in loss of trust and financial losses.

Setting up an automatic backup plan and a recovery process will mitigate the risk of data manipulation and losses. Data validation processes will continuously verify the integrity of both testing and production environments. Furthermore, this control will ensure that data can be efficiently restored during a data breach. Automatic processes of data storage facilities off-site or in the cloud can automatically restore critical infrastructure in the event of a cyber-attack, ensuring the business can swiftly continue operations with minimal disruptions.

10.2: Establish and Maintain a Business Impact Analysis and Business Continuity Process

Create a Business Impact Analysis that clearly defines potential disruptions to the business and the key roles filled by staff if they occur, and keep this analysis updated. Develop a Business Continuity Process to mitigate risks with all relevant stakeholders alert and informed, knowing their roles and responsibilities. This process must be maintained and updated with relevant staff information as necessary.

Possible Risk: If data integrity is compromised and no processes are in place, then service disruptions, financial losses, as well as legal and reputational damages can occur.

A business impact analysis and continuity process will help identify critical and time-sensitive business operations and evaluate the impact of interruptions and disruptions on these operations. This control will establish a set of operational guidelines in which the business can maintain profitability and critical operations in the event of a natural disaster or cyber incident.

10.3: Establish and Maintain a Continuous Improvement Process

Create and maintain a Continuous Improvement process for the implementation of the above Information Security controls. This process must include metrics for each control whereby the effectiveness of the control can be measured and evaluated against a standard. An example metric for control 2.3 may include determining if all login credentials on routers and switches have been changed from the default, and if the firmware of all network devices is up-to-date. Another example metric for control 7.1 may include checking if all employees are recorded as having completed their security induction on the training register.

Possible Risk: If security controls are not measured and assessed regularly, then the controls may be operating inefficiently and ineffectively, leading to an increased attack surface and security incidents.

A continuous improvement process will allow medium businesses to maintain an effective and up-to-date control strategy and provide a proactive and versatile security approach. This control includes targeted measuring and continuous monitoring of the control strategies by assessing the strengths and weaknesses of the control and making changes as necessary. Over time, this approach will yield incremental improvements that will improve the overall security posture of the business (Perara, 2021). Additionally, this control aims at ensuring that the security controls take into account the evolving nature of the threats and vulnerabilities in order to apply appropriate and realistic solutions to mitigate these threats.

SMALL BUSINESS

The ABS defines a small business as one that employs between five and nineteen employees, with an annual revenue turnover of under $10 million (Gilfillan, 2018). As of June 2017, over 4 million people were reported to be working in small businesses across Australia. According to the ACSC Annual Cyber Threat Report (2022), the average cost per cybercrime report for small businesses was $39,000, an increase of 14% from the previous year. This alarming statistic reinforces the need for small business owners and operators to remain vigilant in implementing controls to mitigate cyber security incidents caused by various cyber threats. The ACSC (2021) recommends small businesses strive to reach a target maturity level of one by implementing mitigation strategies outlined in the Essential Eight. The controls recommended for small businesses align with these recommendations, and extend upon them further with the intention of giving owners the opportunity to consider a more robust cyber security strategy. The controls are supported by the table shown in Appendix 3, along with a user-friendly checklist shown in Appendix 4.

CONTROLS

1: Inventory and Control of Technology Assets

1.1: Establish and Maintain a Record of Assets

A record of assets should be created for devices owned by the business, such as computers, phones, network routers, servers, etc. This record could be kept in the form of a spreadsheet or other table/database format, and should be kept up-to-date with every change using a checklist.

Possible Risk: If unauthorised access to an asset occurs, without an asset record, the broader business could be compromised, resulting in more widespread data leaks, malware, and loss of data integrity.

Maintaining a detailed list of company assets is vital for small businesses with limited IT expertise. This control is designed to identify who can access assets, preventing unauthorised access and data breaches. Having this list also ensures securing IT equipment to prevent physical damage, which could disrupt business operations.

Additionally, a well-maintained asset register helps in keeping software up to date, reducing the risk of vulnerabilities that could be exploited. This is especially important for small businesses, where IT resources are limited, and efficient asset management can make a significant difference.

1.2: Establish and Maintain a Record of Vendors and Software

A record of all vendors, service providers, and software used by the business should be maintained. This allows employees to have a reference of their contact details to assist with maintaining relationships and getting assistance when needed.

Possible Risk: If there are vulnerabilities within a piece of software, and support is slow to act, there is more risk of exploitations by attackers, leading to intellectual property leaks and confidentiality breaches.

Small businesses should create and maintain a comprehensive record of all vendors, service providers, and software utilised by the company. This record serves as a valuable resource for employees, offering easy access to contact information, which proves beneficial in the event of a supply chain cyber incident. In addition, this record will be used to ensure only authorised software is being used and that any new software the company will use will be vetted and verified in alignment with the business security practices.

1.3: Establish Device Setup and Maintenance Guides

Devices should be provided to all employees with all software and settings necessary for their role. Best practice instructions should be provided to all employees to follow to ensure their devices have vital software such as anti-malware, email clients, and trusted browsers enabled. Clear instructions should also be provided on how to update operating systems and other software.

Possible Risk: Vulnerable devices are more likely to be infected with malware, causing serious damage to systems and data integrity, resulting in bad actors holding systems to ransom and stealing confidential information.

Establishing a device setup guide is essential for small businesses. It prevents important data from being transferred by employees to external sources and only allows trusted software to run. This stops harmful programs from sneaking in and harming the business. In addition, this guide should provide information on how to turn off unnecessary features that hackers might use to attack the business's end devices.

2: Networking

2.1: Establish and Maintain a Secure Network

Create and use a guide on recommended best practices for configuring network devices. Use the guidance of a reputable vendor if assistance is required.

Possible Risk: If the network has been compromised by an attacker, then sensitive data could be intercepted or manipulated, leading to financial and reputational losses.

Securing the network is a critical step in keeping small business data secure. This control involves setting up essential security measures to protect against a range of threats. It includes creating rules for who can access the network, using firewalls to block malicious activities, and employing trusted vendor systems that can detect and prevent intruders. In addition, educating staff about common tricks used by cybercriminals is crucial to avoid keylogging and spoofing attacks. This comprehensive approach will help protect small businesses from a wide range of digital threats.

2.2: Utilise a Secure Network Architecture Standard

Give employees access to networks only if and when they need it. If an employee no longer needs access to a network, then remove them. Use a Virtual Private Networks (VPN) when accessing sensitive data remotely, and use Firewalls to filter all office network traffic and protect against any bad actors. Use a service provider to create this architecture if necessary.

Possible Risk: If a man-in-the-middle attack occurs, then bad actors may be able to intercept and manipulate communications, resulting in funds transfer fraud and identity theft, with a medium likelihood.

Using a Secure Network Architecture Standard will help small businesses mitigate various cybersecurity threats. This control sets up strong access controls and secure communication channels, which can prevent unauthorised access and man-in-the-middle attacks (Aslan et al., 2023). Additionally, a secure network architecture ensures that various threats like malware and keylogging attacks are detected.

2.3: Network Device Hardening

Change default login credentials on all routers and switches. Regularly update network device firmware and install patches where applicable to mitigate risk. Use a service provider to set up and maintain this standard if necessary.

Possible Risk: If device firmware does not have the latest security updates, then the devices could be exposed to malware, bootkits, or rootkits, leading to corporate espionage, file deletion and information theft.

A crucial aspect of security, network device hardening applies to the infrastructure of a network such as routers, switches, firewalls and servers. Small business operators should strive to keep these updated and enable settings such as encryption and access lists. This will decrease devices' attack surfaces, prevent unauthorised access, and ensure compliance standards are met.

3: Data Protection

3.1: Establish and Maintain a Data Management Plan

Keep a record of all staff and vendors who have access to sensitive data. Assess each new dataset for its level of sensitivity. Only use trusted and reputable vendors that utilise end-to-end encryption for transferring data.

Possible Risk: If a data leak occurs due to non-compliant, negligent behaviour by business operators, then there could be consequences such as significant fines, criminal liability, and reputational losses.

A data management plan will help small business owners ensure the security and integrity of company data. The document should outline how data is shared, stored and managed. This will protect against data loss since data is managed appropriately as well as ensure data validity as instructions in the plan are followed and adhered to.

3.2: Enable Email and Browser Protections

Utilise a reputable software as a service (SaaS) vendor who specialises in web browsers and email to manage these protections and any vulnerabilities with greater resources at their disposal.

