cyber incident response plan

Template

# Using this document

* This document contains guidelines and examples that organisations can follow to support the development of their own Cyber Incident Response Plan (CIRP). The template is not exhaustive. Each organisation's CIRP should be tailored to its unique operating environment, priorities, resources and commitments. Some fields contain **sample text in green**. This text is for sample purposes only and should not be used as the basis of your CIRP.
* An additional CIRP toolbox is also available with checklists and templates that can be used during the development of your CIRP.

Content

[Using this document 2](#_Toc160455502)

[Authority and review 3](#_Toc160455503)

[Document control and review 3](#_Toc160455504)

[Version management 3](#_Toc160455505)

[Aims and objectives 4](#_Toc160455506)

[Standards and frameworks 4](#_Toc160455507)

[Definitions and acronyms 4](#_Toc160455508)

[Incident response process flow 5](#_Toc160455509)

[Common security incidents and responses 6](#_Toc160455510)

[Terminology and definitions 6](#_Toc160455511)

[Common threat vectors 7](#_Toc160455512)

[Common cyber incidents 8](#_Toc160455513)

[Roles and responsibilities 9](#_Toc160455514)

[Contact points for reporting cyber incidents 9](#_Toc160455515)

[Cyber incident response team (CIRT) 9](#_Toc160455516)

[Management Team (MT) 10](#_Toc160455517)

[Roles and relationships 10](#_Toc160455518)

[Communications 11](#_Toc160455519)

[Internal communication 11](#_Toc160455520)

[External communication 12](#_Toc160455521)

[Supporting procedures and roadmaps 12](#_Toc160455522)

[Supporting standard operating procedures (SOPs) 12](#_Toc160455523)

[Supporting Playbooks 12](#_Toc160455524)

[Stakeholder Notification and reporting of incidents 13](#_Toc160455525)

[Incident response process 14](#_Toc160455526)

[Detection, research, analysis and activation 14](#_Toc160455527)

[Incident classification 14](#_Toc160455528)

[questions on incident investigation 15](#_Toc160455529)

[Escalation and de-escalation 15](#_Toc160455530)

[Containment, evidence collection and remediation 16](#_Toc160455531)

[Containment 16](#_Toc160455532)

[Documentation 16](#_Toc160455533)

[Collection and preservation of evidence 17](#_Toc160455534)

[Remediation action plan 17](#_Toc160455535)

[Recovery 18](#_Toc160455536)

[Lessons learned 18](#_Toc160455537)

# Authority and review

## Document control and review

|  |  |
| --- | --- |
| **Document check** |  |
| Author |  |
| Owner |  |
| Date created |  |
| Last revised by |  |
| Last revision date |  |

.

## Version management

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date of approval** | **Approved by** | **Description of change** |
|  |  |  |  |

# Aims and objectives

Describe the purpose of your Cyber Incident Response Plan (CIRP) here.

*For example:*

*The purpose of this CIRP is to support a rapid and effective response to cyber incidents, aligned with the organisation's security and business objectives*.

*Objectives of the CIRP*

* *Provide guidance on the steps needed to respond to cyber incidents.*
* *Outline the roles, responsibilities, accountabilities and authority of staff and teams required to manage responses to cyber incidents.*
* *Outline cyber incident compliance requirements.*
* *Outline internal and external communication processes when responding to cyber incidents.*
* *Provide guidance on post-incident activities to support continuous improvement.*

# Standards and frameworks

The following referenced documents were used as inspiration to arrive at this template. The references are not dated. The latest edition of the referenced document (including any amendments) always applies here.

* [CyberFundamentals Framework](https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework) (www.cyfun.be)
* [NIST SP 800-61](https://csrc.nist.gov/pubs/sp/800/61/r2/final); Manual for handling computer security incidents
* ISO/IEC 27035-1, ISO/IEC 27035-2, ISO/IEC 27035-3 Information security incident management.
* ISO/IEC 27001, Information security, cybersecurity and privacy protection - Information security management systems - Requirements
* ISO/IEC 27002, Information security, cyber security and privacy protection

Information security management systems - Information security management measures.

