­­

School of Design and Informatics

BSc Ethical Hacking, 2022/23

**An Evaluation of Modular Incident Response Plans for Efficient Cyber Incident Mitigation in Businesses**

**Cyber Incident Response Plan**

**Version: 1.0**

**Author:** Martin Georgiev **Supervisor**: Natalie Coull

Head of Division of Cybersecurity Abertay

**Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| Version № | Updated By | Reason for Update/Area Updated | Date Updated |
| vX.X | <Group Name> | <Brief update description> | <Date of Update> |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Approval Record**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version № | Approval Body | Date of Approval | Date of Review | Effective Date |
| vX.X | <Organisation Name> | <Date> | <Date> | <Date of Operation> |
| vX.X | <Department Name> |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Distribution List**

|  |  |
| --- | --- |
| Department Names | Personnel Positions |
| <Name of departments provided with the plan> | <Name of separate positions provided with the plan> |
|  |  |
|  |  |
|  |  |
|  |  |

# **Pre-reading**

The following Cyber Incident Response Plan Template for an Honours Project was created for educational purposes. The plan was designed as generalised to fit different types of incidents, including automated and manual attacks carried out by adversaries or malicious software. The template was created based on the Scottish Cyber Incident Response Template for the Public Sector (Scottish Government, 2021) and Cyber Management Alliance’s CIRP Template (CM Alliance, 2015 – Present Day). It is a more generalised version of the former (fitting different countries rather than just Scotland) and a less technical approach compared to the latter (as it is aimed at both large and small organisations).

Contents

[**Pre-reading** ii](#_Toc134541779)

[**Terminology and Abbreviations** iv](#_Toc134541780)

[**1** **Introduction** 1](#_Toc134541781)

[**1.1** **Purpose** 1](#_Toc134541782)

[**1.2** **Incident Co-ordination Policy** 1](#_Toc134541783)

[**1.3** **Scope of CIRP** 2](#_Toc134541784)

[**2** **Management Roles and Responsibilities** 3](#_Toc134541785)

[**2.1** **Cyber Incident Response Team (CIRT)** 3](#_Toc134541786)

[**2.2** **Crisis Management Team (CMT)** 3](#_Toc134541787)

[**2.3** **RACI Matrix** 4](#_Toc134541788)

[**2.4** **Updating the CIRP** 5](#_Toc134541789)

[**3** **Communications** 6](#_Toc134541790)

[**3.1** **Management** 6](#_Toc134541791)

[**3.2** **Human Resources** 6](#_Toc134541792)

[**3.3** **Third-party Organisations** 6](#_Toc134541793)

[**4** **Response Process** 8](#_Toc134541794)

[**4.1** **Preparation** 8](#_Toc134541795)

[**4.1.1** **Threat Intelligence** 9](#_Toc134541796)

[**4.1.2** **Training and Awareness** 9](#_Toc134541797)

[**4.2** **Identification** 9](#_Toc134541798)

[**4.3** **Incident Reporting** 11](#_Toc134541799)

[**4.4** **Analysis and Assessment** 11](#_Toc134541800)

[**4.4.1** **Severity Assessment** 12](#_Toc134541801)

[**4.4.2** **Severity Guidance** 13](#_Toc134541802)

[**4.5** **Incident Containment** 16](#_Toc134541803)

[**4.6** **Incident Eradication** 16](#_Toc134541804)

[**4.7** **Incident Recovery** 17](#_Toc134541805)

[**5** **Further Awareness and Reporting** 17](#_Toc134541806)

[**6** **References** 19](#_Toc134541807)

# **Terminology and Abbreviations**

***Note: The terminology and abbreviations in this document cover data from the generic CIRP and the respective attack-specific modules!***

CIRT – Cyber Incident Response Team

CIRP – Cyber Incident Response Plan

Malware – Malicious software used to attack computers, cause damage, steal data, etc.

CMD – Command Line, a window used to execute commands

Adversary – Threat actor.

Threat Intelligence – Knowledge and skills concerning cyber and physical threats for an organisation.

Hash – An encrypted signature of a file showing the amount of data. It is different for each file, even if they are the same size.

BIOS – Basic Input-Output System, a system used by Operating Systems (Linux, Windows, MacOS) to communicate with the physical parts of the computer.

String – A set of characters, usually human-readable data.

RACI Matrix – Responsibility Assignment (responsible, accountable, consulted, informed) Matrix.

VirusTotal – An online service combining multiple Anti-Virus solutions.

File Packer – Tools used to compress files. They may be used for legitimate reasons to save space or for malicious reasons to bypass Anti-Virus tools.

crucial information about the packer and what type of file it is.

Sections – The different parts of the file.

Network adapter – Device used for internet connectivity.

Terminal – Linux alternative of the CMD.

Sudo – Allows a user to execute commands as root.

Root – Highest privilege account in the Linux hierarchy.

DNS – Domain Name System, a protocol used to turn IP addresses into names that are easier to remember

IP address – Address of a machine within a network.

MAC address – Physical address of the network adapter.

HTTP – Hyper-text transfer protocol, a protocol used for web traffic.

Registries – Collections of information within the Windows operating system.

RAM – Random Access Memory, memory used to store data for current processes.

Network packets – Pieces of data sent through the network and used for communication.

DHCP Server – Protocol used to dynamically configure IP addresses of new machines. It automates the process and allows users to easily connect and disconnect devices.

Plugin – Additional parts of software that are not essential for its normal workflow. They usually enhance the current capabilities or add new functions.

C&C server – Command-and-Control server used to command the malware, store stolen data, or provide it with more features.

Encryption – Concealing information by making it appear as random data. It can be decrypted using specific keys. Ransomware use this capability to prevent victims from accessing their data.

Obfuscation – Making data appear unclear and difficult to understand.

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

Volatile data – Data such as RAM that can easily disappear, i.e., RAM contents disappear after a computer is turned off.

Phishing – Sending false malicious emails, trying to trick a user into executing the file.

Spearphishing – A variation of phishing that targets a specific target and including their personal data in the emails – mentioning their family, personal events, etc.

