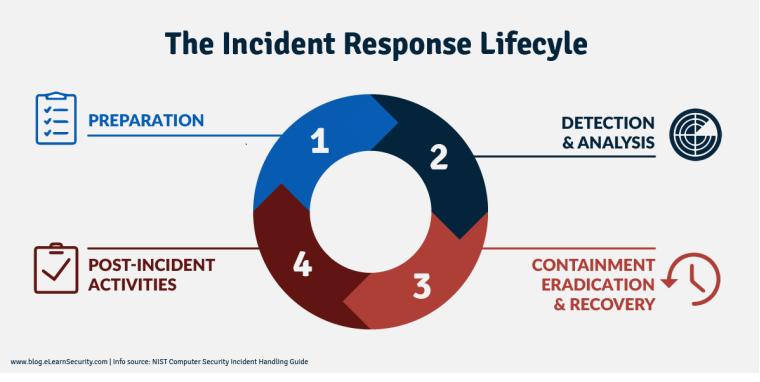
Incident Response and Recovery

IT risk management and incident response are crucial components of any effective cyber security strategy. This unit will cover the basics of incident response, including the development of a response plan and the process of managing and recovering from an IT incident.



What is an IT incident response plan?

An IT incident response plan is a set of written instructions that can help you respond to a variety of potential scenarios, such as data breaches, denial-of-service attacks, firewall intrusions, virus or malware infections, insider threats, damage to equipment or premises, and loss of power or other technology failures. Your incident response plan should identify key individuals who will act in the event of an incident and describe their roles and responsibilities. It should also indicate who is responsible for testing the plan and putting it into action. Your business' incident response plan should be based on thorough and comprehensive IT risk assessments.

IT incident management process

The process of managing an IT incident typically involves six steps:

1. Prepare staff and managers to handle potential incidents should they arise
2. Determine if an event is an IT failure or a security incident
3. Contain the incident and prevent further damage to systems and equipment
4. Find the cause of the incident and remove the affected systems
5. Recover those systems after removing the threats

6. Document and analyze the situation to update, change, or improve procedures

An IT incident can be confined to one or more IT components of your business, or it can be part of a wider crisis, such as a fire, flood, or natural disaster. If a wider emergency occurs, such as a fire, the safety of staff and the public is your first priority. You should include emergency response plans in your incident response strategy.

IT incident recovery planning

How you respond to IT incidents will determine how well your business recovers from them. Planning can help you shorten recovery times and minimize losses. A recovery plan could include your recovery time goals, as well as strategies to recover your business activities in the quickest possible time and a description of the key resources, equipment, and staff needed to recover your operations. It's essential to plan thoroughly to protect yourself from the impact of potential business crises brought on by IT failure or security breaches.

To help you prepare for and plan your response to a cyber incident, the National Cyber Security Centre (NCSC) has produced small business guidance on response and recovery. You can also test and practice your response to a cyber attack with the help of their 'Exercise in a Box' online training tool.

In conclusion, having a robust incident response plan and process in place is crucial for mitigating the damage caused by IT security breaches or failures. By following best practices in IT risk management and incident response planning, businesses can minimize the impact of IT incidents and recover more quickly, ensuring the continuity of their operations.