Possible Risk: If a phishing attack occurs due to poor choice of vendor, then the result could include loss of data, financial losses, compromised data and credentials, and malware infection.

It is commonplace for attackers to try to attack a small business by targeting email and web browsers. Utilising email and DNS filtering services may help prevent employees from accessing malicious domains. Ensuring the business operates using a secure email client with secure configurations will maximise security protections.

4: Account and Access Management

4.1: Establish and Maintain a Record of Users and Accounts

Keep a record of all users and accounts to systems. Update the record any time a change occurs. This includes for internal role changes and resignations.

Possible Risk: If an account is exploited by an attacker, then they may be able to access sensitive company data and resources or launch a cyber attack, leading to data breaches and financial losses.

Small business owners should practise good record keeping to ensure the security and integrity of its data. Keeping up to date records of users and accounts will help when implementing access controls, so only the necessary users have access to confidential information. Small businesses thrive on efficiency, and record keeping streamlines management processes by offering greater insight into how resources are being used.

4.2: Enforce Access Controls

Only give employees access to systems if and when they need it. If an employee no longer needs access to a system, then remove them from it.

Possible Risk: If an account is compromised and credential stuffing occurs, then attackers could gain access to other accounts and websites using these credentials, resulting in data breaches and losses.

Configuring access controls includes setting up policies and procedures that define which users may access certain company resources. These can be based on job responsibilities and the data or resources users require to complete their tasks. By doing so, sensitive data is better protected as the risks of unauthorised access are lowered.

4.3: Enforce Security Standards for Passwords and Multi-Factor Authentication (MFA)

Wherever possible within systems, enforce minimum security standards for all passwords as well as MFA. Ensuring that passwords adhere to a minimum length, with uppercase, lowercase, numbers, and special characters.

Possible Risk: If a brute force attack is successful, then an attacker could access sensitive data and resources, or steal credentials to access other accounts and systems, leading to data leaks, ransomware and malware infections.

Instructing employees to adopt security standards such as setting strong passwords and enabling multi-factor authentication helps build a stronger security posture for the business. Implementation of effective security measures helps protect against cyber threats, preventing sensitive data and resource exposure.

5: Vulnerability and Patch Management

5.1: Resolve Vulnerabilities and Deploy Patches

Resolve vulnerabilities and deploy patches regularly when using self-managed server(s) or system(s).

Possible Risk: If a system is not patched in a timely manner, then it is more vulnerable to attacks, resulting in data breaches, compromised credentials, and malware or ransomware infections.

It is important for small business owners to monitor for vulnerabilities and apply patches when they become available. Patches are necessary to correct errors such as vulnerabilities or bugs in company software. Using vulnerability scanners in servers and systems helps owners to prioritise actions that need to be taken to protect the business and limit the attack surface.

5.2: Perform Penetration Testing on Systems

Utilise a reputable penetration testing vendor to test self-managed systems in conjunction with vulnerability fixes and patch deployment. Resolve vulnerabilities found through the penetration testing.

Possible Risk: If there is a configuration error, then systems and applications are more vulnerable to attacks, leading to malware and ransomware infections.

Penetration testing is becoming more common as a means for small businesses to anticipate attacks instead of waiting for them to occur. Using a reputable vendor, vulnerabilities may be uncovered that could have compromised the business had they been exploited. An analysis of security weaknesses through penetration testing is an opportunity for businesses to revise and adapt their current security controls to become more robust against threats.

6: Audit Log Management

6.1: Utilise Audit Log Software on Self-Managed Systems

Use a reputable and automated audit log vendor for logging all changes, actions, and access across all self-managed systems.

Possible Risk: If session hijacking occurs, then the attacker has the full access of the user whose session was hijacked, resulting in both monetary and identity theft, and compromised sensitive data.

A small business owner or operator should be cautious that incidents are being identified and swiftly acted upon. Utilising auditing software will provide insight into all events and actions that occur on a system, such as file access, login attempts and any other changes. This drives business efficiency by making security incident management much easier.

6.2: Set Up and Investigate Audit Log Alerts

Use software provided by the automated audit log vendor to create alerts for anything unusual. Investigate all audit log alerts produced.

Possible Risk: If a reconnaissance attack occurs, then a business is vulnerable to further exploitation, leading to a larger scale attack with more devastating consequences such as financial losses and damage to business reputation.

Tracking and monitoring user activity is an effective way to detect any suspicious behaviour. Using reputable software that can monitor actions such as login attempts, file access and system changes can enable operators to take action swiftly to prevent an attack.

7: Security Awareness and Skills Training

7.1: Establish Security Induction Training and a Security Awareness Channel

Use a reputable training vendor to produce security induction training that is tailored to the business for all staff to undertake. Create a channel in the business communication platform for advising on security and for staff to raise any questions or concerns.

Possible Risk: If an employee falls for a scam, then they may have unwittingly allowed an attacker access to their accounts, resulting in data breaches and compromised credentials.

Educating employees on the importance of implementing security protections can strengthen a business' security posture. This may be achieved by utilising a training vendor with relevant, up-to-date content that employees can readily understand and apply. Ongoing communications driving cyber awareness keeps employees informed and updated on any recent scams. An opportunity to ask questions and request information through a communication platform gives employees confidence in their ability to operate securely within a business.

7.2: Enforce Annual Security Compliance Training

Use the reputable training vendor who produced the security induction training to also create an annual security compliance training for all staff to undertake.

Possible Risk: If staff do not regularly undergo security compliance training, then they may be unaware of security risks, leading to data compromises and other mishaps.

It is important for employees to receive effective training to maintain a strong security posture. Annual security compliance training drives awareness of company security policies and procedures, with the expectation of compliance. Training typically covers password management, security awareness, data protection and incident reporting.

8: Incident Response Management

8.1: Establish and Maintain a Security Incident Response Plan

Create a clear and concise incident response plan that includes all key roles and responsibilities for undertaking the plan. This plan must include a checklist of all steps.

Possible Risk: If a security incident occurs and no plan is in place, then the business remains compromised for longer, resulting in greater impact on the business' operations, reputation and data.

In order to minimise damage caused by security incidents, including disruption to business operations, a security incident response plan is recommended. This is a comprehensive strategy that gives detailed instructions of what to do in the event of a breach or other security incident. It should contain details such as the roles and responsibilities of the incident responders, communication and reporting procedures, containment and eradication procedures, recovery procedures, and post-incident actions. Preparedness for an incident gives business owners confidence that they will be resilient in the event of an attack

8.2: Conduct Post-Incident Reviews

All relevant senior stakeholders and subject matter experts must conduct a post-incident review after every incident to review the cause, the remediation path, and any improvements that can be made to the incident response plan.

Possible Risk: If the attack surface remains weak, then a company is more susceptible to cyber incidents and data breaches, leading to more cyber attacks, including unauthorised access and data extraction.

A post-incident review will evaluate the effectiveness of the response to a security incident, and identify areas for improvement. It includes identifying the root cause of the attack, assessment of the damages, recommendations for improvement, and reassurance that the incident has been contained and the systems are no longer compromised. In doing so, the business reputation can be salvaged and operations can resume.

9: Business Resilience and Disaster Recovery

9.1: Establish and Maintain Backups and a Data Recovery Plan

Enable and maintain backups of all systems on a regular schedule, at least weekly. These backups enable data recovery. Establish and maintain a data recovery plan with the guidance of a reputable vendor who can be contacted if an event occurs.

Possible Risk: If business data is accessed by unauthorised users, then a ransomware attack could occur, resulting in financial loss for the business and disruption to operations.

A data recovery plan is a comprehensive set of instructions that an organisation should follow to recover from a data loss incident. This could be due to an attack, natural disaster or hardware failure. The plan outlines things such as roles and responsibilities of data recovery team members, communication procedures, data identification and assessments, recovery procedures, and post-recovery procedures. These can be managed by a reputable vendor. Backing up data protects against losses that could affect business continuity. If a business can recover from an incident with minimal downtime without compromising confidential information, customer trust can be maintained and operations can continue.

9.2: Create a Business Impact Analysis and Business Continuity Plan

Create a Business Impact Analysis that clearly defines potential disruptions to the business and the key roles filled by staff. Develop a Business Continuity Plan to mitigate risks with all relevant stakeholders alert and informed, knowing their roles and responsibilities.

Possible Risk: If a business has a large attack surface, then there are many possible points of entry available to exploit, leading to a greater chance of a significant attack occurring.