HDD/SSD – Hard disk drive and solid-state drive – devices used for data storage.

Persistence – Renew the actions after the computer is restarted.

Propagation mechanisms – Capabilities that allow the malware to send itself to other computers.

MBR – Master Boot Record, a sector in the HDD/SSD that contains information about the other data sectors.

Zombie account – Accounts without a verifiable owner.

# **Introduction**

## **Purpose**

This Cyber Incident Response Plan (from here on **CIRP**) aims to provide **<Organisation Name>**’spersonnel with a structure of processes and procedures to effectively respond to incidents that may impact the function and security of assets, information resources, and normal business operations of the organisation.

Cyber-attacks can often promptly escalate and significantly disrupt standard business operations, requiring quick considerations from both the Management and Cybersecurity departments of the affected organisation. Despite the design of this plan to mainly be managed within the IT Security environment of the company, Business Continuity and Resilience Leads should also be constantly notified about the development of the situation so the issue caused by the attack can be managed on multiple levels – not only cyber but also financial, production, etc. Therefore, the Resilience Leads and Business Continuity departments must be familiar with the CIRP.

The CIRP is going to aid the **<Organisation Name>** in the process of identification, management, and mitigation of various cyber incident types. It will guide the **<Organisation Name>** through the initiation of a response and investigation, following a specific structure to ensure the efficacy of the response. Furthermore, various documentation and entities will be mentioned throughout the report based on the severity of the incident and suggested actions.

It should be noted that the plan cannot guide **<Organisation Name>** through all possible incidents. The current situation should be evaluated and considered by the responders and the management to assess its impact, potential adversaries, and the organisation’s needs. The suggested CIRP should be used as a guide and a basis for the response.

This CIRP was created with the following industry standard practices:

* The Standard of Good Practice for Information Security 2018
* ISO/IEC 27035: 2016 Information Security Incident Management
* Existing cyber incident response documentation by organisations of the Scottish Public Sector
* NCC Group experience and knowledge

## **Incident Co-ordination Policy**

All organisations should comply with the governmental cyber incident response policies, which outline any procedures for notifiable cyberattacks impacting the government and public services. To consider notifying the government, the following (but not limited to) incidents or attacks against the public network systems should be carried out by adversaries:

* Carry the likelihood of national media interest and intel leakage;
* Carry the chance that other public, private and/or third-sector corporations could experience or spread a potential attack;
* Carry the potential to disrupt the regular operation of an organisation and/or to deliver public services;
* Bring harm to the government and the public sector’s reputation.

Keeping this in mind, the affected organisation, **<Organisation Name>**, is required to notify the cyber department of their country (i.e., National Cyber Security Centre (NCSC), Scottish Government Cyber Resilience Unit (SG CRU), Cybersecurity and Infrastructure Security Agency (CISA)) depending on the country of origin. With this, the organisation should provide the departments with the requested data to coordinate and manage the incident and consider the police departments for potential criminal investigation.

## **Scope of CIRP**

**Information Security Incidents** specifically affect **<Organisation Name>**’s information (i.e., loss/theft/damage/destruction of data or physical equipment used to store said data) and potentially impact the integrity and confidentiality of the organisation’s intel. In case of unavailability of the information, the situation should typically be identified as IT Service Incidents by the management processes as they are focused on restoring the availability to users as promptly as possible.

**Cyber Incident** is a subcategory of Information Security Incidents that affect both digital and physical assets and does not involve any information printed on paper (Account compromise, malware outbreak and network intrusion).

**Cyber Incident Management** is the process of handling cyberattacks in a carefully planned and controlled way. Such management plans ensure:

* All attacks are managed quickly and efficiently;
* Damage by the attacks is minimised as much as possible;
* A consistent approach is implemented using frameworks and industry standards;
* The chances of reoccurrence are minimised with appropriate countermeasures.

The scope of this CIRP is limited to incidents affecting IT services, electronic data and any digital assets controlled by **<Organisation Name>**. The following list of IT incidents are not treated as cyberattacks in this plan, therefore are outside the limits of the scope:

* Software and technical issues caused by benign activity;
* Performance and unavailability problems in the organisation’s network and systems;
* Hardware failure;

# **Management Roles and Responsibilities**

## **Cyber Incident Response Team (CIRT)**

The Cyber Incident Response Team is who manages cyber incidents, including triage, containment, eradication, countermeasures, and reporting. CIRT is responsible for analysing security breaches, taking appropriate measures and advising the executives regarding breaches and how the CIRT is responding to them. The team is brought together whenever any breaches/risks have been raised and assessed by the **<Head of IT Operations>**. A smaller team from the IT security department (Core IT CIRT) can assess and classify the incident before it is escalated to the entire CIRT. Escalating it to the Extended CIRT is possible to relate to external parties (Government, Police, Governmental Cyber Departments, Legal firms, and Third-party security specialists) and non-IT personnel.

The Core IT CIRT consists of personnel specialising in the identification and response to cyber incidents within **<Organisation Name>** and will be led by the **<Head of IT Operations>** and the following staff members:

* Security Analyst
* Security Architect
* Network Operator
* Systems Admin
* Others

The CIRT includes key personnel from the following departments (based on the Scottish CIRT):

* Chief Information Security Officer (CISO) – Incident Owner
* Head of Operations or IT Senior Officer ( ITSO) – Incident Manager
* Information Security Officer (ISO)
* Senior Information Risk Owner ( SIRO)
* Core CIRT Lead
* Human Resources (HR)
* Legal Services Rep
* Finance Rep
* Audit Rep
* Physical Security Rep
* Communications Lead
* Policy Area Lead
* Resilience Lead
* Business Continuity Lead
* Data Protection Officer (DPO)
* Other relevant employees, contractors and third parties

## **Crisis Management Team (CMT)**

Crisis Management Teams (also known as Senior Management Teams) are often formed to handle any Strategic consequences that are brought up by the CIRT within **<Organisation Name>**. The CMT will consist of **<Personnel Names or Positions>**. This team does not specialise in only Cybersecurity but also business, which is why wider issues are brought to them by the CIRT.