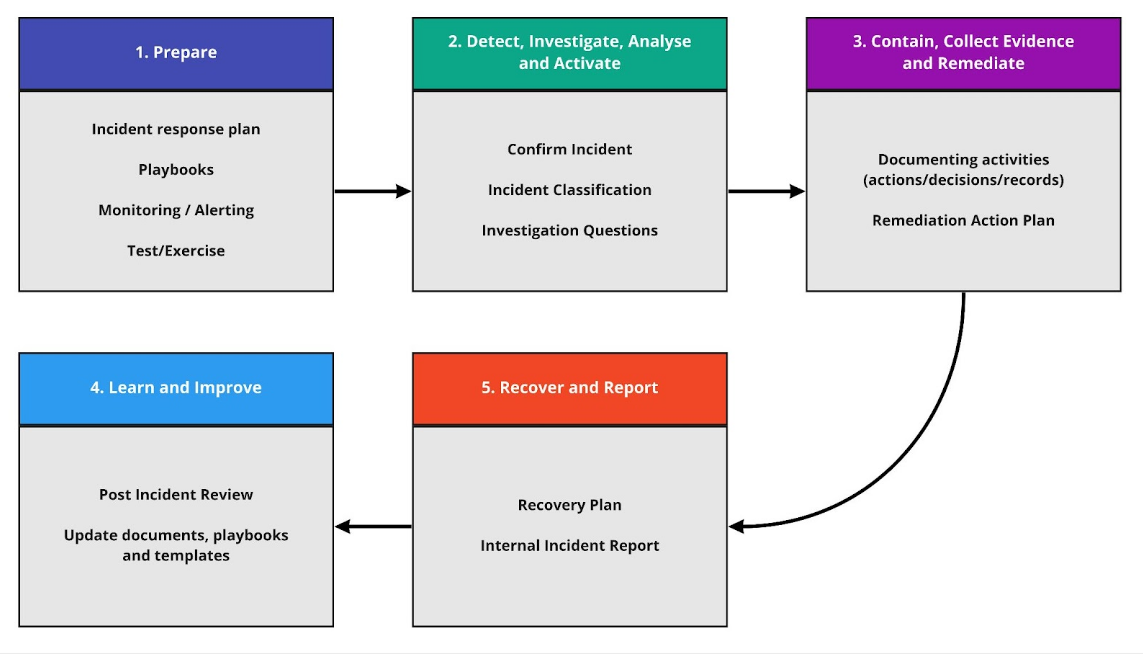
* Australian Cyber Security Centre, Cyber Incident Response plan.

# Definitions and acronyms

In this document, the terms and definitions from ISO/IEC 17000, ISO/IEC 27000 and following abbreviations apply.

|  |  |
| --- | --- |
| **CEO** | Managing director |
| **CFO** | Finance director |
| **CIO** | chief information officer |
| **CIRP** | Cyber incident response plan |
| **CIRT** | Cyber incident response team |
| **CISO** | chief information security officer |
| **COO** | chief operating officer |
| **DDoS** | Distributed denial-of-service |
| **DoS** | Denial-of-service |
| **DPO** | Data protection officer |
| **GBA** | Data protection authority |
| **ICS** | Industrial control system |
| **MT** | Management team |
| **RPO** | Recovery point Objective |
| **RTO** | Target recovery time |
| **SN** | Serial number |
| **SPOC** | Single point of contact |

# Incident response process flow



# Common security incidents and responses

## Terminology and definitions

Using consistent and predefined terminology to describe incidents and their consequences can be useful during a response. Include in your Cyber Incident Response Plan (CIRP) common terms used in your organisation. Cyber threats, events, alerts and incidents are defined as follows:

**Cyber threat**

A cyber threat is any circumstance or event that can damage systems or information. Organisations can list cyber threats of concern. the following list shows the threat environment and key cyber security trends:

* Phishing emails and scams
* Ransomware
* Abuse of security weaknesses
* Compromise on software supply chain
* Compromising business email
* Cybercrime

**Cybersecurity event**

A cyber security event is an event in a system, service or network state that indicates a possible security policy breach, security failure or a previously unknown situation that may be relevant to security. A cyber security event can become a cyber incident, but is not yet one.

Examples of cyber security events include (but are not limited to):

* A user has disabled the antivirus on his computer
* A user has deleted or modified system files
* A user restarted a server
* Unauthorised access to a server or system.

**Cybersecurity alert**

A cybersecurity alert is a notification generated in response to a deviation from normal behaviour. Cybersecurity alerts are used to highlight cybersecurity events.

**Cyber incident**

A cyber incident is an unwanted or unexpected cyber security event, or a series of such events, that has a significant probability of compromising business operations. A cyber incident requires corrective action.