A business impact analysis (BIA) helps businesses prioritise critical business functions and assesses the potential impact of disruptions to them. They allow businesses to identify resources and develop strategies to maintain business continuity if an incident occurs. A business continuity plan (BCP) is a detailed strategy that instructs an organisation on the steps to take if an incident occurs, that will keep the business operational. It outlines the types of incidents that it can be used for with actions aligned to them that minimise loss of life, property and data.

9.3: Establish and Maintain a Continuous Improvement Plan

Create and maintain a Continuous Improvement plan for the implementation of the above Information Security controls. This plan must include regularly checking the instructions written by the business for any inefficiencies where the effectiveness of the control could be improved.

Possible Risk: If an unexpected attack occurs, then the time taken to respond is increased, resulting in loss of business and reputational damage.

A continuous improvement plan allows businesses to prepare for and improve its response to a range of attacks, thus minimising the potential negative impacts to the business. The plan identifies and prioritises critical business functions and makes an assessment of the impact of disruptions to them. Having an understanding of the latest threats to businesses gives owners an opportunity to adapt their security strategy in order to mitigate new risks.

MICRO BUSINESS

Micro businesses fall within the ABS's small business category but are those that only employ between one and four people, inclusive of non-employing businesses (Gilfillan, 2018). Annual turnover is generally less than $2 million. The complexity of the controls recommended for medium and small businesses does not align well with micro businesses. With limited budgets and often a lack of in-house technological expertise, micro business operators may struggle to understand and adopt the controls suggested for medium and small-sized businesses above. Creating a more streamlined list of controls makes implementation as simple and effective as possible. The recommended controls below focus on awareness and education, basic mitigation strategies, and guidance for support and help if necessary, without being overwhelming or too expensive. This information is supported by a table, as shown in Appendix 5, along with an easy to follow infographic, shown in Appendix 6.

CONTROLS

1: Control of Technology Assets

Possible Risk: If a disgruntled former employee accesses a business device or key software, then they could manipulate or export sensitive data, resulting in a loss of data integrity, breach of confidentiality, and reputational damage.

1.1: Establish and Maintain a List of Devices

Keep a list of devices owned by the business, such as computers, phones, network routers, etc. Keep this list up to date with every change.

Retaining an updated list of devices enables micro businesses to manage their assets with greater efficiency. This helps to ensure the right devices are deployed to new starters and that devices are returned by those leaving the business. By keeping the right devices only in the hands of trusted staff, micro businesses are mitigating the risk of unauthorised access to their systems and data (Kaspersky, n.d.).

1.2: Establish and Maintain a List of Vendors and Software Contacts

Keep a list of contacts for all vendors, service providers, and software used by the business for when you need any assistance. Utilise reputable and reliable software to limit the amount of assistance needed.

A list of contacts specific to vendors, service providers, and software ensures micro businesses always know who to contact when issues occur. Having a list of trusted contacts organised and ready is far more efficient than searching through emails or search engines to find the right person. This is of utmost importance for availability of the business and all those who may need access to the list should have this access granted and be made aware of it.

2: Networking

Possible Risk: If the network is attacked by a bad actor, then business availability may be reduced and data leaked, leading to reputational loss.

2.1: Engage a Secure Network Vendor

Utilise a trusted and reputable secure network vendor who can either set up your network for you based on the business needs or advise on how you should proceed. Keep a direct line of contact with the vendor so they are always available when you need assistance or to advise on ways to improve your network.

A business network, just like devices, can often be one of the first ports of attack. The security of the business network is key to both business availability and keeping data secure from bad actors. As such, an expert should advise on setup and maintenance of the network. An open and direct line of contact should be maintained with the aforementioned expert to ensure all issues and patches can be resolved in a timely manner.

3: Data Protection

Possible Risk: If an unauthorised user accesses sensitive data, then such data may be leaked or modified, resulting in compromised data integrity, a loss of trust and financial loss.

3.1: Ensure Only Trusted Access to Data

Ensure only trusted and reputable vendors have access to sensitive data. Only use vendors that utilise end-to-end encryption for transferring data. Keep a trusted contact for when or if you have any concerns around access and management of your data.

End-to-end encryption is one of the main ways to prevent data interception and other man-in-the-middle attacks. It is important to have this enabled with all vendors possible and have all staff using it. Using only trusted and reputable vendors helps to add to peace of mind and often enables a greater level of care and assistance for any concerns.

4: Account and Access Management

Possible Risk: If an employee is granted access to a system, they do not need access to, then they may view sensitive information they should not be privy to, leading to a confidentiality breach.

4.1: Employ the Principle of Least Privilege and Use Strong Authentication

Only give employees access to systems if and when they need it. Educate all employees on using strong passwords (minimum length, uppercase, lowercase, numbers, and special characters) as well as Multi-Factor Authentication (MFA) for all logins.

Utilising least privilege principles for systems access is a way to mitigate the risk of unauthorised access, especially by ex-employees. Passwords need to be strong as they are often the business’s first line of defence against attempts to gain unauthorised access. Adding MFA to any login significantly reduces the risk of unauthorised entry as a bad actor would also need access to the mobile device with the MFA code in order to be able to login. Combining these three key practices helps protect the confidentiality of all business's data.

5: Security Awareness and Skills Training

Possible Risk: If an employee is not security aware and makes an error such as opening a malicious hyperlink, then a bad actor could gain access to a system, resulting in a data breach, reputational damage and financial loss.

5.1: Engage a Security Training Vendor to Provide Advice and Training

Use a reputable training vendor to provide annual security training and advice on best practices that is tailored to the business. Keep a direct contact with the vendor to ensure you can always contact them for help or advice.

While human error is a common cause of cyber-attacks, staff can also be a business's strongest security asset. Security training and best practices provided to employees helps to grow their knowledge and begin taking steps to reduce risk.

6: Incident Response Management

Possible Risk: If the business does not know who to contact in the event of a security incident, then the attacker has more time to harm the business further, leading to a larger data breach or greater impact to system availability.

6.1: Establish and Maintain a List of Security Incident Response Contacts

Create a clear and concise list of important contacts to engage if a security incident occurs. These contacts will be the team to guide you through your response.

A list of key contacts for security incident response ensures that micro businesses always know who to contact if a serious issue was to occur. Having a list of trusted contacts who can guide you through the correct process and response for any kind of attack is vital. This is of utmost importance for reducing the overall attack surface of the business and mitigating the damage caused by any attack.

7: Business Resilience and Disaster Recovery

Possible Risk: If a system is taken down by an attack, then at least some parts of the business will be unable to operate until that system is running again, resulting in reputational and financial loss.

7.1: Automate Backups and Maintain a Support Contact List

Use automated cloud backup of key data. These backups enable data recovery. Keep a list of support contacts who can assist with recovery of data and systems.

Automated backups of key data enable businesses to recover their systems faster ensuring minimal business downtime. By using a cloud service provider to store this backup, there is a greater chance of it surviving an incident as the data is not held on any devices owned by the business. It also allows the business to access the data from anywhere when it is needed. The list of support contacts is important to guide the employees through the process of recovering data and systems from backups and mitigating risk along the way. This helps to ensure maximum business availability after a security incident.

REFERENCES

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics, 12*(6), 1333. https://doi.org/10.3390/electronics12061333

Australian Bureau of Statistics (ABS). (2009). *1321.0 - Small Business in Australia, 2001*. https://www.abs.gov.au/ausstats/abs@.nsf/mf/1321.0

Australian Cyber Security Centre (ACSC). (2021). *Essential Eight Maturity Model FAQ*. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model-faq

Australian Cyber Security Centre (ACSC). (2022). *Annual Cyber Threat Report*. https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf

Australian Taxation Office (ATO). (n.d.). *Medium business income tax gap*. Retrieved September 27, 2023, from https://www.ato.gov.au/About-ATO/Research-and-statistics/In-detail/Tax-gap/Medium-business-income-tax-gap/?page=2

Center for Internet Security (CIS). (2023). *CIS Critical Security Controls*. https://www.cisecurity.org/controls

Crowdstrike. (2022). *What is Privilege Escalation?* https://www.crowdstrike.com/cybersecurity-101/privilege-escalation/

Cybereason. (2023). *A Guide to Post-Incident Review*. https://www.cybereason.com/resources/post-incident-review

D, T. (2021). *Asset management for cyber security*. National Cyber Security Centre. https://www.ncsc.gov.uk/blog-post/asset-management-for-cyber-security

FortMesa. (n.d.). *CIS Critical Security Control 1*. https://land.fortmesa.com/cis-csc-1

Garruba, G., & Ghandi, U. (2023). *Business Email: Uncompromised - Part Three*. Microsoft Defender for Office 365 Blog. https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/business-email-uncompromised-part-three/ba-p/2247693