## **RACI Matrix**

When it comes to more severe cyber incidents which were escalated to the formation of a CIRT, it is crucial to deal with them with clarity, accountability, and delegation. For such cases, the **RACI Matrix** is a tool which can be used to efficiently assign responsibilities to different individuals/departments and/or create a map of the milestones, key decisions, and milestones in managing the cyber incident. With the matrix, **<Organisation Name>** can also assign accountability to specific entities and personnel who should be informed or consulted in specific cases. The tool will allow them to easily develop their CIRT and clearly state each employee’s role. The **RACI Matrix** uses the following terms:

* **Responsible** – Personnel assigned to complete specific tasks to mitigate the incident.
* **Accountable** – An entity that will answer for the result of an activity and assign work to other people, someone taking valuable decisions.
* **Consulted** – Two-way communication personnel who should be contacted regarding related activities. They should be regularly updated regarding any decisions and tasks to be carried out by the **Responsible** personnel.
* **Informed** – Designated personnel (often executives and/or security managers) who should be frequently updated regarding the development of the incident. Communication should remain in a single-channel fashion.

An example of a **RACI Matrix** (based on the Scottish CIRP) with appropriate tasks and personnel can be found in the table below. (**Table 2.3.1**)The table should be altered to specifically fit the organisation using the CIRP template.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Task No. | Task | IT Managed Service Providers | Management Board | <Organisation Name> ISM | Managed Service Provider | CIRT | Other <Organisation Name> Personnel | Third-Party Stakeholders | Impacted individuals | Law Enforcement and Regulators | Insurers |
| 1 | Incident Identification | R | - | A, R | R | - | R | R | - | - |  |
| 2 | Incident Reports | R | - | A, R | R | - | R | R | - | - |  |
| 3 | Incident Capture | - | - | A | R | - | - | - | - | - |  |
| 4 | Incident Assignment | - | - | A | R | - | - | - | - | - |  |
| 5 | Incident Investigation | R | I | A | R | C | R | R, I | I | I | I |
| 6 | Incident Containment | R | I | A | R | C | R | R | I | I | I |
| 7 | Incident Eradication | R | I | A | R | C | R | R | - | I | I |
| 8 | Incident Recovery | R | I | A | R | R, C | R | R | I | I | I |
| 9 | Recovery and Review | R, C | I | A, R | R | R, C | C | C | - | I | I |
| 10 | Incident Mitigation | R, C | I | A, R | R | C | R | R | I | I | I |
| 11 | Policy Impact | - | I | I |  | R, C |  |  |  | I |  |
| 12 | Resilience and Business Continuity Assessment | - | I | I |  | R, C |  |  |  | I |  |

***Table 2.3.1*** *–* ***RACI Matrix*** *example based on the Scottish CIRT Template.*

## **Updating the CIRP**

Ownership of the Cyber Incident Response Plan is assigned to **<Head of IT Operations>** (change role as appropriate to your organisation) and it will be reviewed on a **<Time Frame>** and/or after a cyber incident. For this reason, **<Organisation Name>** must ensure that the owner’s contact details are frequently updated. This is critical for the effectiveness of how the CIRP will operate.

# **Communications**

Communications are a vital part of managing and countering not only cyber but any type of incident. Effectively and timely communication between the departments, third-party organisations and the assigned teams in charge will ensure a faster and more secure resolution of the issue. This in turn will also minimise the damages caused by the attack.

## **Management**

The CIRT is responsible to keep the core management and third-party associates informed regarding all details of confirmed **<Severity Level/s >** severity incidents. The following entities/departments must be identified:

* Relevant executives who are managing the staff, customers, and stakeholders. It is vital to keep them up to date with the development of the situation in case they need to make any changes in their communications with the beforementioned entities and not hurt the organisation’s reputation.
* Core associates from public third-party sectors and organisations who provide public services and may face any disruptions/possibility of the attack propagating to their network.
* Appropriate authorities such as law enforcement and the government depending on the scale and severity of the attack.

## **Human Resources**

Any confirmed cyber incidents where a significant data breach of previous or current employees must be relayed to the HR personnel. They will be responsible for taking appropriate actions based on the situation. They can be (but are not limited to) as follows:

* Cooperation with law enforcement and other legal bodies/services;
* Conduct cyber awareness and training events for the personnel;
* Manage **<Organisation Name>**‘s response to the press and social media;
* Take disciplinary actions if a current employee is responsible for the breach.

