**Cyber Incident Response Plan Template**

**For Small and Medium-sized Businesses**

A cyber incident can hugely impact any business – small or large. A cyber incident response plan is extremely important for responding to a cyber attack, mitigating damage, and getting your business back on track to run smoothly.

Fortunately, performing security controls and following a cyber incident response plan does not have to be complicated and overwhelming. We understand that small business owners don’t have enough resources to learn all the technicalities behind cyber security. Hence, we at the Western Centre of Cybersecurity Aid and Community Engagement (CACE) designed a Cyber Incident Response plan dedicated to small and medium-sized businesses.

The purpose of this document is to introduce business owners to the most common cyber security incidents that could occur to them and prepare their business with the recommended security controls and measures - allowing them to operate in a more safe and secure environment.

Before commencing with the Cyber Incident response template, it is highly recommended for business owners to first assemble their Incident Response team - establish the roles and responsibilities of each member and complete the Key Contact List below. Good communication is the key to every incident, having a clear sense of who is responsible for what and knowing who to contact in an occurrence of an incident will make resolving the incident more systematic and will avoid confusion amongst staff.

The Incident response team is usually composed of:

Text

Description automatically generated

Text

Description automatically generated

Once you’ve established your fundamental Incident response team, it is essential that to populate the Key Contact list below. This key contact list should also be printed and stored in a location known by every single staff in your business.

**Key Contacts:**

|  |  |  |
| --- | --- | --- |
| **Role** | **Name** | **Contact Information** |
| **Incident Manager** | **[Provide the information as needed. Depending on the business size and skills availability, some staff may take multiple roles]** |  |
| **Tech Lead** |  |  |
| **Communications Advisor** |  |  |
| **Legal Advisor** |  |  |

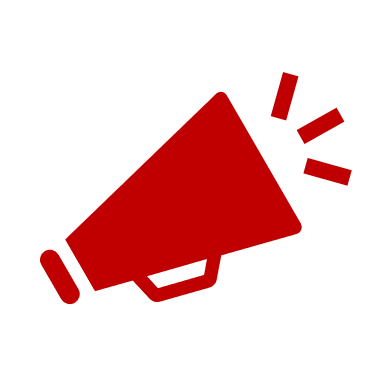
**A cyber incident can happen to anyone. You are not to blame.**

For general information, including cyber security advice on managing your business to operate safely and securely, visit the Western Centre of Cybersecurity Aid and Community Engagement (CACE) website.

Should your business need further support in responding to a cyber incident, do not hesitate to contact the online hotline of Western CACE.

Phone Number: XXX-XXXXX

**Western CACE is here to assist you.**



**IMPORTANT:**

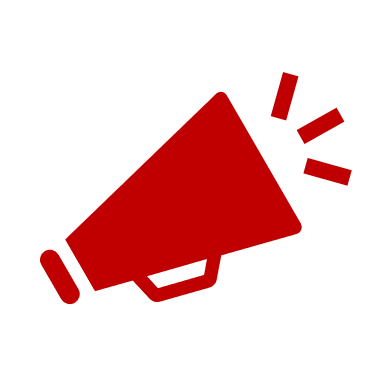
**This Cyber Incident Response Template is designed specifically for Small to Medium Sized Businesses a separate template for Micro-businesses or Family-owned businesses is available at xxxxx.**

**Once the necessary information regarding your business has been supplied in this document, it is important to keep a digital and physical copy of the** Cyber Incident Response Plan Template.

**Keep this document and any copies secured and protected!**

**Why?**

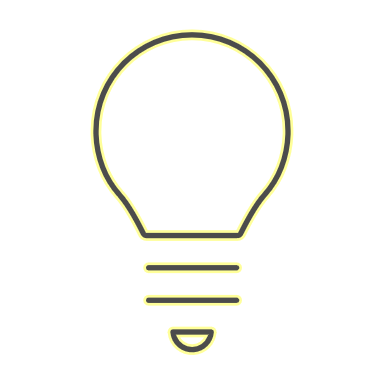
It is critical that business owners should safeguard the Cyber Incident Response Template as this document will include crucial information regarding your cyber security operations. If criminals can easily access your Plan, then they will be one step ahead of you in responding to the incident and this will result in you losing MORE MONEY.

****

**Tips on Document Management:**

.

* If printed out, every employee should know where the plan is located.
* The Key Contact List should be easily accessed.
* The employees should be familiar with the Cyber Incident Response Plan Document before they use it
* If stored online, must be protected with a strong password
  + activate Multi-Factor Authentication when available



**Introduction**

Cyber security is the protection of information and digital assets from compromise, theft, or loss. Therefore, this area of business is critical for all - large and small businesses alike. The purpose of this template is to ensure that responses and resolutions to cybersecurity-relevant incidents encountered in small to medium business settings are addressed and coordinated effectively and efficiently.

