|  |  |
| --- | --- |
| How to use this incident response plan template | |
| This incident response plan template  has been designed to help organisations prepare for any cyber incidents that may occur. Fill it out now and have it ready should an incident happen. | |
| About this template | It is most appropriate for small to medium businesses and similar organisations, including:   * sole traders, * small companies, * charities, * incorporated societies, * not-for-profit organisations, and * non-government organisations.   The template has been built with sections that can be deleted if not applicable to your business.  **NOTE**: This template should not be used as a substitute for professional cyber security advice. |
| Helpful links to start with  * [Create an incident response plan -  Own Your Online](https://www.ownyouronline.govt.nz/business/get-protected/guides/create-an-incident-response-plan/) * [If you have had an online security  incident - Own Your Online](https://www.ownyouronline.govt.nz/business/get-protected/guides/if-youve-had-an-online-security-incident/) |
| Sections in the template | Document control and review: This section is used only to keep track of any updates to the plan over time.  Version control can be deleted if you don’t need to keep track of draft versions. Purpose What the plan is for. Other information This is where you can link to other internal documents your organisation may have that are related. Can be deleted if not applicable. |

|  |  |
| --- | --- |
| Identify assets and roles | |
| Identifying key assets This table is for you to describe everything that  is important to your organisation, that could be affected by cybercrime. Sometimes this is called  “the Crown Jewels” because of their importance.  It could be as simple as a social media account or  as complex as a sales registration system or just  your own website. Remember even a database of customer information is a digital asset that could  be targeted.  Physical assets, such as computers and phones,  should be added but other assets, such as  machinery or vehicles, don’t need to be added  unless they connect to the internet and could be targeted through an online attack.  When an incident occurs, this table will allow you  to quickly remind yourself what you need to do  and what you need to check on. | Key roles These are the people in your organisation  who will be called into action when a cyber  incident happens. Identifying cyber incidents Use this table to determine the type of  incident and the risk level. |

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Explanation | Impact | Risk level |
| Phishing scam (internal) | Email or text message directing you to click a link  or open an attachment with the goal of harvesting personal or financial information. | Financial loss, credentials given over. | Low |
| Phishing scam (external) | Your organisation is impersonated online in an attempt to gain information from your customers, members or other stakeholders. | Financial loss, breach of privacy, brand damage. | Low |
| Insider threat | A current or former employee of your organisation causes disruption due to knowledge or access. | Theft of trade secrets, release of private data, denied access to services, brand damage. | Medium – High |
| Business email compromise | When an attacker gets access to an employee’s email account without their permission, to carry out attacks or scams, such as invoice scams. | Financial loss, breach of privacy, brand damage | Medium – High |
| Data breach | When private information held by an organisation is compromised, stolen, or accidentally released. | Breach of privacy, loss of intellectual property, brand damage. | Medium – High |
| DDoS attack | Your online tools, including websites, are overloaded with requests from ‘bots’. | Unable to load website or use internet. | High |
| Ransomware | Malware which locks and encrypts your systems, denying access unless a ransom is paid. Can be run  in conjunction with data breach | Business disruption, loss of income, breach of privacy. | High |

|  |  |
| --- | --- |
| When an incident happens | |
| Determining the scale and  response required Assess the likelihood and severity for each of the following possible outcomes.   * Impact on your ability to continue * usual operations. * Financial loss to our organisation or others. * Reputational damage, such as reduction  in trust and confidence. * Breach of a legal obligation (for example,  a privacy breach from leaked information).   The assessment is subjective based on how your business works and what has been targeted. Identify and contact the  appropriate people This table outlines who to contact based on what  the incident is. The contact details will be in the  ‘Key roles’ section.  You can use your answers to the ‘Key asset’ table  to fill out the “Risk to asset” column. Review post-incident This is an extra step that you only need after  an incident has occurred.  It’s a good way to see if the plan worked and if  any changes are needed. |  |

|  |
| --- |
| Incident response plan for [organisation name] |

|  |  |  |  |
| --- | --- | --- | --- |
| Author | | Owner | Date created |
| name | | name | \_\_/\_\_/\_\_\_\_ |
| **Last reviewed by** | **Last date reviewed** | **Approval by and date** | **New review due date** |
| name | \_\_/\_\_/\_\_\_\_ | name \_\_/\_\_/\_\_\_\_ | \_\_/\_\_/\_\_\_\_ |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date of approval | Approved by | Description of change |
| Text field | \_\_/\_\_/\_\_\_\_ | name | Text field |

To create a new row click the bracket ‘**]**‘ on the right of the table and press ‘Tab’ on your keyboard.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Purpose**  The purpose of this incident response plan  is to set out the basic steps employees can  follow in the event of a cyber incident. | Other information Further information, related to managing and responding to incidents. [can delete if none]   |  | | --- | | [Insert link to your business continuity plan] | | [Insert link to any other relevant internal documents] | | [Insert link to any relevant documentation from your IT provider] | |

|  |  |
| --- | --- |
| Identify assets and roles | |
| Identifying key assets This table contains the information or technology assets that are most important to our organisation and the risk level if they are targeted. |  |

| Asset | Organisational use | Impact if lost | Risk level |
| --- | --- | --- | --- |
| EXAMPLE: Facebook account | Advertising and communications | Loss of revenue and damage to reputation | Medium/High |
| EXAMPLE: Client database | Contact and invoicing details | Financial loss and severe damage to reputation | High |

To create a new row click the bracket ‘**]**‘ on the right of the table and press ‘Tab’ on your keyboard.

