Incident Management Planning

Incident management in the public sector

Cyber security incidents can be devasting – to both the organization and citizens that rely on your services. They are also a fact of contemporary operations in the public sector. Being prepared, and also being able to respond quickly and effectively, goes a long way to reducing organizational risk and minimizing damage. Effective incident management planning will also help you recover from incidents, and return to normal, safe and secure operations as soon as possible.

As an IT leader in a public sector organization, you'll have a direct role in preparing and preventing cyber security incidents. And it's also very likely you'll have a role in incident management planning. This Learning Summary supplements the Incident Management Planning eLearning module, and provides you with additional details and resources that will better prepare you to engage in incident management planning and support organizational cyber security outcomes.

This Learning Summary is specific to incident management planning; for specific response and recovery actions, you should refer to the Breach Response Learning Summary.

Contents

1. Overview of the incident response life cycle
2. Preparing for incident response
3. Planning across the incident response life cycle
4. What's in your toolbox?

Suggested activities and resources

> **"Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to security incidents, and enable post-incident analysis."**
> **GO ITS 25.0 Security Requirements**

The incident response life cycle:

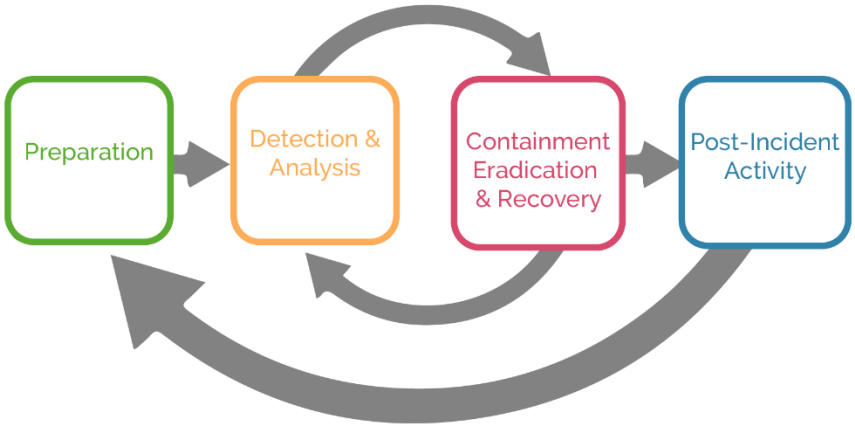

Figure 1 – The NIST Incident Response Life Cycle

There are multiple frameworks that support effective incident management planning. The U.S. National Institute for Standards and Technology (NIST) Special Publication 800-61 Rev. 2 provides a simple framework (Figure 1) that defines common incident response phases and can help an organization plan activities across the incident response life cycle.

Preparation
Steps to ensure that you're prepared for an incident, and that you have the appropriate preventative measures in place.

Detection and analysis
Steps to ensure that you're prepared for an incident, and that you have the appropriate preventative measures in place. [For detailed breach response activities and a guide to a response playbook, see the Breach Response Learning Summary.

Containment, eradication and recovery
Activities to mitigate the effects of the incident, gather necessary evidence and get your organization back to normal operations.

Post-incident activity
Activities to capture lessons learned and organizational improvements.

As organizations across the public service vary in mission, size and technical infrastructure, the activities conducted across these phases will also vary. Regardless, all public service organizations should have an incident management plan and associated procedures in place, to ensure that they're able to effectively manage cyber security incidents and mitigate the effects.

Preparing for Incident Response

There are some common preparatory steps for your organization, including:

Policy, standard and operating procedure development and implementation

Ensure that organizational roles, responsibilities and key scenario-based activities are defined and clearly communicated throughout the organization. Key policy, standards and procedural elements are:

- Responsibilities of the incident management team
- Responsibilities of other organizational representatives
- Internal and external communications processes and authorities
- Internal and external reporting requirements
- Training and awareness requirements
- Testing, reviewing and revision requirements
- Contact information for all key roles and stakeholders

Planning and resource allocation

At a minimum, the following roles should be allocated within the organization and their responsibilities clearly defined:

- Executive/senior incident management leader
- Chief information officer or equivalent
- Corporate security officer or equivalent
- Incident management coordinator
- Incident responders
- Cyber Incident Response Team (CIRT), whether on site or out-sourced
- Other organizational representatives as assigned (e.g., communications, training or IT staff)
- Third-party service providers

[**NOTE:** make sure that incident response is clearly defined in third-party service arrangements.]