## **Third-party Organisations**

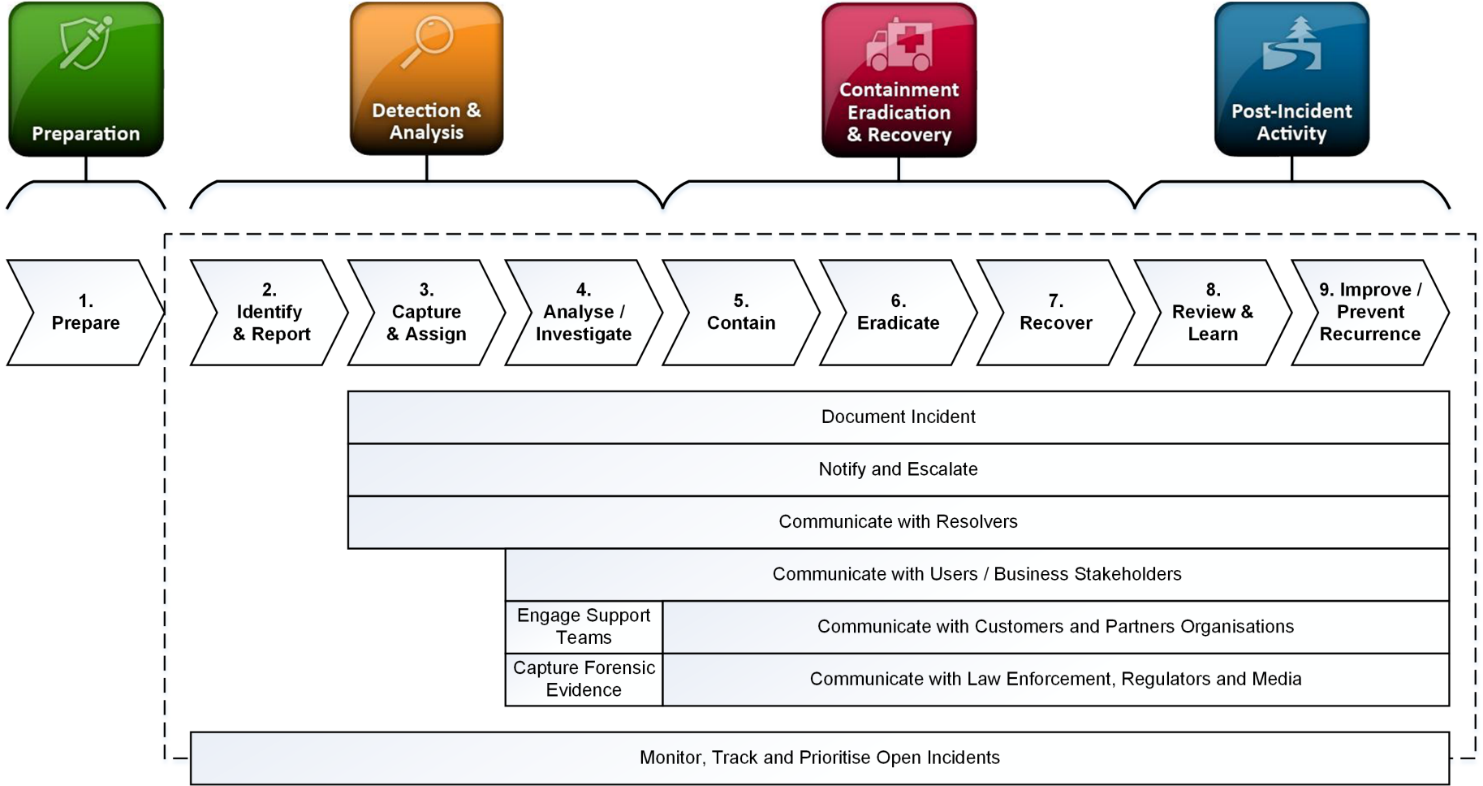
The CIRT is responsible for notifying third-party entities (organisations, customers, etc.) regarding all **<Severity Level/s >** severity incidents where a severe breach of sensitive data is leaked – i.e., account data, payment information, personal information. This also applies to cases where an adversary has lost or altered data. Examples of such incidents are:

* DDoS attacks affecting the DNS;
* Vulnerabilities in software purchased from third-party software vendors;
* Loss, leakage (keyloggers, breach) or alteration of staff and customers' data such as name, address, phone number, etc.

Various service providers such as ISP, DNS management, Penetration Testing and companies with outsourced software development projects must also be notified and consulted if the situation requires additional support.

As previously mentioned, the CIRT and other responsible departments/entities must also report the situation to the appropriate authorities (Police, Government and Governmental Cyber Departments) if the incident can escalate significantly and affect networks and systems on a national scale. This includes the provision of public services, leakage of national data and disruption/destruction of national networks and systems.

# **Response Process**

The response process will follow NIST’s Incident Handling Guide (also called **SP800-61**) (Cichonski; Millar; Grance; Scarfone, 2012). The below graph (**Figure 4.1**) from the beforementioned guide will give a visual representation of the procedure.

***Figure 4.1*** *– NIST’s Incident Handling Process. (Cichonski; Millar; Grance; Scarfone, 2012)*

## **Preparation**

Planning and preparation are the keys to promptly responding to incidents and reducing their impact to a minimum. The defence of a system will be greatly improved if a well-trained team is present and provided with up-to-date documentation. All documentation (i.e., CIRP; workflows; inventory documentation; system/network logs; network and separate system configuration standards; contact information of the entities responsible for resolving the incidents) must be easily accessible and stored in a centralised location. Additionally, the following actions should be carried out to ensure the effective functioning of the Cyber Incident Response Team.

The organisation is also advised to create specific prerequisites to monitor the state of its network as this will help with quicker responses to possible incidents. Such actions can be (but are not limited to):

* Automated alerts when suspicious actions are identified (implementing IDS);
* Create baselines for various activities which cover the network, server, storage, and different applications;
* Daily review of IDS event logs;
* System backups;
* Clock synchronisation with trusted time sources (Network Time Protocol);
* Vulnerability management programs;
* Develop and maintain relationships/partnerships with governmental and third-party organisations (Law Enforcement, Insurance, Threat Intelligence, Digital Forensics, and Incident Response services). They can be used for additional support or even taking down adversaries (phishing websites, infected servers, etc.);
* Review personnel permissions based on their position.

## **Threat Intelligence**

Gathering Threat Intelligence will allow the team to understand the infrastructure of the organisation and its risks, who the potential adversaries may be, as well as their motivations and delivery methods. The information can be obtained from various sources – Cyber Defence departments of the government, Law Enforcement, and OSINT (open-source intelligence) such as security vendors and newsfeeds.

Furthermore, creating security architecture review routines and reviewing the policies for the organisation’s departments (HR, Management, etc.) will be beneficial and will ensure that a defensive structure can be thoroughly planned.

## **Training and Awareness**

Properly trained personnel are also vital for the safety of the organisation’s data and network. For this reason, awareness and training events are highly recommended for both regular employees and the CIRT. Annual recertification/training will ensure that the CIRT is well-informed about new and ongoing threats and ways to mitigate them or counter any infections. They should also be required to learn specific guidelines such as MITRE ATT&CK to become more familiar with how cyberattacks and intrusions occur. Regular staff should be informed regarding phishing campaigns and common social engineering techniques and flags (fearmongering, spearphishing, sense of urgency, poor grammar, fake email addresses) as many attackers obtain access to systems after employees provide them with login credentials or run suspicious files.