Examples of cyber security incidents include (but are not limited to):

* Denial-of-service attacks (DoS)
* Unauthorised access or attempted access to a system
* Compromise of sensitive information
* Outbreak of viruses or malware (including ransomware).

### Common threat vectors

The following table contains common threat vectors from the NIST Computer Security Incident Handling Guide.

|  |  |
| --- | --- |
| **Type** | **Description** |
| **External/removable media** | An attack carried out from removable media or a peripheral device (e.g. malicious code spreading on a system from an infected USB flash drive). |
| **Failure** | An attack in which brute force methods are used to compromise, compromise or destroy systems, networks or services (e.g. a DDoS intended to impede or deny access to a service or application or a brute force attack against an authentication mechanism, such as passwords). |
| **Web** | An attack carried out from a website or web-based application (for example, a cross-site scripting attack used to steal credentials or a redirection to a site that exploits a vulnerability in the browser and installs malware). |
| **Email** | An attack carried out via an e-mail message or attachment (e.g. exploit code disguised as an attached document or a link to a malicious website in the body of an e-mail). |
| **Interdiction in the supply chain** | An antagonistic attack on hardware or software using physical implants, Trojans or backdoors, by intercepting and modifying goods in transit from the vendor or seller. |
| **Imitation** | An attack in which something benign is replaced by something malicious (e.g. spoofing, man in the middle attacks, rogue wireless access points and SQL injection attacks are all related to impersonation). |
| **Improper use** | Any incident resulting from violation of an organisation's acceptable use policy by an authorised user, excluding the above categories (e.g. a user installs file-sharing software, resulting in loss of sensitive data). |
| **Loss or theft of equipment** | Loss or theft of a computing device or medium used by an organisation (e.g. a laptop, smartphone or verification token). |

### Common cyber incidents

The following table lists common types of cyber incidents and the corresponding initial response activities.  
 Briefly describe the initial response to the incident. For example: notify relevant people, isolate affected devices, follow relevant playbooks and procedures.

|  |  |
| --- | --- |
| **Type/Description** | **Response** |
| **Denial of Service (DoS) and Distributed Denial of Service (DDoS):** flooding a service with traffic, sometimes affecting availability. | *As described in playbook X and procedures....., first take local actions to solve the problem.*  *If this is not effective, according to XYZ, ask permission to escalate to the second line, etc.* |
| **Phishing:** misleading messages to elicit sensitive information from users (such as bank logins or business login details) or to execute malicious code to enable remote access. | *If successfully identified by staff as harmful content…*  *training, warn and give copy to security officer.*  *Outline next actions and other external and internal notification actions, etc*. |
| **Ransomware:** a utility used to lock or encrypt victims' files until a ransom is paid. |  |
| **Malware:** a Trojan horse, virus, worm or other malicious software that can damage a computer system or network. |  |
| **Data breach:** unauthorised access to and disclosure of information. |  |
| **Industrial Control System compromise:** unauthorised access to ICS. |  |

# Roles and responsibilities

This section details the roles and responsibilities of key individuals and teams responsible for incident response and decision-making, including the Cyber Incident Response Team (CIRT) at the operational level and the Management Team (MT) at the strategic level.

All staff listed here should be familiar with their responsibilities in this plan and practice their response.

### Contact points for reporting cyber incidents

Primary and secondary (back-up) internal contact points to report cyber incidents during a 24/7 period.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Opening hours** | **Contact details** | **Title** | **Responsibilities** |
| *John Doe* | *09:00-18:00* | *Mobile phone number,* | *Primary contact in case of an incident* | *SPOC* |

### Cyber incident response team (CIRT)

Include details of the CIRT responsible for managing responses to cyber incidents. The composition of your CIRT will vary depending on the size of your organisation and the skills and resources available. Include details of external suppliers providing or managing your ICT systems/applications. If applicable, include details of your external incident response providers and the services they provide.