Develop and test the organization's incident management plan on a regular basis – at least annually

Ensure that your organization's plan has the input of all key stakeholders; then test the plan to ensure that everyone in the organization is familiar with and confident in their role, including senior management. Also, test internal and external communications channels, including potential contingency communications – remember, email or cellphones may not work!

When creating and testing the plan, consider scenarios, such as:

- Information system failures or critical errors
- Denial of service and other loss of availability
- Breaches of private data or leakage of sensitive information
- Ransomware and loss of access to critical business data or information
- Unauthorized use, access, change or other loss of integrity from external or internal threats

Training and awareness

In addition to testing the plan, all personnel with a role in incident management should have the appropriate level of training to ensure that they can perform their tasks. Even those without a specific role should be aware of the cyber security context, and their responsibilities in preventing, detecting and reporting cyber security incidents.

Local team requirements

Within your own team, ensure that you have identified incident management responsibilities, have the required tools (e.g., jump kit, OS image, secure storage) to support incident response activities, and provided necessary staff training.

Planning Across The Incident Response Life Cycle

Detection & Analysis

Detection can occur through users, administrators, security operators or security systems. Rapid detection is key to helping minimize potential damage of a cyber security incident.

Important questions for detection and analysis planning

Are all users aware of the threats, indicators of a cyber security incident and reporting requirements?

Are system managers and administrators aware of:

- System and software vulnerabilities that can be exploited?
- Regular system behaviour, to be able to detect anomalies?
- Security system settings and procedures, to distinguish false positives?
- Reporting requirements?
- Common threats and indicators of compromise?

Analysis is critical to determining the extent and severity of the incident so that your organization can prioritize its response and identify the best course of action.

What analysis capabilities do you have within your organization?
If you don't have the expertise within your organization to do a reasonable level of analysis on the incident, then this expertise should be sought through another organization or third party. In fact, a best practice is to plan for this and ensure that analysis is written into third-party security services agreements.

We've been attacked!

One of your system administrators identifies malware within your system that continuously pings out to another system on your network. They isolate the infected system and the pinging stops. Immediately, the malware encrypts all files/data on that system drive and locks all access to the system.
Had the operator known the malware signature or referred to the recent IoC list, they would've known that this was a common attack pattern of that malware and may have opted for another approach.

Detection and analysis planning also includes:

- Coordination and information-sharing protocols with the Cyber Incident Response Team (CIRT)
- Preparing and having available documentation for recording and reporting incidents
- A leadership educated on organizational threats, incident response and immediate actions

Privacy Breaches – Don't forget! All incidents that involve the potential release of personally identifiable information (PII) and health information of Ontarians must be reported the Information and Privacy Commissioner (IPC).

See the IPC guidance at https://www.ipc.on.ca/wp-content/uploads/2019/09/privacy-breach-protocol-e.pdf

In the development of your incident management plan, you should have tested your plan against several scenarios that fit your organization and threat context. This will help inform a selection of available strategies that support containment, eradication and recovery.

Throughout this phase, you'll need to consider requirements for documenting and preserving evidence.

Containment
Eradication
& Recovery

Containment

Containment can include locking or limiting accounts, removing access, disabling an application, shutting a system down, disabling functions or disconnecting it from the network. Containment does two things:

- It 'stops the bleeding', whether it's data exfiltration or damaging effects of malware
- It also provides time for deciding on appropriate mitigating actions

You should be planning for various containment strategies based upon your organizational priorities, the type of incidents likely to be encountered and the resources available.

Considerations for choosing a containment strategy include:

- Potential damage to or loss of data/information or assets
- Need for evidence preservation
- Service availability requirements
- Time and resources needed to implement the strategy
- Effectiveness of the strategy
- Duration of the solution

"Systems involved in a security incident must be removed from the network if it is determined that they are adversely affecting, propagating problems of some type to, or jeopardizing the security of, other systems or data." (GO ITS 25 Security Requirements) However, systems must not be turned off without consultation with the security authority. This is to ensure memory integrity.

Eradication

Eradication is not necessarily required for all incidents. For example, system errors or inadvertent losses are mitigated in other ways. Malware, on the other hand, requires deletion or disabling of affected accounts. A variety of tools and resources are required for mitigation and/or eradication.