Gilfillan, G. (2018). *Small business sector contribution to the Australian economy*. Parliament of Australia. https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1819/SmallBusinessSector

Gill, R., Smith, J., Looi, M., Clark, A. (2005). *Passive techniques for detecting session hijacking attacks in IEEE 802.11 wireless networks*. ResearchGate. https://www.researchgate.net/publication/27478338_Passive_techniques_for_detecting_session_hijacking_attacks_in_IEEE_80211_wireless_networks

Kaspersky. (n.d.). *How Data Breaches Happen*. https://www.kaspersky.com/resource-center/definitions/data-breach

Kent, K., & Souppaya, M. (2006). *Guide to Computer Security Log Management* (Special Publication 800-92). National Institute of Standards and Technology (NIST). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

KPMG. (2023). *Four Must Know Cyber Trends for the Mid Market*. https://kpmg.com/au/en/home/insights/2023/04/four-must-know-cyber-trends-midmarket.html

Lanfear, T. (2023). *Azure backup and restore plan to protect against ransomware*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware

Microsoft. (2023). *What Is Zero Trust Architecture?* Microsoft Security. https://www.microsoft.com/en-au/security/business/security-101/what-is-zero-trust-architecture

National Security Agency (NSA). (2018). *NSA'S Top Ten Cybersecurity Mitigation Strategies*. https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf

Perara, A. (2021). *Business Impact Analysis (BIA): Understanding the purpose of Business Impact Analysis*. BusinessTechWeekly.com. https://www.businesstechweekly.com/operational-efficiency/business-continuity/business-impact-analysis-bia/

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensors, 23*(8), 4060. https://doi.org/10.3390/s23084060

Sadowski, J., & Charrier, C. (2023). *Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace*. Mandiant. https://www.mandiant.com/resources/blog/zero-days-exploited-2022

Tidmarsh, D. (2022). *Insecure Direct Object Reference (IDOR) Vulnerability Detection and Prevention*. EC-Council. https://www.eccouncil.org/cybersecurity-exchange/web-application-hacking/idor-vulnerability-detection-prevention/

Yan, D., Niu, Y., Liu, K., Liu, Z., Liu, Z., & Bissyande, T. F. (2021). Estimating the Attack Surface from Residual Vulnerabilities in Open Source Software Supply Chain. *2021 IEEE 21st International Conference on Software Quality, Reliability and Security (QRS)*, 493-502. https://doi.org/10.1109/qrs54544.2021.00060

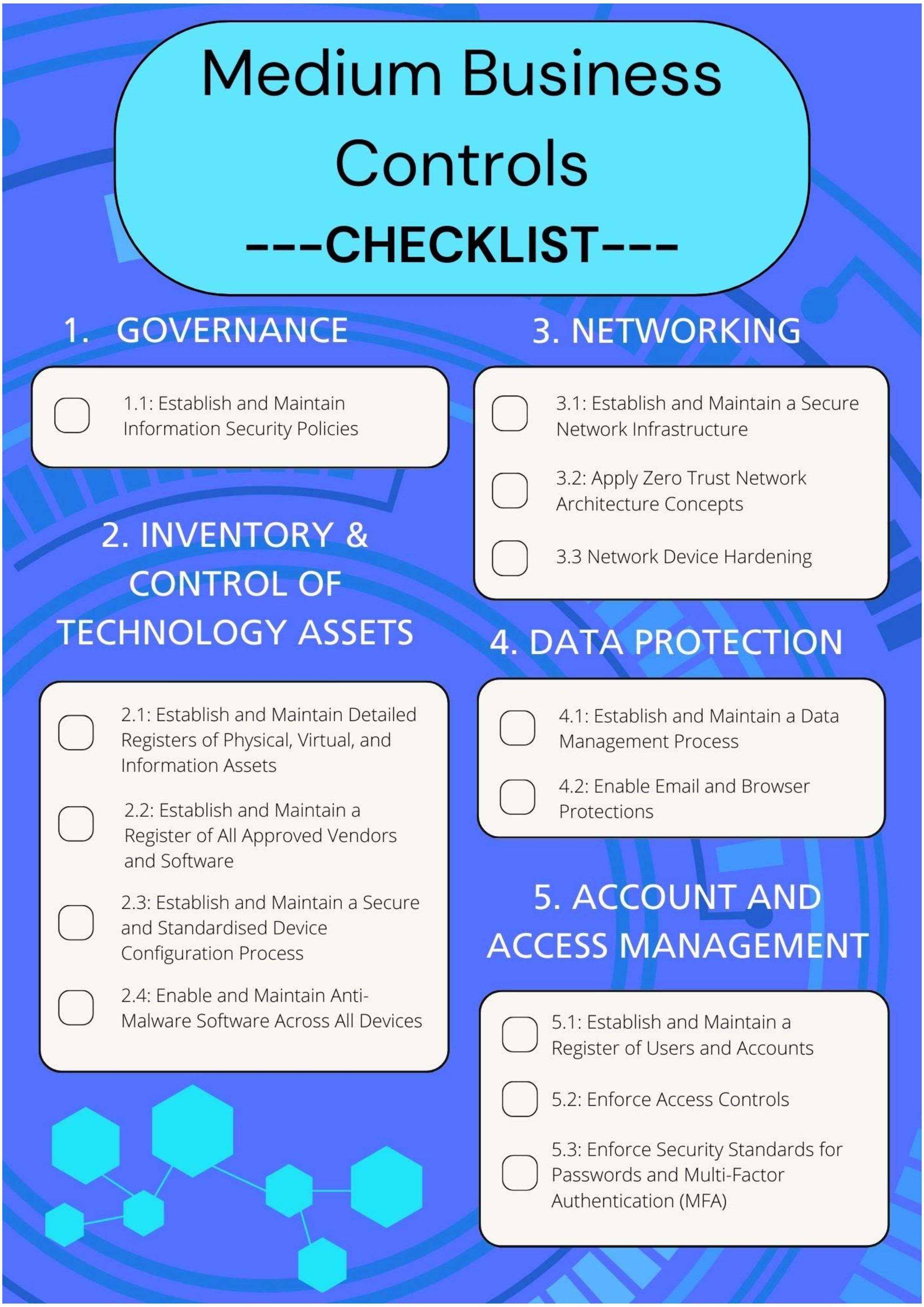
Appendix 1: Medium Business Controls

CONTROLS	*DESCRIPTION*
1: Governance	**Risks:** Non-compliance, incorrect processes, and increased attack surface.
1.1: Establish and Maintain Information Security Policies	Create Information Security Policies that align with the business needs and focus to maintain standards and processes. These policies must include documents covering all of the controls in this framework. Regularly update and publish these policies and all updates to them for the company to review, acknowledge, and follow.
2: Inventory and Control of Technology Assets	**Risks:** Unauthorised access, physical damage, asset mismanagement, supply chain attacks, software vulnerabilities, unauthorised software installation, data exfiltration, and malware infections.
2.1: Establish and Maintain Detailed Registers of Physical, Virtual, and Information Assets	A separate register should be created for Physical, Virtual, and Information Assets. These registers should be maintained upon every change with a checklist for the responsible person to follow. A clear and defined process should be created for maintaining these registers. Physical Assets are server infrastructure and devices like laptops, phones, and hard drives owned and managed directly by the business. Virtual Assets are infrastructure managed virtually through a third party, such as servers managed by a cloud computing platform. Information Assets are your business data, including customer information, trade secrets, and other information held both locally, in the cloud, and with vendors.
2.2: Establish and Maintain a Register of All Approved Vendors and Software	A register of all formally approved vendors, service providers, and software should be maintained. This allows employees to have a reference of the vendors, service providers, and software they are allowed to use without needing to proceed with an approval process. All vendors, service providers, and software in the register should be classified or tagged into clearly defined tiers based on the data the vendor receives from the business. For example, Tier 1 vendors may have access to confidential information, Tier 2 vendors may have access to internal information that is not confidential, and Tier 3 vendors may have access to public information.
2.3: Establish and Maintain a Secure and Standardised Device Configuration Process	A device configuration process should be maintained for all physical assets, such as laptops. This process should include vital software such as anti-malware, device tracking, remote device wiping, email clients, and trusted browsers. If possible, a mobile device management (MDM) software should be used to standardise and automate this configuration along with updating the operating systems and software of all deployed devices.
2.4: Enable and Maintain Anti-Malware Software Across All Devices	Anti-Malware software should be installed on all physical assets. This software should be maintained through regular updates. Utilising MDM software, these updates can be rolled out automatically to all deployed devices.
3: Networking	**Risks:** Unauthorised access, man-in-the-middle attacks, malware, firmware and software vulnerabilities, keylogging attacks, brute force attacks, and spoofing.
3.1: Establish and Maintain a Secure Network Infrastructure	Use current recommended best practices for ensuring the network infrastructure is secured with advanced standards. Ensuring a network intrusion detection solution is implemented. Network infrastructure includes any WiFi networks and intranets.