CIRT members responsible for managing responses to cyber incidents:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Organisation Role** | **Contact details** | **CIRT role Title** | Responsibilities CIRT |
|  |  |  | *Cyber incident manager* | *Scheduling of responses*  *CIRT operations* |
|  |  |  | *network engineers,* |  |
|  |  |  | *system administrators,* |  |
|  |  |  |  |  |
|  |  |  |  |  |

For more significant cyber security incidents, the CIRT can be expanded:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Organisation Role** | **Contact details** | **CIRT role Title** | **Responsibilities CIRT** |
|  |  |  | *Communications manager* | *Information and warnings*  *Internal communication* |
|  |  |  | *Legal advisor* | *Legal advice*  *(incl. regulatory compliance)* |
|  |  |  |  |  |

### Management Team (MT)

Significant cyber incidents may require the formation of the MT to provide strategic oversight, direction and support to the CIRT, focusing on:

* Identify and manage strategic issues
* Stakeholder engagement and communication (including contact with administration and ministries, if   
  applicable)
* Demand for resources and capabilities (including urgent logistical or financial requirements and personnel considerations during the response effort).

MT members responsible for managing responses to cyber incidents:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Contact details** | **Title** | **MT Role** |
|  |  | *CEO* | *Chair* |
|  |  | *CIO* | *Deputy chairman* |
|  |  | *CISO* | *Security alert and monitoring of CIA* |
|  |  | *COO* | *Operational functions of the company* |
|  |  | *CFO* | *Emergency purchases and expenditure monitoring* |
|  |  | *Legal council* | *Regulatory compliance, cyber insurance* |
|  |  | *Communications manager* | *Public relations and stakeholder engagement* |
|  |  |  |  |

### Roles and relationships

The following diagram shows the relationship between key staff and teams involved in the response.



# Communications

During incident response, there is a constant need for information from many different stakeholders. Each of them will need a different type of information. Make your own list of potential stakeholders and make sure the right contact information is available! Note that the organisation should have this contact information available, but does not always need to communicate with all parties.

Organisations should bear in mind that once a party is notified, they will ask for periodic updates regarding the incident in question. There is usually no one-off communication and the communication schedule should take into account these periodic updates.

The first step in your incident-specific communication plan is to determine with whom you will communicate. To do this, you need to determine which potential stakeholders may be (adversely) affected by the cyber security incident you are facing and whether you are legally required to notify certain entities.

* Internal stakeholders: top management, affected managers, employees
* External stakeholders: media, customers, suppliers, other partners, etc.
* Official stakeholders: GBA, sector supervisor, police,....

When deciding what to communicate and with whom, a good rule of thumb is to communicate only on a need-to-know basis. There will be stakeholders with whom you want to communicate to contain the cybersecurity incident, and there will be stakeholders with whom you need to communicate because they are asking you for information (e.g. the media) or because you are legally obliged to inform them.

### Internal communication

*Guidance:*

In addition to regular situation reports, it may be necessary to inform employees of your organisation about a cyber incident. This is important if the organisation's IT networks, operating systems or applications stop working as expected, or if the situation could generate media or public interest.

Key messages for employees include

* What happened and why?
* What will happen in the near future?
* What is expected of employees?
* Who can employees contact if they have questions?

### External communication

*Guidance:*

Depending on the impact and severity of a cyber incident, it may be necessary to communicate with external stakeholders (including ministers, media and the public). This is especially important if the incident affects IT networks, control systems or applications that third parties rely on, such as websites or services for the public.

Important messages to consider when communicating with external stakeholders include:

* What happened and why?
* Which systems/services are affected?
* What steps are being taken to resolve the situation?
* Is it possible to say when the situation will be resolved?
* What is expected from external stakeholders?
* Who can external stakeholders contact if they have questions/concerns?

**All communications must be reviewed and approved by *the Communications Manager and the Incident Manager* before release.**

# Supporting procedures and roadmaps

### Supporting standard operating procedures (SOPs)

The Standard Operating Procedures (SOPs) available to support incident response:

* *Detection, triage and analysis of events*
* *Business continuity plan*
* *Disaster Recovery Plan.*

### Supporting Playbooks

The available playbooks provide step-by-step guidelines for responses to common incidents:

* *Cybersecurity incident response plan -* ***Phishing***
* *Cybersecurity incident response plan* ***- data intrusion/theft***
* *Cybersecurity incident response plan* ***- Malware***
* *Cybersecurity incident response plan* ***- Ransomware***
* *Cyber Security Incident Response Playbook* ***- Denial of Service.***