Recovery

Recovery is about safely and securely returning to normal operations. It should therefore be carefully and formally controlled by the Incident Response Coordinator or other relevant authority, to ensure that systems/data are brought back up and online without any further risk to the organization. Guidance should be available in your Business Continuity Plan and Disaster Recovery Plan, and planning for recovery includes important elements such as:

- ✓ Recovery processes within the incident management plan are in place and have been tested
- ✓ Backups are available and secure
- ✓ Tools, applications and systems required for recovery operations are available and up-to-date
- ✓ Security controls and patches are up-to-date and working as intended

For a detailed discussion of recovery, see the BCP and Breach Procedures Learning Summaries.

Post-incident data collection

A significant part of post-incident activity is data collection and, accordingly, planning for post-incident analysis means ensuring that throughout incident response, the organization is collecting relevant data.

Post-incident Activity

Post-incident activity is largely focused on problem analysis and closing out the incident. It typically has three key elements:

1. Analyzing the incident, the organizational response and what actually occurred.
2. Identifying improvements that will prevent further occurrences.
3. Wrapping up all reports and documentation related to the incident.

Suggested data requirements associated with organizational incident response:

- Type of incident and impact
- Date/time of detection and systems/devices affected
- Interpreted events as reported by Intrusion Detection/Prevention Systems
- Courses of action considered/taken
- Client activity or requests (both allowed and denied)
- Server configuration changes and/or administrator login and use of privilege
- System activity; types of mitigations and when they were deployed
- Date/time of containment
- Recovery actions taken
- Date/time of full recovery

These can be further refined to include team or individual-based response actions and decisions if that level of granularity is required.

Planning for cyber security and incident response improvement!

Planning for cyber security and incident response improvement!

What's in your incident response toolbox?

- ☐ Asset list
- ☐ Account/user list
- ☐ Port lists
- ☐ Application/software lists
- ☐ Copies of OS & critical applications
- ☐ Network diagrams & system maps
- ☐ Cryptographic hashes
- ☐ Segregated systems (sandbox) for analysis
- ☐ Spare workstations, servers, VM for administration & support recovery
- ☐ Removeable media for storage
- ☐ Secure storage for forensic evidence
- ☐ Analysis tools (e.g., packet sniffers & protocol analyzers)
- ☐ Digital forensic software
- ☐ Evidence gathering tools & materials (e.g., software, digital cameras, logs, recorders, chain of custody forms, evidence storage bags & tags, etc.)

Suggested Activities and Resources

In addition to the following, you are encouraged to continue researching topics of interest, and keep scanning the environment for tools, best practices and benchmarks that will support improvements.

Suggested Activities

- ☐ Review your organization's incident management policies and plan
- ☐ In collaboration with the Incident Management Coordinator, identify any potential gaps in the incident management plan and have them addressed
- ☐ Encourage incident management training and awareness within the organization
- ☐ Advocate for organization-wide testing of the incident management plan if not recently conducted
- ☐ Determine team responsibilities during incident response
- ☐ Identify personal and team learning requirements to support incident response
- ☐ Review and update tools and documentation within your scope of responsibility
- ☐ Test your team's ability to fulfill their responsibilities during incident response

Resources

Canadian Centre for Cyber Security (2018), An Introduction to the Cyber Threat Environment

Canadian Centre for Cyber Security (2019), Develop an incident response plan https://www.cyber.gc.ca/en/develop-incident-response-plan

Canadian Centre for Cyber Security (2012), IT Security Risk Management: A Lifecycle Approach (ITSG 33), IT Security Risk Management: A life-cycle approach

Canadian Centre for Cyber Security (2019), Top 10 IT Security Actions

Center for Internet Security (2020), CIS Controls V7.1

Government of Canada (2019), Cyber Security Event Management Plan (GC SEMP)

Government of Ontario (2012), GO ITS 25.0 General Security Requirements

Government of Ontario (2012), GO ITS 37.0 Enterprise Incident Management Process

Information and Privacy Commissioner of Ontario (2019), Privacy Breaches – Guidelines for Public Sector Organizations

National Institute of Standards and Technology (2012), Special Publication 800-61 Revision 2 *Computer Security Incident Handling Guide*

National Institute of Standards and Technology (2016), Special Publication 800-184, Guide for Cybersecurity Event Recovery