|  |  |
| --- | --- |
| Identify and contact the appropriate people |  |

Depending on the nature of the incident, you may need to contact external   
service providers. This table is a guide to who to contact. [tick relevant fields].

| Risk to asset | Who to contact | | | | |
| --- | --- | --- | --- | --- | --- |
| CERT NZ (part of the NCSC) | IT Provider | Bank | Web Host  or platform | Lawyer |
| EXAMPLE: Unable to use social  media | ✔ | ✔ | ✔ | ✔ | ✔ |
| EXAMPLE: Theft of trade secrets | ✔ | ✔ | ✔ | ✔ | ✔ |
| EXAMPLE: Financial loss | ✔ | ✔ | ✔ | ✔ | ✔ |
| EXAMPLE: Breach of client data in a ransomware attack | ✔ | ✔ | ✔ | ✔ | ✔ |

To create a new row click the bracket ‘**]**‘ on the right of the table and press ‘Tab’ on your keyboard. Copy and paste the ticks where required.

If personal data has been leaked or stolen, we are legally required to report to the Privacy Commission within 72 hours. CERT NZ (part of the NCSC) can give more advice on this. [can delete if your business   
does not hold any personally identifying information]

| Incident | Report to | Contact Details |
| --- | --- | --- |
| Data or privacy breach | Privacy Commission | [Office of the Privacy Commissioner | NotifyUs - For organisations to reoprt privacy breaches](https://www.privacy.org.nz/responsibilities/privacy-breaches/notify-us/) |

|  |  |
| --- | --- |
| Identify assets and roles | |
| Key roles If you suspect a cyber security incident has occurred, these are  the people notify in the first instance. |  |

| Affected asset | Name & Organisation | Role | Contact Details |
| --- | --- | --- | --- |
| EXAMPLE: Internal computer system | Bill Gates – Windows Security | EXAMPLE: IT specialist | 555-5555 BillyGates007@Microsoft |
| EXAMPLE:  Facebook page locked or copied | Text field | EXAMPLE> Social media manager | Text field |

To create a new row click the bracket ‘**]**‘ on the right of the table and press ‘Tab’ on your keyboard.

|  |  |
| --- | --- |
| If the incident is confirmed, escalate to the following. |  |

| Role | Name & Organisation | Phone Number | Email Address |
| --- | --- | --- | --- |
| CERT NZ (part of the NCSC) | Incident response team | 0800 CERT NZ | Online reporting form |
| EXAMPLE: CEO | Text field | Text field | Text field |
| EXAMPLE: External IT support | Text field | Text field | Text field |

To create a new row click the bracket ‘**]**‘ on the right of the table and press ‘Tab’ on your keyboard.

|  |  |
| --- | --- |
| Key contact list Any important contacts not listed above. |  |

| Service | Name & Organisation | Phone Number | Email Address |
| --- | --- | --- | --- |
| EXAMPLE: Bank | Text field | Text field | Text field |
| EXAMPLE: Website | Text field | Text field | Text field |
| EXAMPLE: Lawyer | Text field | Text field | Text field |

To create a new row click the bracket ‘**]**‘ on the right of the table and press ‘Tab’ on your keyboard.

|  |  |
| --- | --- |
| When an incident happens | |
| Determining the scale and response required Use the following risk assessment chart to determine the scale and  response required for the incident and fill in the impact table. |  |

A screenshot of a computer

Description automatically generated

# Impact table

|  |  |  |  |
| --- | --- | --- | --- |
| Impact type | Severity | Likelihood | Risk level |
| Impact on usual operations | Text field | Text field | Text field |
| Reputational damage | Text field | Text field | Text field |
| Financial loss | Text field | Text field | Text field |
| Breach of legal obligation | Text field | Text field | Text field |
| Overall | Text field | Text field | Text field |

If the risk is assessed to be Medium-High or High, then immediately contact   
CERT NZ (part of the NCSC) for assistance. 0800 CERT NZ or [www.cert.govt.nz](http://www.cert.govt.nz)

|  |
| --- |
| Communications When an incident happens communicating with staff and external stakeholders needs to be done  quickly and with care. Own Your Online has information on how best to communicate to customers and stakeholders about the incident, including an Incident Communication Framework that we can use. Or contact NCSC directly for more personalised help.  [Communicating in an online security incident - Own Your Online](https://www.ownyouronline.govt.nz/business/get-protected/guides/communicating-in-an-online-security-incident/) |

|  |  |
| --- | --- |
| Review post-incident | |
| Share with the wider organisation as appropriate.  Ensure any employees and external service providers involved in  responding to the incident are involved in the debrief. |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Discuss | Comments | Action Required | Person Responsible | Due Date |
| What went well? | Text field | Text field | Text field | Text field |
| What could have been done better? | Text field | Text field | Text field | Text field |
| Does this response plan need updating? | Text field | Text field | Text field | Text field |
| What changes need to be made to day-to-day systems and processes? | Text field | Text field | Text field | Text field |

|  |  |
| --- | --- |
| Cyber security incident key contact list | |
| Keep this in a place you’ll easily find it when an incident happens. |  |

| Name & Organisation | Role | Phone Number | Contact Details |
| --- | --- | --- | --- |
| CERT NZ (part of the NCSC) | Advice and help with any incident | 0800 CERT NZ (0800 2918 69) | Online reporting form: <https://www.cert.govt.nz/report/business-and-individuals/>  info@cert.govt.nz |
| Bill Gates – Windows Security | EXAMPLE: IT specialist | 555-5555 | BillyGates007@Microsoft |
|  |  |  |  |
|  |  |  |  |

To create a new row click the bracket ‘**]**‘ on the right of the table and press ‘Tab’ on your keyboard.