# Stakeholder Notification and reporting of incidents

Processes for internal and external notification and reporting of incidents include:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type of incident/**  **threshold** | **Organisation  wishing to  receive  a notification  or report** | **Contact details  of the notifying organisation.** | **Key notification and reporting requirements and link to organisational information** | **Responsible staff** |
| Ransomware | Centre for Cybersecurity Belgium. CERT.BE | info@ccb.belgium.be | https://www.cert.be/en/report-incident-0 | Cyber incident manager |
| Breach of personal data | Data protection authority | +32 (0)2 274 48 00  +32 (0)2 274 48 35  contact@apd-gba.be | https://www.gegevensbeschermingsautoriteit.be/professioneel/acties/datalek-van-persoonsgegevens | Legal counsel or DPO |

* **list the legal and regulatory requirements for your business.**
* **If there is a cyber insurance policy, check the requirements in the policy to make sure you comply.**

# Incident response process

# Detection, research, analysis and activation

Refer to your own standard operating procedures for detecting, investigating and analysing incidents. These may include how you become aware of an event or incident and what you do immediately in response.

Incidents can be detected in various ways, including but not limited to:

* Self-detected incidents (e.g. Intrusion Detection and Prevention systems)
* Receiving notifications from service providers or vendors
* Reports received from trusted third parties such as the Centre for Cyber Security Belgium, MITRE ATT&CK, ENISA....

### Incident classification

This can help prioritise resources. Classification factors can be:

* Consequences of the incident (confidentiality, integrity and availability of information and systems)
* Stakeholders involved (internal and external)
* Type of incident
* Impact on business and community.

|  |  |
| --- | --- |
| **Classification of incidents** | **Descriptions** |
| **Critical** | *A critical incident with a very high impact. It often involves a complete system failure, loss of customer data, major security breaches or critical infrastructure failures.* |
| **High** | *A major incident with significant impact. It can include partial system failures or affect critical functionalities.* |
| **Medium** | *A moderate impact incident that may affect non-critical functionality or cause inconvenience to users.* |
| **Low** | *A small low-impact incident that may consist of non-critical function failures or low-priority user complaints.* |

### questions on incident investigation

A list of investigation questions can help you in your efforts to respond to an incident and to understand the scope and impact of the incident. Not all questions can be answered with the available data, and questions may change as the investigation progresses.

* *Who discovered or reported the incident?*
* *When was the incident discovered or reported?*
* *Where was the incident discovered or located?*
* *What impact does the incident have on operations?*
* *What is the extent of the network and applications incident?*

### Escalation and de-escalation

Cyber incidents can be escalated or de-escalated. The roles that can escalate or de-escalate should be tabulated.

|  |  |  |  |
| --- | --- | --- | --- |
| **Classification of incidents** | **Action** | **Reason for escalation/de-escalation** | **Decider** |
|  |
| **Critical** | De-escalating to high |  |  |  |
| **High** | Escalating to criticism |  |  |  |
| De-escalating to average |  |  |  |
| **Medium** | Escalating to high |  |  |  |
| De-escalating to low |  |  |  |
| **Low** | Escalating to average |  |  |  |

# Containment, evidence collection and remediation

### Containment

Containment is important before an incident overwhelms resources or increases damage. Most incidents need containment, so this is an important consideration early in the handling of any incident. Containment provides time to develop a tailored recovery strategy. An essential part of containment is decision-making (e.g. shut down a system, disconnect from a network, disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident. Organisations should define acceptable risks when dealing with incidents and develop strategies accordingly.

Containment strategies vary depending on the type of incident. For example, the strategy for containing a malware infection via e-mail is very different from that for a DDoS attack over a network. Organisations should prepare separate containment strategies for each major incident type, with clearly documented criteria to facilitate decision-making. Criteria for determining the right strategy include:

* Possible damage to and theft of resources
* Preservation of evidence
* Availability of services (e.g. network connectivity, services provided to external parties)
* Time and resources needed to implement the strategy
* Effectiveness of the strategy (e.g. partial containment, full containment)
* Duration of solution (e.g. emergency solution to be removed within four hours, temporary solution to be removed within two weeks, permanent solution).

In some cases, some organisations redirect the attacker to a sandbox (a form of containment) so that they can monitor the attacker's activities, usually to gather additional evidence. The incident response team should discuss this strategy with the legal department to determine whether it is feasible. Ways of monitoring an attacker's activities other than sandboxing should not be used; if an organisation knows that a system has been compromised and allows the compromise to continue, it may be held liable if the attacker uses the compromised system to attack other systems. The delayed containment strategy is dangerous because an attacker can escalate unauthorised access or compromise other systems.