As indicated on the cover page, this template is specifically designed for Small to Medium Sized Businesses; **a separate template for micro-business is available on XXXXX.**

**The table below provides a guide for better understanding on the difference between Small Businesses and micro-businesses.**

Graphical user interface, application, website, PowerPoint

Description automatically generated

This template is divided into 3 main sections which illustrates the common phases in a typical cyber incident:

**Pre-Incident** – What to prepare for?

**During an Incident** – What to do and who to contact during an Incident?

**Post Incident** – Reviewing Lessons Learned from the Incident

Diagram

Description automatically generated with low confidence

Pre - Incident – What to prepare for?

As the famous Scout’s motto “Be Prepared”, this should also be instilled to every aspect of your business structure from the technology used down to the people involved. You must acknowledge that cyber incidents are unavoidable, having a “we’ll figure it out when the time comes” mentality is a BIG NO when dealing with a cyber-attack. Being prepared and having an Incident response plan can have a significant advantage – from dealing to a critical incident to just a minor interruption.

The preparation and planning stage is the most crucial phase in protecting your business from cyber incidents - you plan and prepare in order to prevent and respond well for an eventual cyber-attack.

In this section we will introduce the top three most common cyber-attacks small business can encounter and security measures that can be implemented to help protect your business :

# Phishing

Data Breach

Ransomware

Graphical user interface, text, application

Description automatically generated

<https://www.cyber.gov.au/acsc/view-all-content/programs/stay-smart-online/scam-messages/quiz>

Text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Some guides

Step-by-step guides provided by the Australian Cyber Security Centre (ACSC) to implement security controls for certain operating software and devices are available at:

<https://www.cyber.gov.au/acsc/small-and-medium-businesses/step-by-step-guides>

Along with the preventive measures mentioned above, there are the 8 Essential Controls developed by the Australian Signals Directorate (ASD) which you can learn more about from the following links:

<https://www.vmia.vic.gov.au/-/media/Internet/Content-Documents/Tools/Cyber/Improving-Cyber-Maturity-with-the-Essential-8-Guide.ashx?rev=c341ae7661fc4715adcc5650246010e9>

<https://www.cyber.gov.au/acsc/view-all-content/essential-eight>

Checklists

It is highly recommended that you follow the checklists provided below in order to improve the security of your business.

**Software Considerations**

|  |  |
| --- | --- |
| **Checklist Item** | **🗸** |
| Ensure you have security software (antivirus) on your computers |  |
| Turn on automatic updates for your operating system |  |
| * Set up a convenient time for these to occur |  |
| Ensure you keep backups, and regularly verify you can restore your backups |  |
| Enable Multi-Factor Authentication wherever possible |  |

*\*\*\* A key point in handling an incident well as a small business is to ensure that the affected device should not be tampered with, without an appropriate expert.*

## **People and Procedures**

|  |  |
| --- | --- |
| **Checklist Item** | **🗸** |
| Establish an Access Control System to determine who should have access to what |  |
| * Restrict administrator privileges to an ‘as required’ basis |  |
| * Do not share passphrases e.g. individual logins |  |
| * Remember to revoke accounts when employees leave the business |  |
| Enable Multi-Factor Authentication wherever possible |  |

|  |  |
| --- | --- |
| **Checklist Item** | **🗸** |
| Incorporate, update and regularly repeat cyber security training and awareness amongst your employees |  |
| Familiarise all with a cyber security incident response plan |  |
| Reward employees who find threats |  |
| Create a cyber security culture and encourage regular discussions |  |
| Always be cautious of malicious emails with special attention to: |  |
| * Requests for money, especially if urgent or overdue |  |
| * Bank account changes |  |
| * Attachments, especially from unknown or suspicious email addresses |  |
| * Requests to check or confirm login details |  |

## **Passwords Consideration**

## 

|  |  |
| --- | --- |
| **Checklist Item** | **🗸** |
| Use strong passphrases |  |
| * Use with Multi-factor authentication |  |
| * Ensure the password is complex |  |
| * Ensure the password is Unique |  |

## 

## **Key Contact Table**

Fill out the table below with all the appropriate information you have. Note that smaller businesses can have one person who has multiple IT-related titles within the structure.

This table can be modified as needed to suit the needs of the business.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name Title** | **Who does what if cyber incident?** | **Contact Information** | **Next Steps** |
|  |  |  | Cyber insurance company listed with contact details and person |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Third Party Support and Response**

Thorough comprehension of Incident Response is necessary for third parties and insurances. The list below contacts needed for support

|  |  |  |  |
| --- | --- | --- | --- |
| **Service Provider** | **Services** | **Contact** | **Response** |
| Service Provider name | Services Provided; Insurance Providers, Internet Service Provider (ISP), Cloud Service Provider (CSP) etc. | Immediately after any financial or data loss. | Response time will vary amongst Service Providers. |
|  |  |  |  |
|  |  |  |  |

# During an incident

Even with all the security controls implemented in your system and all the staff awareness training, cyber incidents can still occur. Having an organised incident response plan can mitigate and reduce the risks of the cyber-attack whilst still maintaining business operations.