**<Organisation Name>**‘s Human Resources department must maintain a strict record of the staff’s security training to ensure that all personnel are properly instructed.

Together with the training and exercises, **<Organisation Name>** should carry out appropriate testing programs on their systems to sustain and refine their capacity to deal with incidents. One recommended program is **NIST Special Publication 800-84 Guide to Test, Training and Exercise Programs for IT Plans and Capabilities** (Grance; Nolan; Burke; Dudley; White; Good, 2006) but others may be used to better suit the organisation. Based on the beforementioned program, the testing should include annual penetration and Red Team tests, insider threat assessment and usage of simulated scenarios to examine **<Organisation Name>**‘s incident response plan capabilities (Ransomware, DDoS, Phishing, Data theft, Lateral Movement detection, etc).

## **Identification**

It is important that the staff can properly identify the type of incident as reporting a false type would potentially result in more damages while the CIRT is attempting to mitigate and analyse the wrongly reported attack. Some of the most common incident types are provided in Table 4.2.1 below this paragraph.

|  |  |  |
| --- | --- | --- |
| № | Incident Type Name | Incident Description |
| 1 | Phishing | Phishing can have two different incidents. The first type covers personnel from the organisation who receive suspicious emails from someone who claims to be a specific individual/organisation. The second type covers third-party individuals who receive an email from someone who claims to work in **<Organisation Name>** without being a part of the organisation. |
| 2 | Social Engineering | Attempts to gain access to the **<Organisation Name>**‘s data or systems by deceiving or extorting users – customers, staff or external contractors. |
| 3 | Installation and/or execution of unknown software. | Any attempts or actual execution of unknown software on **<Organisation Name>**‘s devices. This covers both detections from anti-virus software and/or whitelisting software. |
| 4 | Loss, theft, or damage of company assets. | Any cases of loss, theft and/or damage of **<Organisation Name>**‘s data and devices. This includes removable media (external drives, USBs, etc.) and work devices (computers, IoT devices, etc.) |
| 5 | Impersonation | Any cases of account compromise/hijacking. It covers attacks on the **<Organisation Name>**‘s authentication capabilities, password sharing, suspicious login cases, accounts without a verifiable owner (zombie accounts), etc. |
| 6 | Network intrusion and enumeration | Any cases of network intrusion and probing – alerts generated by security equipment such as IDS/IPS (reconnaissance, a connection from outside devices, etc). |
| 7 | Privilege escalation | Any cases of users being moved to a group with more privileges or gaining excessive privileges through exploits or account switching. |
| 8 | Questionable use of legitimate privileges | Any case of a user abusing their privileges (accessing large amounts of data, sending data to unknown recipients, moving data to removable devices or inappropriate locations on the network). |
| 9 | Communication channel interception and service spoofing | Any cases of **<Organisation Name>**‘s data being intercepted by an unknown adversary. This includes instances of sensitive data transfers through MITM (man-in-the-middle) attacks or other means, the creation of fake websites that appear to be owned by **<Organisation Name>** or spoofing of any other services. |
| 10 | Inappropriate use of devices | Any cases of illegal activity of staff members through company assets. This includes browsing inappropriate websites, threatening/obscene/harassing communications, access/storage of illegal data and any other actions breaching the law and **<Organisation Name>**‘s policies. |
| 11 | Denial of Service (DoS) and excessive consumption | Any cases of instances where high demands are placed on specific systems that would force them to significantly slow down due to excessive bandwidth consumption or even working (crash, freeze, etc.) |
| 12 | Unlisted types | Any security events which are identified as malicious and covered by the CIRT but are not listed in the categories above. |

***Table 4.2.1*** *– Example Incident Types*

It is also important to appropriately classify the affected data (based on levels of sensitivity) as this could significantly affect the response of the CIRT. The team should review any data classification guidance provided by the government of their country. The provided example below covers the guidance of the UK’s government which splits the classification into three major categories – official, secret, and top secret:

* **Official** – Most data created and processed in and by the public sector (such as business operations and other information), which can be lost, stolen, or illegally published but will not result in a heightened threat profile. A limited part of such data can be considered more damaging when published online (Governmental figures and/or government data). Such information is classified as **Official–Sensitive**.
* **Secret** – Very sensitive data which could harm military capabilities, investigation or serious organised crimes or even public/international relations.
* **Top Secret** – The Government’s most sensitive data which requires the highest levels of protection from threats. Compromise of such intel could lead to loss of life and threats to the economy of the UK and other friendly nations.

Classification standards may vary in each country and organisations should comply with their laws and conventions.

## **Incident Reporting**

The successfully identified incident type and affected information should be reported to the appropriate entities. It is important that the staff can collect data to the greatest of their extent as it will set the priority of the incident and identify whether it should be reported to the authorities and if **<Organisation Name>** will require coordination with law enforcement or other third-party organisations. Some of the most valuable information about incidents is – the contact information of the individual/s reporting the incident, the type of the incident, hostnames and IP addresses of suspected systems, the type of affected data with its potential impact on other businesses/the country and a description of the activity with evidence (IDS logs, suspicious activity, phishing emails, etc.)

When the above information is obtained and forwarded, the **<Organisation Name>** can assign a priority to the cyber incident and then decide whether it is a cyberattack even which should be referred to the **CIRT** and any other affected entities.

In countries complying with the GDPR (Article 13), the appropriate entity (ICO for the United Kingdom) must be informed within 72 hours of the discovery of an incident which creates a “risk to the rights and freedoms of the involved parties”. The **<CIRT/Responsible staff member>** will determine if there is any data breach which requires it to be reported to a Data Protection Regulation organisation. If a decision to report the incident has been made, the following data must be provided:

* Contact data of the responsible staff member if more information is required;
* Description of the nature of the incident and an approximate number of affected individuals, as well as implications of the data breach;
* Description of any countermeasures and mitigation of adverse effects.

If the incident meets the requirements of local authorities, law enforcement and the appropriate governmental Cybersecurity department will be informed and offer any support where appropriate. The decision will be taken by the responsible staff member and can be reported even if the requirements are not met but a severe risk still exists.