3.2: Apply Zero Trust Network Architecture Concepts	Apply a zero-trust approach where every device and user must be continuously authorised and authenticated based on Identity and Access Management (IAM) principles. This includes the use of Virtual Private Networks (VPN), Anti-Malware software, and Firewalls to filter and scan all network traffic and protect against any bad actors.
3.3: Network Device Hardening	Change default login credentials on all routers and switches. Regularly update network device firmware and install patches where applicable to mitigate risk.
4: Data Protection	**Risks:** Data leaks, unauthorised data access, data manipulation, non-compliance with data protection laws, phishing attacks, SQL injection, and cross-site scripting (XSS).
4.1: Establish and Maintain a Data Management Process	Establish a process whereby data management is based on the C.I.A. Triad - Confidentiality, Integrity, Availability. This includes a data classification scheme, access controls, data retention, and encrypting data both in transit and at rest.
4.2: Enable Email and Browser Protections	Standard email and browser protections should be enabled across the organisation. Utilising a reputable software as a service (SaaS) vendor who specialises in email can manage these protections and any vulnerabilities with greater resources at their disposal.
5: Account and Access Management	**Risks:** Ghost accounts, spoofing, privilege escalation, credential stuffing, brute force attacks, remote work vulnerabilities, pharming, and keylogging attacks.
5.1: Establish and Maintain a Register of Users and Accounts	Establish a register of users and accounts to ensure each user's access is noted and updated whenever necessary. This includes for internal role changes and resignations.
5.2: Enforce Access Controls	Limit access to systems and accounts based on the principle of a user's need to know. Utilise role-based access control wherever possible. When a user changes role internally, review their access as per the register and ensure they still need access to the systems they have access to.
5.3: Enforce Security Standards for Passwords and Multi-Factor Authentication (MFA)	Wherever possible within systems, enforce minimum security standards for all passwords as well as MFA.
6: Vulnerability and Patch Management	**Risks:** Zero-day vulnerabilities, unpatched software exploits, configuration errors, and unauthorised access.
6.1: Establish and Maintain a Vulnerability and Patch Management Process	Utilise a vulnerability and patch management process when managing your own server(s) or system(s). This helps to ensure all steps are regularly taken to assess and mitigate risk caused by existing vulnerabilities.
6.2: Establish and Maintain a Penetration Testing Program	A penetration testing program should be used in conjunction with a vulnerability and patch management process. This ensures that vulnerabilities found from the penetration testing are resolved in a timely manner.
7: Audit Log Management	**Risks:** Distributed Denial-of-Service attacks (DDoS), session hijacking, Insecure Direct Object Reference (IDOR), botnets, and reconnaissance attacks.
7.1: Establish and Maintain an Audit Log Management Process	Use a standardised and automated audit log process across all systems where it is possible.
7.2: Regularly Check, Maintain, and Investigate the Logs	The audit logs must be regularly checked for unusual behaviour, kept updated, and investigated wherever needed.

8: Security Awareness and Skills Training	**Risks:** Human error, drive-by downloads, whaling attacks, overall attack surface, and many more.
8.1: Establish and Maintain a Security Awareness Program	Create and maintain a security awareness program including a security induction for all new employees. A record of all training and inductions should be kept on a training register.
8.2: Enforce Annual Security Compliance Training	All employees must undertake annual security compliance training. All software engineers must undertake an annual secure code training. A record of all training should be kept on a training register.
9: Incident Response Management	**Risks:** Weaker overall security infrastructure, overall attack surface, and all previously identified risks.
9.1: Establish and Maintain a Security Incident Response Plan	Establish a clear and concise incident response plan that includes all key roles and responsibilities for undertaking the plan.
9.2: Conduct Post-Incident Reviews	All relevant senior stakeholders and subject matter experts must conduct a post-incident review after every incident.
10: Business Resilience and Disaster Recovery	**Risks:** Data integrity, business availability, confidentiality, overall attack surface, and all previously identified risks.
10.1: Establish and Maintain Automated Backups and a Data Recovery Process	Enable and maintain automated backups of all information assets on a regular schedule, such as weekly. These backups enable data recovery. Establish and maintain a data recovery process with clear guidance and order of procedure.
10.2: Establish and Maintain a Business Impact Analysis and Business Continuity Process	Create a Business Impact Analysis that clearly defines potential disruptions to the business and the key roles filled by staff if they occur, and keep this analysis updated. Develop a Business Continuity Process to mitigate risks with all relevant stakeholders' alert and informed, knowing their roles and responsibilities. This process must be maintained and updated with relevant staff information as necessary.
10.3: Establish and Maintain a Continuous Improvement Process	Create and maintain a Continuous Improvement process for the implementation of the above Information Security controls. This process must include metrics for each control whereby the effectiveness of the control can be measured and evaluated against a standard. An example metric for control 2.3 may include determining if all login credentials on routers and switches have been changed from the default, and if the firmware of all network devices is up to date. Another example metric for control 7.1 may include checking if all employees are recorded as having completed their security induction on the training register.

Appendix 2: Medium Business Checklist



Medium Business Controls

---CHECKLIST---

1. GOVERNANCE

- □ 1.1: Establish and Maintain Information Security Policies

2. INVENTORY & CONTROL OF TECHNOLOGY ASSETS

- □ 2.1: Establish and Maintain Detailed Registers of Physical, Virtual, and Information Assets
- □ 2.2: Establish and Maintain a Register of All Approved Vendors and Software
- □ 2.3: Establish and Maintain a Secure and Standardised Device Configuration Process
- □ 2.4: Enable and Maintain Anti-Malware Software Across All Devices

3. NETWORKING

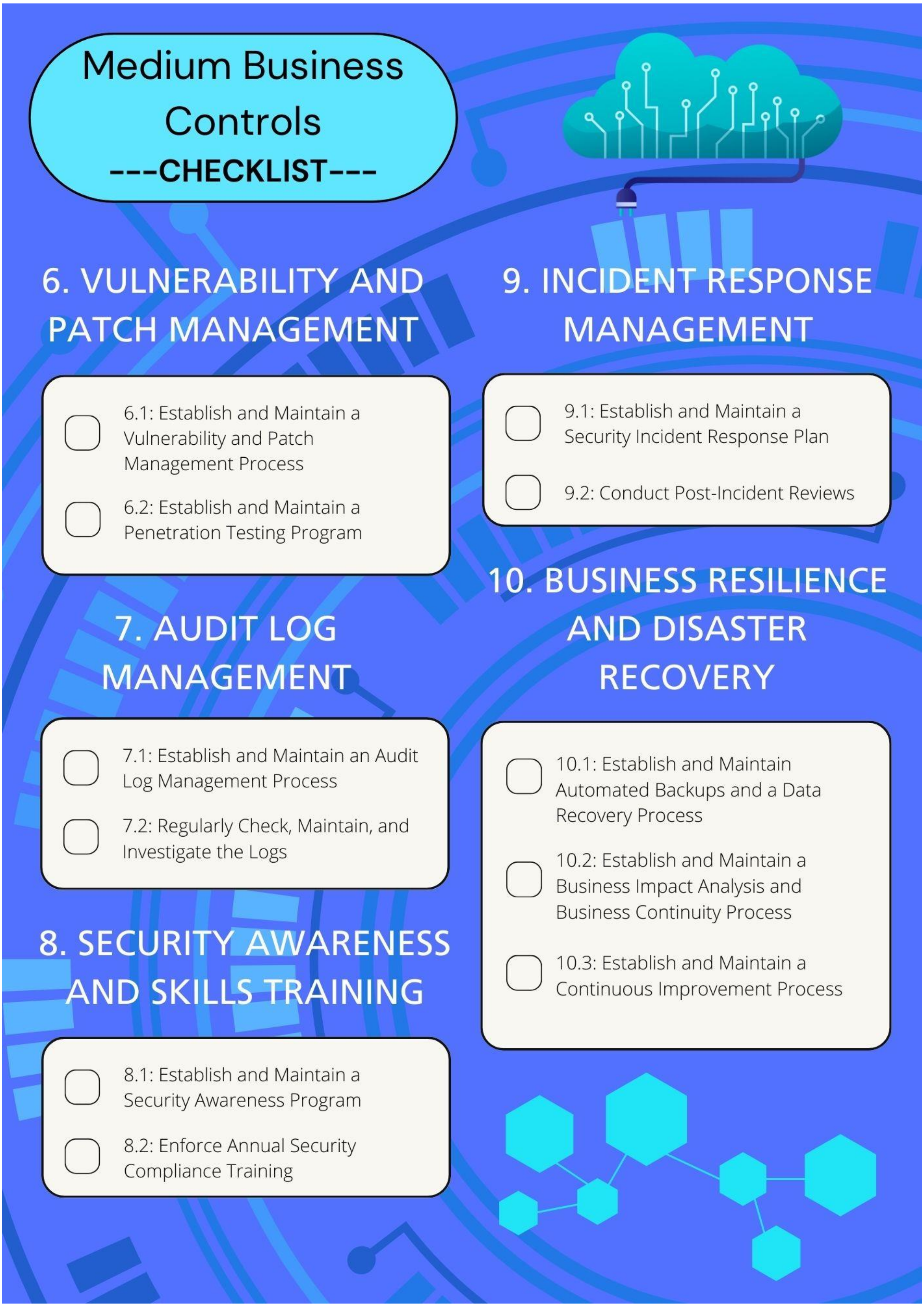
- □ 3.1: Establish and Maintain a Secure Network Infrastructure
- □ 3.2: Apply Zero Trust Network Architecture Concepts
- □ 3.3 Network Device Hardening

4. DATA PROTECTION

- □ 4.1: Establish and Maintain a Data Management Process
- □ 4.2: Enable Email and Browser Protections

5. ACCOUNT AND ACCESS MANAGEMENT

- □ 5.1: Establish and Maintain a Register of Users and Accounts
- □ 5.2: Enforce Access Controls
- □ 5.3: Enforce Security Standards for Passwords and Multi-Factor Authentication (MFA)



Medium Business Controls

---CHECKLIST---

6. VULNERABILITY AND PATCH MANAGEMENT

- □ 6.1: Establish and Maintain a Vulnerability and Patch Management Process
- □ 6.2: Establish and Maintain a Penetration Testing Program

7. AUDIT LOG MANAGEMENT

- □ 7.1: Establish and Maintain an Audit Log Management Process
- □ 7.2: Regularly Check, Maintain, and Investigate the Logs

8. SECURITY AWARENESS AND SKILLS TRAINING

- □ 8.1: Establish and Maintain a Security Awareness Program
- □ 8.2: Enforce Annual Security Compliance Training

9. INCIDENT RESPONSE MANAGEMENT

- □ 9.1: Establish and Maintain a Security Incident Response Plan
- □ 9.2: Conduct Post-Incident Reviews

10. BUSINESS RESILIENCE AND DISASTER RECOVERY

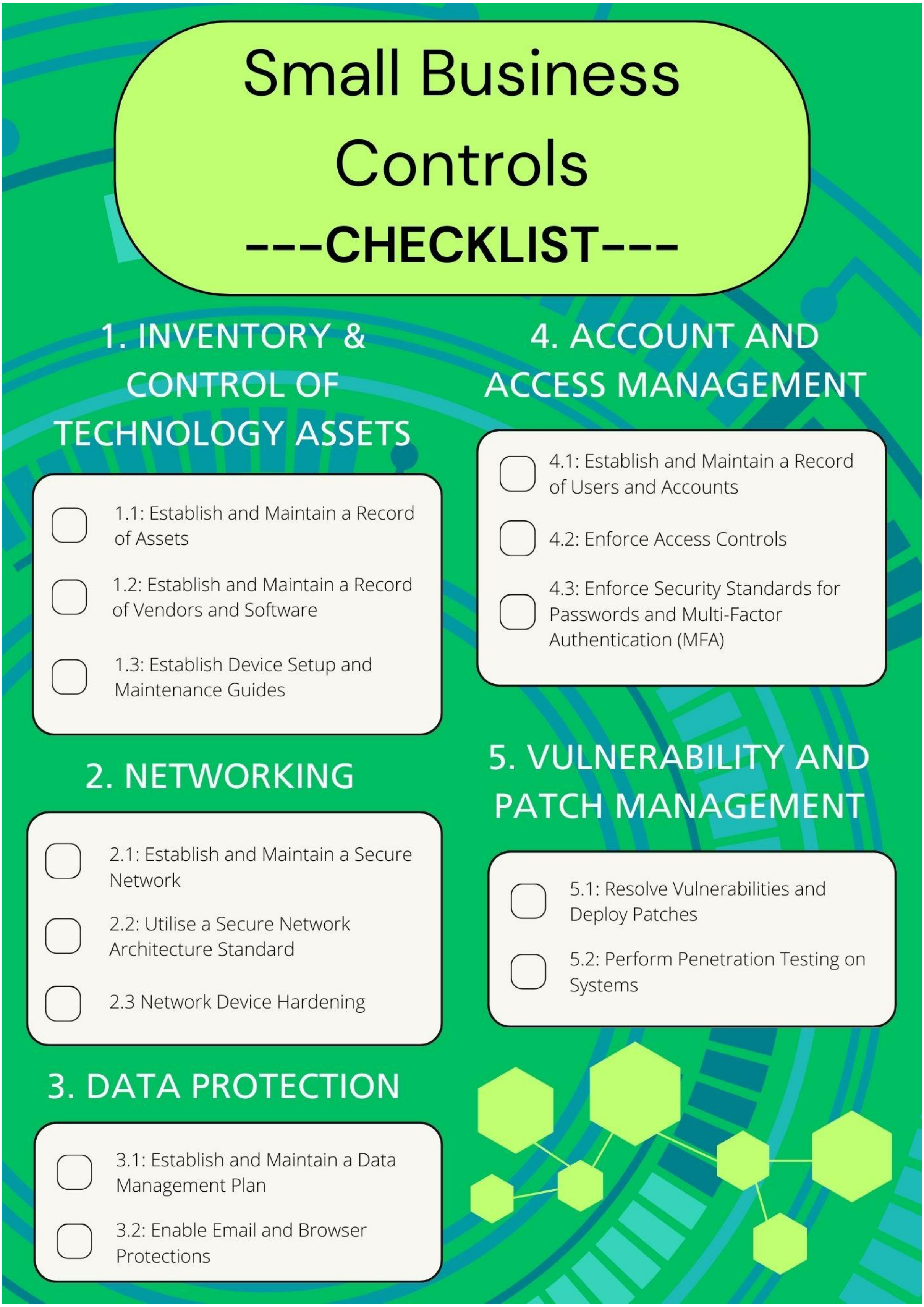
- □ 10.1: Establish and Maintain Automated Backups and a Data Recovery Process
- □ 10.2: Establish and Maintain a Business Impact Analysis and Business Continuity Process
- □ 10.3: Establish and Maintain a Continuous Improvement Process

Appendix 3: Small Business Controls

CONTROLS	*DESCRIPTION*
1: Inventory and Control of Technology Assets	**Risks:** Unauthorised access, physical damage, asset mismanagement, supply chain attacks, software vulnerabilities, unauthorised software installation, data exfiltration, and malware infections.
1.1: Establish and Maintain a Record of Assets	A record of assets should be created for devices owned by the business, such as computers, phones, network routers, servers, etc. This record could be kept in the form of a spreadsheet or other table/database format, and should be kept up-to-date with every change using a checklist.
1.2: Establish and Maintain a Record of Vendors and Software	A record of all vendors, service providers, and software used by the business should be maintained. This allows employees to have a reference of their contact details to assist with maintaining relationships and getting assistance when needed.
1.3: Establish Device Setup and Maintenance Guides	Devices should be provided to all employees with all software and settings necessary for their role. Best practice instructions should be provided to all employees to follow to ensure their devices have vital software such as anti-malware, email clients, and trusted browsers enabled. Clear instructions should also be provided on how to update operating systems and other software.
2: Networking	**Risks:** Unauthorised access, man-in-the-middle attacks, malware, firmware and software vulnerabilities, keylogging attacks, brute force attacks, and spoofing.
2.1: Establish and Maintain a Secure Network	Create and use a guide on recommended best practices for configuring network devices. Use the guidance of a reputable vendor if assistance is required.
2.2: Utilise a Secure Network Architecture Standard	Give employees access to networks only if and when they need it. If an employee no longer needs access to a network, then remove them. Use a Virtual Private Networks (VPN) when accessing sensitive data remotely, and use Firewalls to filter all office network traffic and protect against any bad actors. Use a service provider to create this architecture if necessary.
2.3: Network Device Hardening	Change default login credentials on all routers and switches. Regularly update network device firmware and install patches where applicable to mitigate risk. Use a service provider to set up and maintain this standard if necessary.
3: Data Protection	**Risks:** Data leaks, unauthorised data access, data manipulation, non-compliance with data protection laws, phishing attacks, SQL injection, and cross-site scripting (XSS).
3.1: Establish and Maintain a Data Management Plan	Keep a record of all staff and vendors who have access to sensitive data. Assess each new dataset for its level of sensitivity. Only use trusted and reputable vendors that utilise end-to-end encryption for transferring data.
3.2: Enable Email and Browser Protections	Utilise a reputable software as a service (SaaS) vendor who specialises in web browsers and email to manage these protections and any vulnerabilities with greater resources at their disposal.
4: Account and Access Management	**Risks:** Ghost accounts, spoofing, privilege escalation, credential stuffing, brute force attacks, remote work vulnerabilities, pharming, and keylogging attacks.
4.1: Establish and Maintain a Record of Users and Accounts	Keep a record of all users and accounts to systems. Update the record any time a change occurs. This includes for internal role changes and resignations.
4.2: Enforce Access Controls	Only give employees access to systems if and when they need it. If an employee no longer needs access to a system, then remove them from it.

