CENTRE FOR
CYBERSECURITY
BELGIUM

CYBER INCIDENT RESPONSE PLAN

TEMPLATE

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Using this document

- This document contains guidelines and examples that organizations can follow to support the development of their own Cyber Incident Response Plan (CIRP). The template is not exhaustive. Each organization'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 for your CIRP.

- An additional CIRP toolbox is also available with checklists and templates that can be used during the development of your CIRP.

Contents

Authority and review

DOCUMENT CONTROL AND REVIEW

Document Control	
Author	
Owner	
Date created	
Last revised by	
Last revision date	

.

VERSION CONTROL

Version	Date of approval	Approved by	Description of change

Purpose and objectives

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

For example:

The goal of this CIRP is to support a rapid and effective response to cyber incidents, aligned with the organization'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 personnel 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 (www.cyfun.be)
- ✓ NIST SP 800-61; 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, cybersecurity and privacy protection Information security management systems - Information security management measures.
- ✓ Australian Cyber Security Center, Cyber Incident Response plan.

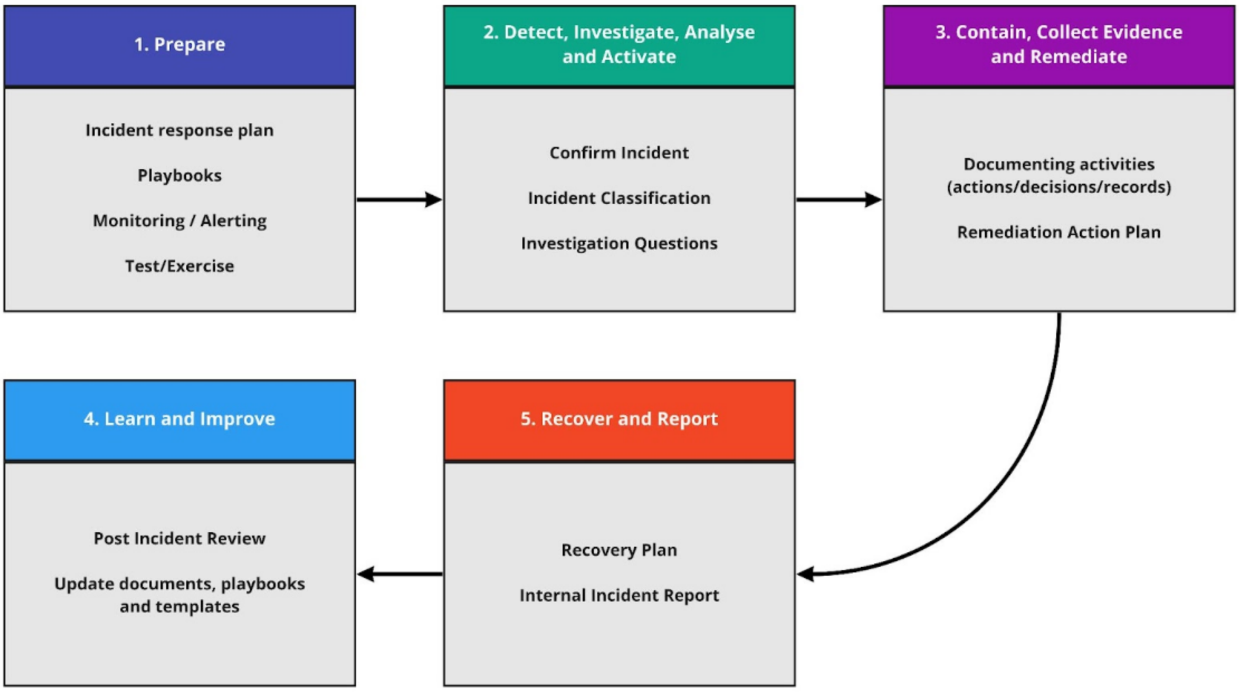
Definitions and acronyms

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	One 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 helpful during a response. Include in your Cyber Incident Response Plan (CIRP) common terms used in your organization. Cyber threats, events, alerts and incidents are defined as follows:

significant incident	Any incident that significantly affects the provision of any of the services in the sectors or subsectors listed in Annexes I and II of the Act and that: ✓ Has caused or may cause serious operational disruption to any of the services in the sectors or subsectors in Annexes I and II or financial losses to the entity concerned; or ✓ Affected or may affect other natural or legal persons by causing significant material or immaterial damage.
near-incidents	an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by or accessible through network and information systems, but which was successfully prevented or did not occur;
Cyber threat	A cyber threat is any circumstance or event that can damage systems or information. Organizations can include a list of 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 e-mail ✓ 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 incident can become a cyber incident but is not yet one. Examples of cybersecurity events include (but are not limited to): ✓ A user disabled the antivirus on his computer ✓ A user deleted or modified system files ✓ A user restarted a server ✓ Unauthorized access to a server or system.
Cybersecurity Alert	A cybersecurity alert is a notification generated in response to a deviation from normal behavior. Cybersecurity alerts are used to raise awareness of 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 cybersecurity incidents include (but are not limited to):

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

COMMON THREAT VECTORS

The following table lists 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 that uses brute force methods to compromise, compromise or destroy systems, networks or services (e.g., a DDoS designed 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 performed from a Web site or Web-based application (for example, a cross-site scripting attack used to steal credentials or a redirection to a site that exploits a browser vulnerability and installs malware).
Email	An attack carried out through 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 altering goods in transit from the vendor or seller.
Imitation	An attack in which something benign is replaced by something malicious (for example, 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 organization's Acceptable Use Policy by an authorized 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 organization (e.g., a laptop, smartphone or verification token).

COMMON CYBER INCIDENTS

The following table provides a list of common types of cyber incidents and the corresponding initial response activities.

Briefly describe the initial response to the incident. For example: notify relevant individuals, 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 for permission to escalate to the second line, etc.*
Phishing: deceptive messages to elicit sensitive information from users (such as bank	*If identified by staff by successful malicious content training, warn and give a copy to the security officer. Outline next actions and other external and internal notification actions, etc*.

logins or business login credentials) or to execute malicious code to enable remote access.	
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: unauthorized access to and disclosure of information.	
Industrial Control System compromise: unauthorized 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 personnel listed here should be familiar with their responsibilities in this plan and practice their response.

CONTACT POINTS FOR REPORTING CYBER INCIDENTS

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

Name	Opening hours	Contact details	Title	Responsibilities
John Doe	*9 a.m.-6 p.m.*	*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 organization and the skills and resources available. Include details of external vendors that provide or manage 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	Organization Role	Contact details	CIRT role Title	Responsibilities CIRT
			Cyber incident manager	*Scheduling responses* *CIRT operations*
			network engineers,	
			system administrators,	

For more significant cybersecurity incidents, the CIRT can be expanded:

Name	Organization 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:

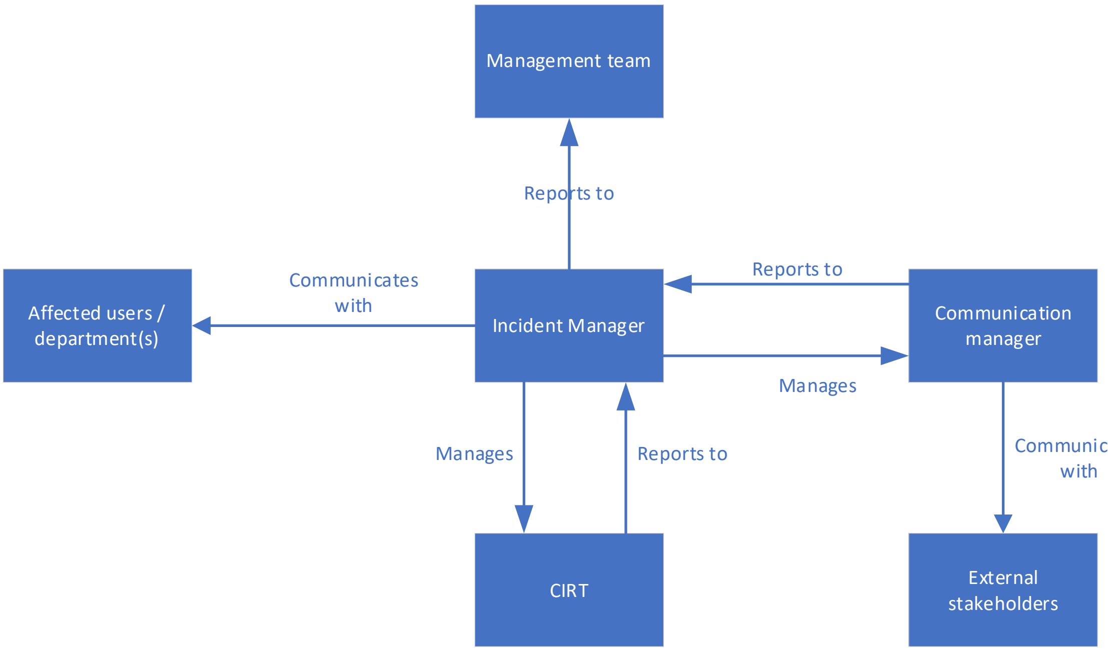
- ✓ Identify and manage strategic issues
- ✓ Stakeholder engagement and communication (including contact with administration and ministries, if applicable)
- ✓ Demand for resources and capabilities (including urgent logistical or financial requirements and personnel considerations during the response 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 personnel 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 organization should have this contact information available, but does not always need to communicate with all parties.

Organizations should keep in mind that once a party is notified, they will request periodic updates regarding the incident in question. There is usually no one-time communication, and the communication schedule must take into account these periodic updates.