## **Analysis and Assessment**

The Core IT CIRT is required to perform an initial triage of any identified and suspected incidents to confirm their validity and potential implications of the cyber incidents. The first classification may be altered with the development of the investigation as obtaining more details may reveal additional capabilities or implications of the attack. As mentioned in the previous section, all incidents must be reported to the assigned department, which will then in turn give an initial priority based on the information and send all intel to the CIRT members.

In the event of a received alert, the Core CIRT must research the incident by rapidly collecting data and performing an initial analysis of the situation. Those actions aim to acquire further information regarding the event, determine its classification, and estimate the severity. The first Incident Responder (initial individual/entity to receive the alert) should conduct this initial triage and provide the beforementioned intel (classification and severity) to the incident manager. Any false positive cases should be properly documented and/or closed according to the appropriate incident-tracking procedures of the organisation. If an event meets a certain severity score of **<Severity scores>** (an example will be provided with **medium**, **high,** and **critical**), the incident must be escalated to the entirety of the CIRT to take further actions in countering the attack.

## **Severity Assessment**

One of the best ways to identify the criticality of an incident and its implications is by using a risk matrix. To create the matrix, this CIRP will use threat levels (threat types in hierarchical order based on their severity) and criticality levels (importance of systems/information in hierarchical order). Both can be found in descending order in **Table 4.4.1** and **Table 4.4.2** respectively. The tables are based on the examples in the Scottish Cyber Incident Response Plan Template.

|  |  |
| --- | --- |
| Threat Levels | Description |
| Threat 1 | Full compromise controlled by a human:   * External personnel without appropriate authorisation (cyber intrusion). * External stakeholders with inappropriate authority. * Internal staff exceeding intended authority.   Close-Access Breach (physical penetration of a site)   * Fake Wi-Fi network. * Router pivoting (redirection of traffic). |
| Threat 2 | Partial compromise controlled by a human:   * External personnel without appropriate authorisation (cyber intrusion). * External stakeholders with inappropriate authority. * Internal staff exceeding intended authority. |
| Threat 3 | Automated full compromise controlled by malware |
| Threat 4 | Automated partial compromise controlled by malware |
| Threat 5 | DoS (Denial of Service, affecting connectivity) |
| Threat 6 | Directed Scanning (vulnerability and open port identification) or malware not controlled by a command and control server. |

***Table 4.4.1*** *– Threat types converted to levels based on the Scottish CIRP Template.*

|  |  |
| --- | --- |
| Criticality Levels | Description |
| Criticality 1 | Enterprise-Wide Resources (Vital Services, Network Devices, DNS, Firewall. etc.). |
| Criticality 2 | Critical Data – Confidential Data (Intellectual Property, Blueprints, etc.). |
| Criticality 3 | Critical Systems (AD Servers, Web Services, etc.). |
| Criticality 4 | Sensitive Data – Restricted Data (Corporate Information, Financial Documentation, User Data, etc.). |
| Criticality 5 | Non-Critical Systems (File Servers and other systems that are not vital for the organisation’s workflow). |
| Criticality 6 | Regular Data and Separate Systems. |

***Table 4.4.2*** *– Criticality levels based on the Scottish CIRP Template.*

The threat and criticality levels provided above are examples and can be altered to **<Organisation Name>**‘s needs. When the two components are created and thoroughly discussed, their impact can then be shown with the help of a **risk matrix**. The incident’s severity can be assessed when the separate components are placed in the matrix provided below (**Table 4.4.3**). This will provide the CIRT with an estimate of the attack’s severity.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Criticality Level | Threat Level | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | Critical | Critical | Critical | High | High | Medium |
| 2 | Critical | Critical | High | High | Medium | Medium |
| 3 | Critical | High | High | Medium | Medium | Medium |
| 4 | High | High | Medium | Medium | Medium | Low |
| 5 | High | Medium | Medium | Medium | Low | Low |
| 6 | Medium | Medium | Medium | Low | Low | Low |

***Table 4.4.3*** *– Risk Matrix based on the Scottish CIRP Template.*

## **Severity Guidance**

With the following guideline, **<Organisation Name>** can categorise the severity of an incident based on the obtained intelligence and potential implications to the organisation. It will help with a critical decision point in the process of countering the attack – prioritisation of the response and its appropriate resources. The CIRT must tackle incidents based on multiple factors – the risk they pose to the organisation and its assets (both digital and physical. This section will give further information regarding the severity scores (Critical, High, Medium, and Low) from the Risk Matrix in section [**4.4.1 Severity Assessment**](#_Severity_Assessment)as well as the structure of how to determine the risk levels in **Table 4.4.4**. **<Organisation Name>**‘s assigns **<Severity Level>** to the Core CIRT (recommended level – Low), whilst **<Severity Levels>** should be handled by the entire CIRT (recommended levels – anything above Low).