When faced with a cyber incident, the first rule is *do not panic*.

When detecting a cyberattack there never is one process, detection involves:

* Indicators: Alerts you receive using intrusion detection software or your systems behaving strangely with various unknown files popping up are usually indicators of a cyber-attack that may have occurred.
* Security Monitoring: When a third-party service provider alerts you to a possible attack.
* Precursors: The rarest form of detection, this happens when you detect a cyber-attack that possibly could happen in the future. For example, when a new ransomware is released or a company that provides you with some service has been affected by a breach.

Other precautions you can take during a cyber-attack:

* Trying to minimize the damage by blocking the malicious traffic using various firewall rules.
* Notifying authorities and anyone else who could be affected by the cyber-attack.
* Try to contact experts in the area to guide you through the problem.
* Assessing the attack in a calm mind to make sure it’s not a false positive before you go all panic mode.
* Try to contain the damage of an attack by shutting down all affected systems before the malware moves to other parts of your network.

Here are some indicators you may notice during or before a cyber-attack:

* Multiple staff accounts being locked out of their systems.
* Reports of multiple staff members being targeted by phishing emails
* Multiple systems acting slower than usual.
* Weird files being created throughout the computers.
* Unusual traffic being sent through your network (This could be a potential DDoS attack)
* System logs showing multiple failed attempts for log-ins.
* Reports of your companies’ services being inaccessible/shutdown.
* Anti-virus showing alerts for suspicious activity or files on your system.

If you are looking for an expert to assist, please check out website for trusted industry partners.

Post Incident – What to do after an Incident has occurred?

This phase is often overlooked at but serves as an important part of any cyber incident response plan. In every cyber incident encountered there is an opportunity to learn and continuously improve on cyber incident management of your business.

Post Incident Review

A post incident review is beneficial in identifying what security measures were insufficient or configured improperly to stop the attack. All staff members involved in resolving the cyber incident will come together for a post incident review with the goal of answering the following questions:

1. When was the Incident detected and when was it resolved?
2. How can this incident be resolved faster?
3. How well did the employees and management deal with the incident?
4. List all the tasked performed along with the time and classify which task made positive, negative or no impact.
5. What information should be provided sooner?
6. What actions can be improved the next time a time a similar incident occurs?

Actionable Tasks: Implementing Security Controls

Evaluating how the cyber incident occurred, and the performance of your response can aid you in determining which security controls needs to be activated or updated.

<link to WIREFRAME SECURITY Controls Activation>

Contact WesternCACE for a free consultation if you are experiencing challenges to implement security controls. Please see our industry sponsors for trusted Australian cybersecurity businesses who can provide services for payment.

**Common Cyber Security Terms**

**Availability:** Availability refers to the reliable accessibility of the data, that is, keeping necessary data for the business “live” or “online”.

**Business email compromise:** Business e-mail compromise (BEC) is when an attacker hacks into a corporate e-mail account and impersonates the real owner to defraud the company, its customers, partners, and/or employees into sending money or sensitive data to the attacker's account.

**Confidentiality:** Confidentiality refers toensuring the protection of data and the prevention of unauthorised disclosure of information.

**Data breach:** Personally Identifiable Information (information that can be used to identify an individual) or sensitive data is compromised due to an attacker having unauthorised access to the system and its associated data.

**Denial of Service (DoS):** A mass amount of network traffic is sent to a victim, causing the network to fail, therefore halting access to necessary data or infrastructure necessary for business operations.

**Distributed Denial of Service (DDoS):** A large-scale DoS attack usually from several devices.

**Event:** An event is something that affects the normal operation of IT systems, services and infrastructure. It is important to note that not all events become incidents

**Incident:** An incident is an event as defined by the Australian Cyber Security Centre (ACSC) as an unwanted or unexpected cybersecurity event or series of events that have a significant probability of negatively affecting business operations. Incident Severity can be determined by considering the effect the incident has on the confidentiality, integrity and availability of data, along with the systems that have been affected by the incident.

**Integrity:** Integrity refers to the accuracy and validity of the data. That is, measures put into place to protect the integrity of data are focused on the prevention of modification or misuse of data.

**Malware (Malicious software):** An entity such as a virus, Trojan horse, worm etc that can successfully disrupt and interfere with the host.

**Ransomware**: A type of malware in which the host’s device is locked by an attacker and a ransom is demanded in order to unlock the device

**Social Engineering:** Social engineering is a potential vector for an attack and occurs when an attacker tries to manipulate the victim into divulging sensitive data that can compromise the business and/or business network in some way.