4.3: Enforce Security Standards for Passwords and Multi-Factor Authentication (MFA)	Wherever possible within systems, enforce minimum security standards for all passwords as well as MFA. Ensuring that passwords adhere to a minimum length, with uppercase, lowercase, numbers, and special characters.
5: Vulnerability and Patch Management	**Risks:** Zero-day vulnerabilities, unpatched software exploits, configuration errors, and unauthorised access.
5.1: Resolve Vulnerabilities and Deploy Patches	Resolve vulnerabilities and deploy patches regularly when using self-managed server(s) or system(s).
5.2: Perform Penetration Testing on Systems	Utilise a reputable penetration testing vendor to test self-managed systems in conjunction with vulnerability fixes and patch deployment. Resolve vulnerabilities found through the penetration testing.
6: Audit Log Management	**Risks:** Distributed Denial-of-Service attacks (DDoS), session hijacking, Insecure Direct Object Reference (IDOR), botnets, and reconnaissance attacks.
6.1: Utilise Audit Log Software on Self-Managed Systems	Use a reputable and automated audit log vendor for logging all changes, actions, and access across all self-managed systems.
6.2: Set Up and Investigate Audit Log Alerts	Use software provided by the automated audit log vendor to create alerts for anything unusual. Investigate all audit log alerts produced.
7: Security Awareness and Skills Training	**Risks:** Human error, drive-by downloads, whaling attacks, overall attack surface, and many more.
7.1: Establish Security Induction Training and a Security Awareness Channel	Use a reputable training vendor to produce security induction training that is tailored to the business for all staff to undertake. Create a channel in the business communication platform for advising on security and for staff to raise any questions or concerns.
7.2: Enforce Annual Security Compliance Training	Use the reputable training vendor who produced the security induction training to also create an annual security compliance training for all staff to undertake.
8: Incident Response Management	**Risks:** Weaker overall security infrastructure, overall attack surface, and all previously identified risks.
8.1: Establish and Maintain a Security Incident Response Plan	Create a clear and concise incident response plan that includes all key roles and responsibilities for undertaking the plan. This plan must include a checklist of all steps.
8.2: Conduct Post-Incident Reviews	All relevant senior stakeholders and subject matter experts must conduct a post-incident review after every incident to review the cause, the remediation path, and any improvements that can be made to the incident response plan.
9: Business Resilience and Disaster Recovery	**Risks:** Data integrity, business availability, confidentiality, overall attack surface, and all previously identified risks.
9.1: Establish and Maintain Backups and a Data Recovery Plan	Enable and maintain backups of all systems on a regular schedule, at least weekly. These backups enable data recovery. Establish and maintain a data recovery plan with the guidance of a reputable vendor who can be contacted if an event occurs.
9.2: Create a Business Impact Analysis and Business Continuity Plan	Create a Business Impact Analysis that clearly defines potential disruptions to the business and the key roles filled by staff. Develop a Business Continuity Plan to mitigate risks with all relevant stakeholders' alert and informed, knowing their roles and responsibilities.
9.3: Establish and Maintain a Continuous Improvement Plan	Create and maintain a Continuous Improvement plan for the implementation of the above Information Security controls. This plan must include regularly checking the instructions written by the business for any inefficiencies where the effectiveness of the control could be improved.

Appendix 4: Small Business Checklist



Small Business Controls

---CHECKLIST---

1. INVENTORY & CONTROL OF TECHNOLOGY ASSETS

- ☐ 1.1: Establish and Maintain a Record of Assets
- ☐ 1.2: Establish and Maintain a Record of Vendors and Software
- ☐ 1.3: Establish Device Setup and Maintenance Guides

2. NETWORKING

- ☐ 2.1: Establish and Maintain a Secure Network
- ☐ 2.2: Utilise a Secure Network Architecture Standard
- ☐ 2.3 Network Device Hardening

3. DATA PROTECTION

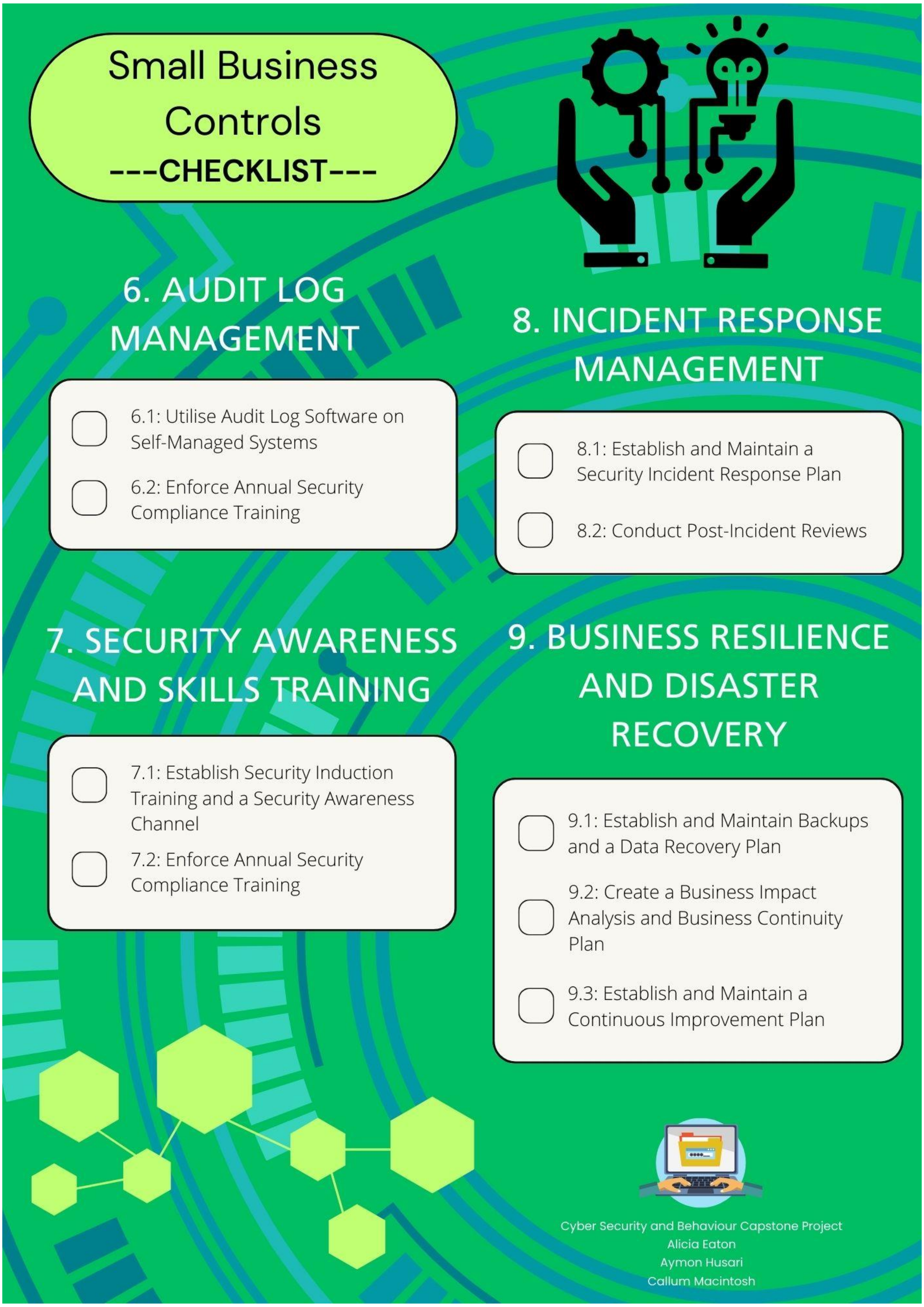
- ☐ 3.1: Establish and Maintain a Data Management Plan
- ☐ 3.2: Enable Email and Browser Protections