Another potential problem related to containment is that some attacks can cause additional damage when contained. For example, a compromised host may run a malicious process that periodically pings another host. When the incident handler tries to contain the incident by disconnecting the compromised host from the network, subsequent pings will fail. As a result of this failure, the malicious process may overwrite or encrypt all data on the host's hard disk. Handlers should not assume that just because a host has been disconnected from the network, further damage to the host has been prevented.

### Documentation

Documenting all related information about the incident is essential. The following list is an indication of relevant information that should be documented. If reports are made for management or other stakeholders, this information should be in the report.

* Date and time of incident
* Current status of the incident
* Contact details of relevant persons (incident manager, CISO, CEO, ....)
* Scope and impact
* severity
* Incident type and classification
* Need external help? YES / NO. Please include contact details.
* Actions taken to contain and resolve the incident.
* Information about the next incident update (date, time, who will be informed)

### Collection and preservation of evidence

When collecting evidence, keep a detailed log that clearly documents how all evidence was collected. This should include who collected or handled the evidence, when the evidence was collected and handled, and details of each item collected (including physical location, serial number, model number, hostname, log files, IP address, operating system, ....).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date, time of collection** | **Collected by** | **Evidence Details** | **Location of evidence** | **Access** |
| *01/01/2024* | *Mr Janssens* | *Laptop hard disk with SN, model no.* | *Disc with SN....*  *Stored in safe in server room* | *ICT manager, CIRT team* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Remediation action plan

Establish an action plan to resolve the incident, following successful containment and evidence collection.

When preparing the recovery action plan, consider the following questions. These questions are not limited, only indicative.

* What actions are needed to resolve the incident?
* What resources (internal & external) are needed to resolve the incident?
* Who owns the incident being resolved?
* Is there a priority for systems or services needed to resolve the incident?
* Who and what does the resolution affect?
* What is the timetable for closing the incident?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date, time of incident** | **Category**  **(Controlling, recovering,...)** | **Action** | **Action owner** | **Status**  **(not assigned, being worked on, closed)** |
| *01/01/2024* | *Contains* | *Disconnect the infected host from the network.* | *System administrator (including name)* | *In progress* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Recovery

Create recovery plans for different scenarios. The recovery plan should detail the approach to restore IT and/or OT networks, systems and applications once containment and remediation is complete.

When developing a recovery plan, keep the following in mind:

* The Recovery Time Objective (RTO) & Recovery Point Objective (RPO).
* Create a process for monitoring the systems to ensure they are no longer compromised and working as expected.
* What can be implemented to prevent similar incidents?

# Lessons learned

One of the most important parts of incident response is also most often skipped: learning and improvement. Every incident response team must evolve to reflect new threats, improved technology and lessons learned. Holding a "lessons learned" meeting with all involved parties after a major incident, and possibly periodically after smaller incidents if resources allow, can be very helpful in improving security measures and the incident response process itself. Multiple incidents can be discussed during one "lessons learned" meeting. This meeting provides an opportunity to conclude an incident by discussing what happened, what was done to intervene and how well the intervention worked. The meeting should be held within a few days of the end of the incident.

Questions to be answered at the meeting include:

* What exactly happened and at what times?
* How well did staff and management handle the incident? Were the documented procedures followed? Were they adequate?
* What information was needed earlier?
* Have any steps or actions been taken that may have hindered recovery?
* What would staff and management do differently if a similar incident occurred next time?
* How could information sharing with other organisations have been improved?
* What corrective measures can prevent similar incidents in the future?
* What precursors or indicators should be watched for in the future to detect similar incidents?

Lessons learned meetings have other benefits. Records of these meetings are good material for training new team members by showing them how more experienced team members respond to incidents. Updating incident response policies and procedures is another important part of the learning process. A post-mortem analysis of how an incident was handled will often reveal a missing step or an inaccuracy in a procedure, prompting change. Due to the changing nature of information technology and changes in personnel, the incident response team should periodically review all related documentation and procedures for handling incidents.

**Regular testing of the Cyber Incident Response Plan is important to ensure that these documents remain current and known to relevant personnel. Testing methods could include discussion or functional exercises.**

**Cyber Incident Response Plan training exercises of different scenarios are of great value to get more and more information from the lessons learned. During these test scenarios, a lot of information can be missing or processes are not executed as defined. These are great outcomes so you can adjust procedures and processes for when you really need the cyber incident response plan!**