|  |  |  |  |
| --- | --- | --- | --- |
| Severity Level | Impacts | | IR Characteristics |
| Critical | | Highest level of severity. The impact can potentially be catastrophic for the company and its employees, including loss of business, public trust and/or impact on its operations. The following implications are indicators of this degree of severity:   * Threat to life or physical safety of customers, public or personnel. * Significant destruction of IT assets (hardware and software). * Significant disruption of business operations for a long period. * Significant damage to **<Organisation Name>**‘s reputation. * Significant destruction of corporate capabilities. * Risks of considerable financial loss. * Loss/Leakage of confidential information. | Due to the nature of this severity level, immediate and continual action from the CIRT is required. Such incidents have the highest impacts on the organisation and involve extensive and persistent operations, which often use complex attacks that are hard to counter. This severity level will trigger the policies of the Cyber Defence Departments of the country where **<Organisation Name>** is based. Possible indicators for such incidents are:   * Potentially involving law enforcement. * Potentially involving multiple media outlets and support from multiple organisations. * **<Organisation Name>**‘s executives will have an immediate and continual interest in the incident and its development. Possible requirement for multiple levels of reporting (regulatory and/or compliance). |
| High | | Substantial impact affecting the proper operations of **<Organisation Name>**‘s business operations, public trust, and impacts on their personnel. The following impacts are indicators of this severity level:   * Large loss of confidential data, restricted information, and public confidence. * Destruction of corporate assets and capabilities with a large impact. * Substantial disruption of the normal operation process. * Large damages to the reputation. * Risk of large financial loss. | Albeit milder than the previous severity level, this one also requires the immediate attention of both the Core and extended CIRT. It may require extended work hours or even around-the-clock response activities. Such incidents have substantial negative impacts on operations and involve persistent and sophisticated attacks. Such attacks require large amounts of resources to contain, control and counter them. This level will also trigger policies from the local Cyber Defence Department. Possible indicators of this incident are:   * **<Organisation Name>**‘s executives will have an immediate and continual interest in the incident and its development. Possible requirement for multiple levels of reporting (regulatory and/or compliance). * Potentially involve law enforcement, engagement by some media outlets and support from multiple organisations. |
| Medium | | Moderate impacts on the proper functionality of **<Organisation Name>**‘s business operations and personnel. The following implications indicate this severity level:   * Some disruptions in the operations over a sustained period. * Limited loss of public trust and reputation damage. * Moderate loss/manipulation of restricted data. * Risk of moderate financial loss. * Multiple business departments and sites may be affected. | This severity level requires the notification of the extended CIRT and may involve several or most of its members. Selected members from both Core and extended CIRT may be selected to engage with the incident response. Initially may require extended work hours until the situation is contained. Such incidents have some impact on the organisation and involve attacks which require an organised effort to counteract. This severity level also triggers the policies of the local Cyber Defence Department. Possible indicators are:   * May require external support. * May involve law enforcement and a limited level of reporting. * Not likely to involve media outlets |
| Low | | Highly limited impacts on the proper functionality of the organisation and its personnel. The following implications specify this severity level:   * Limited or no disruption of business functionality. * Only one site/department is affected. * Limited or no unauthorised access to restricted intel. * No impact on reputation and public trust. * Risk of minimal financial loss. | This level is unlikely to require any response from the extended CIRT, however, some may be notified by the core CIRT if deemed necessary. It is unlikely to require extended work hours and all or most of the actions will be conducted during normal work times. It has limited to no impact on the organisation. Possible indicators are:   * Extended support and law enforcement are generally not engaged. * Regulatory reporting and involvement with media outlets are unlikely. |

***Table 4.4.4*** *– Severity Levels Example Table (*UK Cabinet Office, 2018)*.*

The following entities must be contacted in cases of severity levels above **<Severity Level>** (**Table 4.4.5**):

|  |  |
| --- | --- |
| Contact | Contact Details |
| <Local Cyber Defence Department> | Email:  Phone:  Address:  Comments: i.e., ask for specific staff title” |
| <Local Police Department> | Email:  Phone:  Address:  Comments: i.e., ask for specific staff title” |
|  |  |
|  |  |

***Table 4.4.5*** *– Entity Contact Details.*

## **Incident Containment**

The responsibility for the containment of the incident is given to the core or extended CIRT depending on the scale of the attack. This can be achieved in a multitude of ways depending on the type of infection and its capabilities. The following examples (but are not limited to) will show various ways of different cyber incidents:

* Identify systems, services, and timeframes (IP/MAC addresses, hostnames, protocols, active services, locations, user accounts and timestamps) and take appropriate actions against them:
  + Remove users from critical infrastructures;
  + Remove elevated privileges of users;
  + Stop any affected services;
  + Isolate any of the identified systems if needed.
* Isolate connections with external networks to prevent further spread.
* If required, contact specialists for help with the containment and documentation.
* Do not power off affected systems as this could alter valuable evidence
* Identify, acquire, and preserve any possible sources of evidence:
  + Live data (encrypted files, RAM, network connections);
  + Application data (temporary files, emails, images, swap, and hibernation files);
  + Logs (event, network traffic, Anti-virus);
  + Electronic documents (databases, PDF files, presentations, documentation);
  + Mobile phones (call logs, contacts, emails, SMS, and appropriate application data);
  + Storage media (HDD/SSD, USB, MicroSD cards, etc.);
  + Metadata (dates, authors, access/creation/alteration times);
  + Navigation data (GPS data).
* Documenting all actions in chronological order (i.e., Chain of Custody System):
  + Personal information of the entity collecting and analysing the data as it must be done only by trained personnel;
  + Information regarding how the actions were undertaken (acquisition, preservation, analysis, and storage);
  + Backups for forensic copies and write blockers/permissions to ensure that all data will remain untouched and safe (i.e., ACPO Guidelines) (ACPO, 2007);
  + Any changes to forensic evidence as sometimes they are required to access specific data (i.e., Phone rooting to bypass its password);
  + All evidence of a cyber incident must be secured within 24 hours.

If in doubt, further advice should be obtained from appropriate specialists such as Digital Forensic Analysts in third-party partner companies or the local police department.

## **Incident Eradication**

After containing the incident and successfully analysing the cause and how it affects **<Organisation Name>**‘s assets and workflow, the core or extended CIRT (depending on the scale and severity) must eradicate the incident. It can be achieved in multiple ways depending on the type and cause of the incident. The following examples (but are not limited to) can be used to eliminate the cyberattack:

* Address the incident symptoms and correct them:
  + Malware infection:
    - Identify the type of malware;
    - Counter any capabilities of the malicious software (encryption, data leakage, data destruction, backdoor functionalities)
    - Attempt to find and eradicate any persistence mechanisms
    - Attempt to halt any propagation mechanisms
    - If hit by ransomware, consult third-party organisations regarding the risks of attempting decryption and possible data leakage/destruction;
    - If a Trojan horse is present, identify the backdoor it has created and stop it to prevent adversaries from accessing the network.
* Manual attack by an adversary (using the Pyramid of Pain (Bianco, 2013) or the Diamond Model (Caltagirone; Pendergast; Betz, 2013)):
  + - Try to identify the attacker and any leads towards them or other systems they may be using
    - Find network and host artefacts related to the attack (installed software, altered files, file transfer, scan logs, etc.)
    - Identify their capability capacity and the adversary’s arsenal – what tools were used and what vulnerabilities/exposures allowed the exploitation of the network;
    - Identify the TTPs (Tactics, Techniques and Procedures) used by the adversary (i.e., MITRE ATT&CK) (MITRE, 2018) to show all steps taken by the attacker to compromise the system.
    - Make appropriate corrections (vulnerability patches, closing any backdoors, cooperating with other companies which may be affected by the attack, i.e., the attacker uses their servers)
* Address the root cause of the issue to prevent immediate reoccurrence:
  + Change network rulesets;
  + Change the IP address/network segment of the infected machines to prevent further spread;
  + Constrain access to valuable data to users who need it for the normal operation of the organisation.
* Create own or use third-party Cyber Incident Response Playbooks (CIRP) as they provide eradication actions for specific attacks and malware infections based on the industry and key stakeholders – e.g., Singapore Shipping Association (SSA, 2018) CIRP.

## **Incident Recovery**

Once the core or extended CIRT confirms that the attack has been eradicated, **<Organisation Name>** can take action for the recovery of its operations back to a pre-incident state. It is still recommended to carefully monitor the network and its hosts (and their appropriate behaviour or services) to ensure that all vulnerabilities have been patched and that no traces of the incident remain. The following recovery actions (but are not limited to) can be taken:

* Restart stopped services after applying the newest security patches;
* Confirm host and application behaviour is benign;
* Conduct further vulnerability scans if the CIRT considers such as appropriate;
* Ensure performance (separate host performance and network bandwidth) remain unaffected as in the pre-incident state;
* Provide appropriate access to all personnel/customers to the data they are expected to access;
* If traffic was switched to a backup network, revert it to the main network.

## **Further Awareness and Reporting**

The CIRT is required to create an incident report for every cyberattack the organisation has encountered. The incidents must be thoroughly reported (including acquisition, analysis, eradication, and recovery) and must be reviewed within **<Time Frame>** after the incident’s resolution. It is recommended to review all previous incidents in meetings with the Chief Information Security Office of the organisation every **<Time Frame>** to ensure that everything is kept up to date and appropriate actions will be taken to prevent future incidents with similar attack vectors and/or react in a significantly faster manner. Such reviews are highly important to both the business itself and its CIRT because they can improve its systems and procedures and reduce the impacts of incidents. All third-party entities also involved in the resolution of the incident should be considered and included in the report.

The Incident Response Report should include the following:

* Time and means of the initial detection and the initial classification;
* List of notified people;
* List of people actively working on the incident;
* Concise timeline of the actions taken by the CIRT;
* Positive and negative points of the response (what should continue and what should stop/be improved);
* Was any internal/external escalation required? (i.e., Governmental organisations or law enforcement);
* Was there any legal action? Any prosecution will take more than the specified time frame for review after the incident was resolved and initial data regarding the legal action must be included;
* Estimated costs of the incident (partial details included) – damages, legal costs, loss of revenue, fines, etc.;
* Awareness of how the incident occurred and recommendations for policy, procedure, and system improvements;
* Review documentation of past incidents and wargames to identify how the current procedure can be improved for future defence;
* Implementation plans of the recommended improvements.

After the publication and discussion of the Incident Report, **<Appointed Entity>** should relay the information to the executives and seek feedback on the report’s content. Additionally, they should confirm if the recommendations in the report are viable and discuss appropriate funding with the executives and/or the company’s Chief Information Security Officer. Further responsibilities (but are not limited to) are:

* Identification of approximate costs and duration of all viable proposed changes;
* Identify who is responsible for carrying out the changes and its target date;
* Review the funding route for each recommendation;
* Notify **<Responsible person or CISO>** if any recommendations are accepted/rejected and/or if risks of them not being funded;
* Monitor the progress of the changes and request frequent reports from **<Responsible Person or CISO>**;
* Create Wargames – synthetic attack/infection simulations which the Risk Management and CIRT can use to train for similar situations;
* Consider sharing awareness regarding the incident with third-party entities such as law enforcement, governmental departments, external partners, etc.

# **References**

CM Alliance (2015 – Present Day). *Cyber Incident Response Plan Template*. [online] Available at: https://www.cm-alliance.com/cyber-incident-response-plan-template [Accessed 29 Oct. 2022].

Scottish Government (2021). *Cyber resilience: incident management*. [online] Available at: https://www.gov.scot/publications/cyber-resilience-incident-management/ [Accessed 15 Nov. 2022].

Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. *Computer Security Incident Handling Guide*, 2(2). doi:10.6028/nist.sp.800-61r2 [Accessed 20 Nov. 2022].

Bianco, D. (2013). *Pyramid of Pain*. [online] Available at: https://www.sans.org/tools/the-pyramid-of-pain/ [Accessed 20 Nov. 2022].

Caltagirone, S., Pendergast, A. and Betz, C. (2013). *The Diamond Model of Intrusion Analysis*. [online] Available at: https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf [Accessed 20 Nov. 2022].

Singapore Shipping Association (2021). *Cyber Incident Response PLAYBOOK*. [online] SSA. Available at: https://www.ssa.org.sg/wp-content/uploads/2021/09/Cyber-Incident-Response-Playbook.pdf [Accessed 20 Nov. 2022].

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G. and Good, T. (2006). Guide to test, training, and exercise programs for IT plans and capabilities. [online] doi:10.6028/nist.sp.800-84 [Accessed 21 Nov. 2022].

UK Cabinet Office (2018). *Government Security Classifications*. [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/715778/May-2018\_Government-Security-Classifications-2.pdf. [Accessed 21 Nov. 2022].

Association of Chief Police Officers (2007). *ACPO Guidelines*. [online] Available at: https://www.npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence\_Vers%205\_Oct%202011\_Website.pdf [Accessed 22 Nov. 2022].

MITRE (2018). *MITRE ATT&CK*. [online] Available at: https://attack.mitre.org/ [Accessed 28 Nov. 2022].