4. ACCOUNT AND ACCESS MANAGEMENT

- ☐ 4.1: Establish and Maintain a Record of Users and Accounts
- ☐ 4.2: Enforce Access Controls
- ☐ 4.3: Enforce Security Standards for Passwords and Multi-Factor Authentication (MFA)

5. VULNERABILITY AND PATCH MANAGEMENT

- ☐ 5.1: Resolve Vulnerabilities and Deploy Patches
- ☐ 5.2: Perform Penetration Testing on Systems



Small Business Controls

---CHECKLIST---

6. AUDIT LOG MANAGEMENT

- □ 6.1: Utilise Audit Log Software on Self-Managed Systems
- □ 6.2: Enforce Annual Security Compliance Training

7. SECURITY AWARENESS AND SKILLS TRAINING

- □ 7.1: Establish Security Induction Training and a Security Awareness Channel
- □ 7.2: Enforce Annual Security Compliance Training

8. INCIDENT RESPONSE MANAGEMENT

- □ 8.1: Establish and Maintain a Security Incident Response Plan
- □ 8.2: Conduct Post-Incident Reviews

9. BUSINESS RESILIENCE AND DISASTER RECOVERY

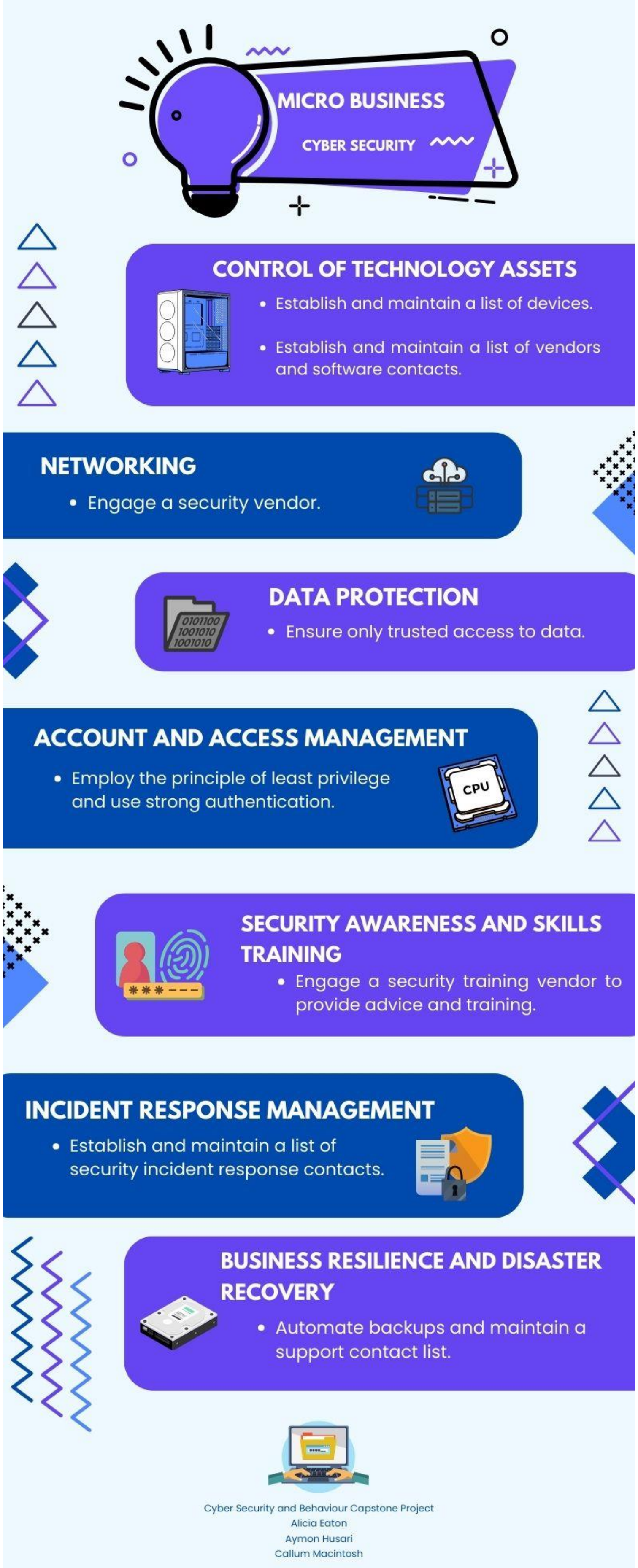
- □ 9.1: Establish and Maintain Backups and a Data Recovery Plan
- □ 9.2: Create a Business Impact Analysis and Business Continuity Plan
- □ 9.3: Establish and Maintain a Continuous Improvement Plan

Cyber Security and Behaviour Capstone Project
Alicia Eaton
Aymon Husari
Callum Macintosh

Appendix 5: Micro Business Controls

CONTROLS	*DESCRIPTION*
1: Control of Technology Assets	**Risk: Unauthorised access.**
1.1: Establish and Maintain a List of Devices	Keep a list of devices owned by the business, such as computers, phones, network routers, etc. Keep this list up to date with every change.
1.2: Establish and Maintain a List of Vendors and Software Contacts	Keep a list of contacts for all vendors, service providers, and software used by the business for when you need any assistance. Utilise reputable and reliable software to limit the amount of assistance needed.
2: Networking	**Risk: Business availability.**
2.1: Engage a Secure Network Vendor	Utilise a trusted and reputable secure network vendor who can either set up your network for you based on the business needs or advise on how you should proceed. Keep a direct line of contact with the vendor so they are always available when you need assistance or to advise on ways to improve your network.
3: Data Protection	**Risk: Data integrity.**
3.1: Ensure Only Trusted Access to Data	Ensure only trusted and reputable vendors have access to sensitive data. Only use vendors that utilise end-to-end encryption for transferring data. Keep a trusted contact for when or if you have any concerns around access and management of your data.
4: Account and Access Management	**Risk: Confidentiality.**
4.1: Employ the Principle of Least Privilege and Use Strong Authentication	Only give employees access to systems if and when they need it. Educate all employees on using strong passwords (minimum length, uppercase, lowercase, numbers, and special characters) as well as Multi-Factor Authentication (MFA) for all logins.
5: Security Awareness and Skills Training	**Risk: Human error.**
5.1: Engage a Security Training Vendor to Provide Advice and Training	Use a reputable training vendor to provide annual security training and advice on best practices that is tailored to the business. Keep a direct contact with the vendor to ensure you can always contact them for help or advice.
6: Incident Response Management	**Risk: Overall attack surface.**
6.1: Establish and Maintain a List of Security Incident Response Contacts	Create a clear and concise list of important contacts to engage if a security incident occurs. These contacts will be the team to guide you through your response.
7: Business Resilience and Disaster Recovery	**Risk: Business availability.**
7.1: Automate Backups and Maintain a Support Contact List	Use automated cloud backup of key data. These backups enable data recovery. Keep a list of support contacts who can assist with recovery of data and systems.

Appendix 6: Micro Business Infographic



MICRO BUSINESS

CYBER SECURITY

CONTROL OF TECHNOLOGY ASSETS

- Establish and maintain a list of devices.
- Establish and maintain a list of vendors and software contacts.

NETWORKING

- Engage a security vendor.

DATA PROTECTION

- Ensure only trusted access to data.

ACCOUNT AND ACCESS MANAGEMENT

- Employ the principle of least privilege and use strong authentication.

SECURITY AWARENESS AND SKILLS TRAINING

- Engage a security training vendor to provide advice and training.

INCIDENT RESPONSE MANAGEMENT

- Establish and maintain a list of security incident response contacts.

BUSINESS RESILIENCE AND DISASTER RECOVERY

- Automate backups and maintain a support contact list.

Cyber Security and Behaviour Capstone Project
Alicia Eaton
Aymon Husari
Callum Macintosh