DEVELOPING YOUR INCIDENT RESPONSE PLAN

CANADIAN CENTRE FOR CYBER SECURITY

May 2021 | ITSAP.40.003

Your incident response plan includes the processes, procedures, and documentation related to how your organization detects, responds to, and recovers from incidents. Cyber threats, natural disasters, and unplanned outages are examples of incidents that will impact your network, systems, and devices. When you have a proper plan, you will be prepared to handle incidents when they happen, mitigate the threats and associated risks, and recover quickly.

BEFORE CREATING A PLAN

Before you create an incident response plan, determine what information and systems are of value to your organization. Determine the types of incidents you might face and what would be an appropriate response. Consider who is qualified to be on the response team and how you will inform your organization of your plan and associated policies and procedures.

CONDUCT A RISK ASSESSMENT

The results of your risk assessment inform your response plan. A risk assessment will identify your assets and analyze the likelihood and impact of your assets being compromised. With your risks and potential threats clearly identified, you can prioritize your response efforts. Some questions to answer during the assessment include:

- What data is valuable to your organization?
- Which business areas handle sensitive data?
- What controls do you currently have in place?
- Can this lead to a privacy breach for your organization?

DEVELOP YOUR POLICIES

Your incident response activities need to align with your organization's policy and compliance requirements.

Write an incident response policy that establishes the authorities, roles, and responsibilities for your incident response procedures and processes. This policy should be approved by your organization's senior management and executives.

ESTABLISH YOUR RESPONSE TEAM

The goal of your team is to assess, document, and respond to incidents, restore your systems, recover information, and reduce the risk of the incident reoccurring.

Your team should include employees with various qualifications and have cross-functional support from other business lines.

Roles to consider for your incident response team include:

- Incident handler
- Technical lead
- Human resources specialist
- Communications advisor
- Notetakers
- Data analysts

Incidents are unpredictable and require immediate response. Ensure you designate backup responders to act during any absences when an incident occurs.

CREATE YOUR COMMUNICATIONS PLAN

Your plan should detail how, when, and with whom your team communicates. This plan should include a central point of contact for employees to report suspected or known incidents.

Your notification procedures are critical to the success of your incident response. Identify the internal and external key stakeholders who will be notified during an incident. You may have to alert third parties, such as clients and managed service providers. Depending on the incident, you may need to contact law enforcement or a consider engaging a lawyer for advice.

EDUCATE YOUR EMPLOYEES

Update your employees on current incident response planning and execution.

Tailor your training programs to your organization's business needs and requirements, as well as your employees' roles and responsibilities.

A well-trained workforce can defend against incidents.

An **event** is an observable occurrence in a system or network (e.g. a user sending email).

An **incident** is an adverse event in an information system or network, or the threat of such an event.

An **environment** is your network and everything attached to it, such as peripheral devices (e.g. printers, computers, routers). Is your environment open to everyone or is it secure?

An **open environment** allows information to be transmitted in and out of the network, without restrictions.

A **secured environment** restricts what information is allowed in and out of the network.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

DEVELOPING YOUR INCIDENT RESPONSE PLAN

CANADIAN CENTRE FOR CYBER SECURITY

MAY 2021 | ITSAP.40.003

CREATE YOUR INCIDENT RESPONSE PLAN

Your incident response plan should define the objectives, stakeholders, responsibilities, communication methods, and escalation processes used throughout the incident response lifecycle. Keep the plan simple and flexible. Test, revisit, and revise it annually to keep it effective. The following list details the phases of the incident response life cycle which can be followed to structure your plan.

1 PREPARE

Lay out the objectives of your incident response strategy, as well as your related policies and procedures. Define your goals to improve security, visibility, and recovery.

Implement a reliable backup process to create copies of your data and systems and help you restore them during an outage.

Have a detailed strategy for updating and patching your software and hardware. Use this strategy to track and fix vulnerabilities and mitigate the occurrence and severity of incidents.

Develop exercises to test your plan and response. You can revise and improve your plan using your test results.

2 OBSERVE

Monitor your networks, systems, and connected devices to identify potential threats. Produce reports on a regular basis and document events and potential incidents. Analyze these occurrences and determine whether you need to activate your incident response plan. Determine the frequency and intensity of your monitoring. You may want to consider monitoring your networks on a 24/7 basis or in a more ad hoc manner.

3 RESOLVE

Gain an understanding of the issue so you can contain the threat and apply effective mitigation measures.

An effective mitigation measure is disabling connectivity to your systems and devices to block the threat actor from causing further damage. It might be necessary to isolate all systems and suspend employee access temporarily to detect and stop further intrusions.

Eradicate the intrusion by restoring your systems from a backup. You should also run anti-malware and anti-virus software on all systems and connected devices. If you uncover vulnerabilities, you will need to patch and update your devices.

Preserve evidence and supporting documentation to assist in your analysis of the incident.

4 UNDERSTAND

Identify the root cause of the incident and collaborate with the response team to determine what can be improved. Evaluate your incident response processes and highlight what went well and which areas require improvement. Create a lessons learned document that details how you will adjust and improve your plan for future incidents.

Document the steps taken to uncover and resolve the incident. This will assist you in responding to future incidents by providing insight into possible mitigation measures and lessons learned to offer a faster, more effective recovery.

TYPES OF INCIDENTS

Ransomware is a type of malware that locks you out of files or systems until you pay a ransom to a threat actor. Payment doesn't guarantee you will regain access to your information.

Data theft occurs when threat actors steal information stored on servers and devices. The data is most commonly accessed using stolen user credentials. Advanced persistent threat (APT) is one method of data theft where a threat actor gains prolonged access to a network without being identified. APT allows attackers to monitor traffic, access sensitive information, and steal data over a prolonged period of time.

Active exploitation takes advantage of unpatched software, hardware, or other vulnerabilities to gain control of your systems, networks, and devices. These attacks can go unnoticed before you have the opportunity to apply a patch or update. Your plan should provide instructions for mitigating active exploitation, such as temporarily suspending Internet access or ceasing online activity.

IN-HOUSE OR PROFESSIONAL SERVICES

When planning your response plan, determine which actions and services you can conduct internally and which actions you will outsource. Professional services can be obtained to assist you with incident response initiatives, such as developing your plan, determining your backup processes, and monitoring and patching your systems.

LEARN MORE

If you want to learn more about some of the key points identified here, check out the following publications on our website (cyber.gc.ca).

- Ransomware: How to Prevent and Recover (ITSAP.00.099)
- Developing Your IT Recovery Plan (ITSAP.40.004)
- Have You Been Hacked? (ITSAP.00.015)
- Preventative Security Tools (ITSAP.00.058)
- Tips for Backing up Your Information (ITSAP.40.002)
- Offer Tailored Cyber Security Training to Your Employees (ITSAP.10.093)

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada