CYBERSECURITY TOOLKIT

clearbridge

INCIDENT RESPONSE PLAN TEMPLATE

Detect, respond to, and limit the consequences of a **malicious cyberattack.**

203-2600 Gladys Ave
Abbotsford BC Canada V2S 0E9
support@clearbridge.ca
(778) 383-6726

Your incident response plan (IRP) will help you:

- Respond to security incidents effectively and efficiently
- Document the roles, responsibilities, and steps to follow
- Establish incident handling and response capabilities

Reach out to us today for assistance with understanding and using your incident response plan!

Company name:

Date:

By:

What is an incident response plan (IRP) and why do you need it?

Your business should have a formal, focused, and coordinated approach when responding to security incidents. An **incident response plan (IRP)** is an organized method that allows you to document the roles, responsibilities and steps your team will follow to identify, contain, eradicate, and recover from security incidents.

Steps include Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

Examples of security incidents include unauthorized attempts to access systems or data, insider threats, phishing attacks, malware attacks, password attacks, man-in-the-middle attacks, etc.

1 - Revision History

The incident response plan (IRP) has been modified as follows:

Date	Version	Modification	Modifier
2022-09-15	1.0	Plan created	<author>

Review Cycle

The incident response plan (IRP) must be reviewed at least annually.

2 - Purpose & Scope

Purpose

Your business IS A TARGET. Today's cybercriminals are equipped with sophisticated methods that put your data, systems, and information at risk. That's WHY you need an incident response plan (IRP). It ensures that your business is prepared to manage cyberincidents effectively and efficiently. With the right plan and team in place, your business will be better prepared to handle inevitable incidents, contain any damage made and mitigate further risk to your company. Your incident response plan will allow you to deploy resources in an organized fashion with exercised skills and communication strategies.

This document is an overall plan for responding to security incidents. It identifies the structure, roles and responsibilities, types of common incidents, and the approach to preparing, identifying, containing, eradicating, recovering, and conducting lessons learned to minimize the impact of future incidents.

The priority is to ensure your business can respond to security incidents effectively and efficiently.

Scope

The incident response plan (IRP) applies to all networks, systems, and data and impacts all internal and external stakeholders. Your business will select employees to lead or participate with the incident response team. They should familiarize themselves with the incident response plan (IRP) and be prepared to collaborate to minimize adverse impacts on your company.

This document assists the organization with establishing incident handling and incident response capabilities and determines the appropriate response for common security incidents.

3 - Authority

Responsibility for the security of information resides with the <title>. During times when a high or critical security incident is underway this responsibility is entrusted to the <title>.

4 - Definitions

Event

An event is an observable occurrence in a system or network.

Examples of events include when an employee connects to a file share, a server receives a request for a web page, or an employee sends an email.

Incident

An incident is an adverse event or the threat of the occurrence of an adverse event in an information system or network.

As a rule, an incident violates or threatens computer security policies, acceptable use policies, or standard security practices. It implies harm or the attempt to harm.

5 - Roles & Responsibilities

Internal contacts (note: every role should have a secondary and often a tertiary identified)

Role	Name	Title	Phone	Email
Incident Handler (lead)				
Incident Handler (backup)				
Incident Response (lead)				
Incident Response (backup)				
Note-taker				
Communications				
Incident Management				
Security				
Privacy				

Role	Name	Title	Phone	Email
Network				
Desktop (Windows)				
Desktop (other)				
Server (Windows)				
Server (other)				
Datacenter				
Legal				
Law Enforcement (local)				
Law Enforcement (federal)				
Human Resources				
Executive				
Executive				

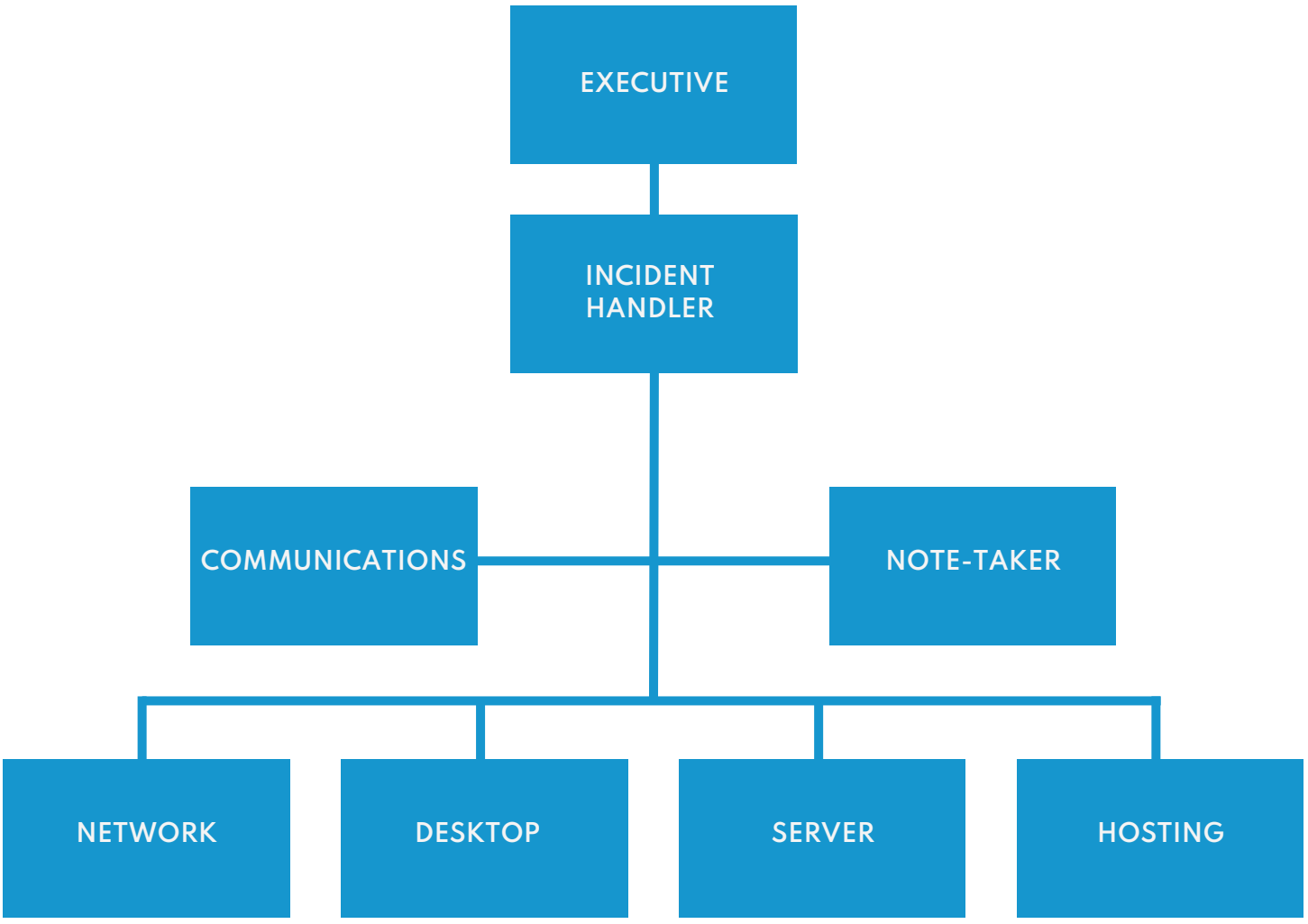
External contacts

Role	Organization	Name	Title	Phone	Email
Vendor	IR on retainer				
Vendor	IR on retainer				
Vendor	Service Provider				
Vendor	Service Provider				
Vendor	Technology Vendor				
Vendor	Technology Vendor				
Connected Organization	Peer				
Connected Organization	Peer				

Other stakeholders

Role	Organization	Name	Title	Phone	Email
Customers/clients					
Shareholders					
Board of directors					

6 - Team Structure



7 - Incident Types

Type	Description
Unauthorized Access or Usage	Individual gains physical or digital access to a network, system, or data without permission.
Service Interruption or Denial of Service	Attack that prevents access to the service or otherwise impairs normal operation.
Malicious Code	Installation of malicious software (for example a virus, worm, Trojan, or other code).
Network System Failures (widespread)	Incident affecting the confidentiality, integrity, or availability of networks.
Application System Failures	Incident affecting the confidentiality, integrity, or availability of applications or systems.
Unauthorized Disclosure or Loss of Information	Incident affecting the confidentiality, integrity, or availability of data.
Privacy Breach	Incident that involves real or suspected loss of personal information.
Information Security/Data Breach	Incident that involves real or suspected loss of sensitive information.
Other	Any other incident that affects networks, systems, or data.

8 - Severity Matrix

The incident response team has three main goals:

1 - Determine the severity of the security incident.

The team must consider whether single or multiple systems are affected.

They must determine if the situation is critical and whether it impacts single or multiple persons, the team, or the entire organization.

The team will verify if it's single or multiple business areas impacted.

It is also crucial at this stage to understand the relevant business context and what else is happening within the business at the time to assess the impacts and urgency of remediation.

2 - Consider the available information to determine the known magnitude of an impact compared with the estimated size, likelihood and rapidness of spread.

The team must determine the potential impacts on the business, whether financial damage, brand and reputational damage or other harms. The incident may be due to a sophisticated or unsophisticated threat, automated or manual attack, or could be nuisance/vandalism.

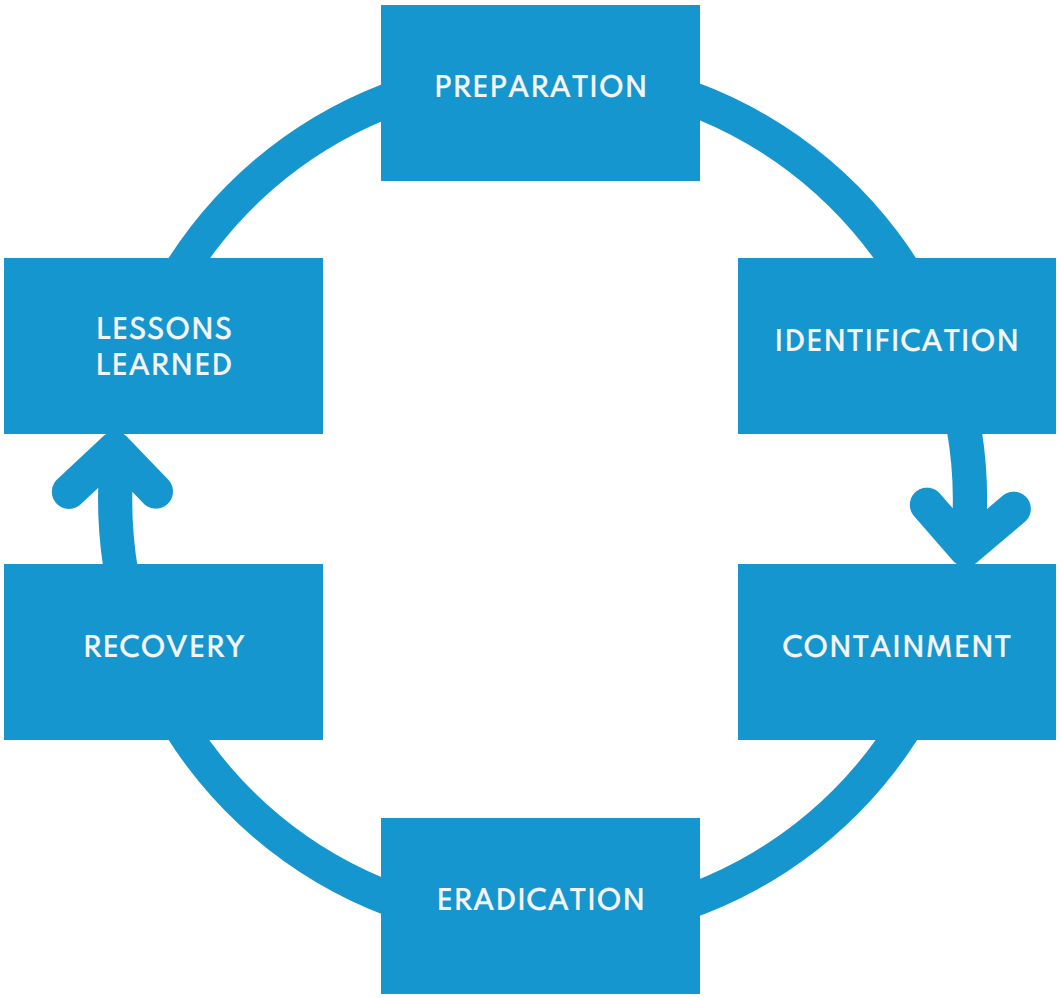
3 - Determine whether there is a vulnerability, exploit, evidence of an exploited vulnerability, or known patch.

Finally, the team will determine if this is a new threat (zero-day) or a known threat and the estimated effort to contain the problem.

Category	Indicators	Scope	Action
1 - Critical	Data loss, malware	Widespread and/or with critical servers or data exfiltration	Mitigate Take action and refine process, implement mitigation, document performance, conduct post-mortems
2 - High	Theoretical threat becomes active	Widespread	Manage Coordinate efforts, assign tasks, share incident status, report on progress
3 - Moderate	Email phishing or active spreading infection	Widespread	Assess Enrich and evaluate event against best practices, regulatory requirements, threat intelligence
4 - Low	Malware or phishing	Individual host or person	Prepare Run simulations to train the team Escalate events from existing systems

9 - Incident Handling Process

In the event of a security incident the incident response team (IRT) will adhere to the PICERL process as follows:



Preparation

- [ ] **Build an incident response plan (IRP):**
  - Establish mandate, delegate authority, and chain of command.
  - Review/update annually.
- [ ] **Ensure you have an incident response team (IRT):**
  - Dedicated, virtual, or on-retainer.
  - Provide training, as necessary.
- [ ] **Document roles and responsibilities:**
  - Delegate authority.
  - Provide training, as necessary.
- [ ] **Conduct exercises, and drills regularly:**
  - Consider that most incident types are known in advance.
  - Prepare for the known so can focus on the unknown.
  - Test the plan, team, and tools.
- [ ] **Understand the environment:**
  - Diagrams, location of critical systems and data.
  - Ensure adequate visibility into networks and systems.
  - Vendor environment.
  - Understand dependencies.
- [ ] **Understand what controls are in place:**
  - Are they sufficient to mitigate risk to an acceptable level?
- [ ] **Understand impacts:**
  - Determine maximum tolerable downtime (MTD) and acceptable interruption window (AIW).
  - Prioritized list of assets and downtime.
- [ ] **Prepare war room and/or conference bridge(s):**
  - Require a location physically or digitally to convene.
  - Ensure the location is secure and appropriately equipped.
- [ ] **Establish a communications plan:**
  - How will you inform internal and external stakeholders?
- [ ] **Establish agreements in advance:**
  - E.g. incident response on retainer.
  - Ensure annual plan review/update.
  - Regular exercises.
  - Familiarity with the environment in advance.
  - Preferred pricing.
  - Established SLA, response times.

Notification

- [ ] **Ensure a central point of contact exists for employees to report real or suspected security incidents.**
- [ ] **Ensure all employees are required to report security incidents.**
- [ ] **Ensure all employees know they are required to report security incidents and how.**
- [ ] **Ensure all employees do report security incidents in a timely fashion.**

Convene

- [ ] **Bring together those who are aware of the incident.**
- [ ] **Engage incident response team (IRT) members**
- [ ] **Remind responsible members to maintain need-to-know:**
  - Otherwise leads to managing misinformation.
- [ ] **Communicate effectively and efficiently.**
- [ ] **Convene in the war room or conference bridges:**
  - Ensure the location is secure and appropriately equipped.
- [ ] **Often more than one location is required for different needs (e.g.: management and technical team).**