The first step in your incident-specific communications plan is to determine with whom you will communicate. To do this, you must determine which potential stakeholders may be (adversely) affected by the cybersecurity 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 required by law to notify them.

INTERNAL COMMUNICATIONS

Guidance:

In addition to regular situation reports, it may be necessary to inform employees of your organization about a cyber incident. This is important if the organization'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 COMMUNICATIONS

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* prior to release.

REPORTING REQUIREMENT FOR NIS2

Essential and important entities, as defined in Chapter 4 (Art 11 & Art 12) in the Belgian NIS2 legislation, are **required** to comply with a number of requirements to report early warnings or **significant incidents*** to the national CSIRT (CERT.be).

These alerts or significant incidents should be reported to the CERT within **twenty-four hours** of their discovery. This notification shall include the following information, among others:

- ✓ Is the incident the result of a wrongful or malicious act?
- ✓ Does hot incident have cross-border implications?

Within seventy-two hours of reporting the incident, the organization -if applicable- provides a:

- ✓ Update to the above information
- ✓ An initial assessment of the significant incident, including severity and consequences.
- ✓ Indicators of degradation.

No later than one month after reporting the significant incident, a final report is prepared and forwarded to the CERT that includes the following:

- ✓ Detailed description of the incident, including severity and consequences.
- ✓ The type of threat or root cause (root cause) that likely led to the incident.
- ✓ Applied and ongoing risk mitigation measures (both technical and organizational).

- ✓ If applicable, the cross-border impact of the incident.

If the incident is still not resolved after these 30 days, a progress report will be prepared and forwarded to the CERT. A final report will be prepared and sent within one month after the incident is resolved.

In addition to the above reporting requirement, **voluntary** reports to the CERT may be made:

- ✓ *For essential and important entities*: incidents, cyber threats, near incidents.
- ✓ *Other organizations, whether or not they are in the scope of NIS2*: significant incidents, cyber threats and near incidents

Supporting procedures and scripts

SUPPORT STANDARD OPERATING PROCEDURES (SOPS).

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

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

SUPPORTING PLAYBOOKS

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	Organization wishing to receive a notification or report	Contact details of the notifying organization.	Key notification and reporting requirements and linkage to organizational information	Responsible staff
Ransomware	Center for Cybersecurity Belgium. CERT.BE	info@ccb.belgium.be	https://www.cert.be/en/report-incident-0	Cyber incident manager
Personal data breach	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 analyzing 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 a variety of ways, including but not limited to:

- Self-detected incidents (e.g., Intrusion Detection and Prevention systems)
- Receive notifications from service providers or vendors
- Notifications received from trusted third parties such as the Center for Cybersecurity Belgium, MITRE ATT&CK, ENISA....

INCIDENT CLASSIFICATION

This can help prioritize resources. Classification factors may include:

- 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 functionality.*
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.*

INCIDENT INVESTIGATION QUESTIONS

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 business operations?*
- *What is the extent of the incident with the network and applications?*

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 that 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., shutting down a system, disconnecting from a network, disabling certain functions). Such decisions are much easier to make if predetermined strategies and procedures are in place for containing the incident. Organizations must 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 email is very different from that for a DDoS attack over a network. Organizations should create separate containment strategies for each major incident type, with clearly documented criteria to facilitate decision-making. Criteria for determining the appropriate 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 organizations redirect the attacker to a sandbox (a form of containment) so 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 if it is feasible. Ways to monitor an attacker's activities other than sandboxing should not be used; if an organization knows a system has been compromised and allows the compromise to continue, it could 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 unauthorized 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 be running 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 can overwrite or encrypt all data on the host's hard drive. 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 produced for management or other stakeholders, this information should be in the report.

- Date and time incident
- Current status of the incident
- Contact details of relevant individuals (incident manager, CISO, CEO, ...)
- Scope and impact
- Ernst
- Type of incident and classification

- Need external help? YES / NO. Please include contact information.
- Actions taken to contain and resolve the incident.
- Information about the next incident update (date, time, who will be notified)

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, the time the evidence was collected and handled, and the details of each item collected (including physical location, serial number, model number, host name, log files, IP address, operating system, ...).

Date, time of collection	Collected by	Evidence Details	Location of evidence	Access
01/01/2024	*Mr. Janssens*	*Hard drive of laptop with SN, model no.*	*Disk with SN....* *Stored in safe in server room*	*ICT manager, CIRT team*

REMEDIATION ACTION PLAN

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

When creating the recovery action plan, consider the following questions. These questions are limited, indicative only.

- 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?
- On whom 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, consider the following:

- 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 permit, 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 bring closure to 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 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 previously needed?
- 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 organizations 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, providing the impetus for change. Because of 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 may be missing or processes may not be executed as defined. These are great outcomes so you can adjust procedures and processes for when you really need the cyber incident response plan!