Identification

- [ ] Determine whether an incident has occurred:
  - Is it an event or an incident?
  - Search for correlating information to increase confidence there is a real incident.
- [ ] Perform triage and ensure a collective understanding of how it was detected and who is aware.
- [ ] Analyze the precursors and indicators.
- [ ] Perform research (e.g.: search engines, knowledge base).
- [ ] Document investigation and evidence gathering.
- [ ] Prioritize handling of the incident based on relevant factors (functional impact, information impact, recoverability effort, etc.).
- [ ] Determine severity, urgency and initial impact.
- [ ] Review information and actions taken to date.
- [ ] Report incidents to appropriate internal personnel and external organizations.

Communication

- [ ] Create a communications plan respecting need-to-know.
- [ ] Develop a stakeholder relationship map to determine the level of stakeholder involvement.
- [ ] Ensure reported information is factually based on the evidence available at the time.
- [ ] Ensure a point of contact knows the current status at all times.

Containment

- [ ] Implement an incident response playbook (strategies and actions for future events/incidents).
- [ ] Prevent further damage by containing the incident.
- [ ] Determine the source, and what vulnerability was exploited.
- [ ] Continue impact/damage assessment and confirm incident scope.
- [ ] Determine what was changed (e.g.: files, connections, processes, accounts, access etc.).
- [ ] Acquire, preserve, secure and document evidence and preserve the chain of custody.
- [ ] Continue taking notes, ensuring a detailed log about what was found and what you did about it.

Eradication

- [ ] Eradicate the incident:
  - Remove all traces of the infection or other incidents.
  - Identify and mitigate all vulnerabilities that were exploited.
  - Remove malware, inappropriate materials, and other components.
- [ ] If more affected hosts are discovered (e.g.: new malware infections), ensure to perform the identification steps on the newly identified examples, then contain.
- [ ] Ensure the incident cannot re-occur and further understand the attack vector.
- [ ] Continue taking notes, ensuring a detailed log.
- [ ] Ensure any compromised machines are removed or formatted before placing them back into service:
  - Ensure necessary evidence has been collected.

Recovery

- [ ] Return affected systems one-by-one to an operationally ready state.
- [ ] Monitor closely to ensure the incident does not re-occur or is not still ongoing.
- [ ] Ensure systems are restored from a trusted source.
- [ ] Confirm the affected systems are functioning normally.
- [ ] Implement additional monitoring to look for future related activity if necessary.

Lessons Learned

- [ ] Hold lessons learned meeting within 2 weeks.
- [ ] Create a follow-up report.
- [ ] Walk through and review the play-by-play of the incident report:
    - How was the incident detected, by whom, and when?
    - What was the scope and severity of the incident?
    - What methods were used in containment and eradication?
- [ ] Identify opportunities for improvement to better prepare for next time.
- [ ] Ensure accountability to follow up on identified opportunities.

10 - Approvals

Responsible Party

Responsibility for the security of government information resides with the following responsible party:

Responsible Party Name and Title	Responsible Party Signature

The Responsible Party has reviewed the incident response plan (IRP) and delegates the responsibility for mitigating harm to the organization to the Incident Handler. During times when a high or critical security incident is underway this responsibility is entrusted to the Incident Handler or their delegate.

Incident Handler

The Incident Handler has reviewed the incident response plan (IRP) and acknowledges that when a high or critical security incident is underway, responsibility for managing the incident is entrusted to the Incident Handler or their delegate. The Incident Handler or their delegate is expected to handle the incident in a way that mitigates further exposure of the organization. The incident will be handled according to process including identification, containment, eradication, recovery, and lessons learned.

Incident Handler Name and Title	Incident Handler Signature

References

Security Incident Response Plan, https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/security_incident_response_plan_-_template.docx

National Institute of Standards and Technology (NIST), NIST Special Publication 800-61 Revision 2, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

SysAdmin, Audit, Network & Security (SANS), https://www.sans.org/reading-room/whitepapers/incident

SysAdmin, Audit, Network & Security (SANS), https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901