Blueprint: Incident response

Blueprint: Incident response

Your cyber attack response plan should include short and long-term goals, measurements for success and training required so employees and management can respond effectively to incidents and the business can recover from the event and continue to thrive.[52]

Preparation

□ **Create roles** Put at least one person, but preferably a pair of employees, in charge of your cyber security response. They must oversee all actions, track progress and communicate to all relevant parties, including those to whom your business outsources key roles, such as PR, technical or legal responsibilities.

□ **Delegate** Define roles and responsibilities and chain of command. Depending on the size of your business, you may need to delegate authority to key employees or team leaders, such as IT, legal, PR, HR and Insurance. Ideally, you'll need a key contact and a deputy in each case. Outline their decision-making authority.

□ **Communicate** Adopt a clear and simple process of communication. Create a central channel for all involved, such as a conference call number or Whatsapp group so everyone can participate in discussions. Decide how you will communicate with your list of contractors, suppliers, clients and insurers.

□ **Practice** When people are placed under stress, they can panic or overreact. Practice your incident response based on real-life scenarios so employees become confident and prepared. External experts can run exercises and provide impartial advice. These could be tactical, technical or strategic. Run exercises in all areas, document them and learn from mistakes to hone your response.

□ **Train** Targeted training helps employees respond appropriately. Key employees will need to understand the technical aspects of your system so they can triage issues and take remediation measures. If your IT function is outsourced, discuss your cyber response in detail with your service provider and ensure these aspects are covered in any agreement with them.

[52] US National Institute of Standards and Technology NIST SP 800-61

Blueprint: Incident response (continued)

Detection and Analysis

□ **Detect**

As in any emergency situation, when a cyber attack actually happens, triage is the first step to assess the severity of the incident and then act.[53]

First confirm what has happened, determine the scope of compromise and the impact on your business and its customers/clients.

□ **Analyse**

- Accessibility – how are your employees impacted? How many are blocked from accessing data and information systems? Is it a total service outage and is your core functionality broken?[54]
- Privacy – how much sensitive data has the cyber criminal leaked or stolen and how many customers/clients have been affected?
- Integrity – has the cyber criminal commandeered and compromised your system or data so you can no longer trust its integrity?
- What kind of attack have you experienced: malware, phishing, denial of access or ransomware? See the glossary (link) for more information about types of cyber attacks.[55]

Gather information quickly to understand enough to contain, mitigate and ultimately remediate the attack. Engage with involved employees to understand what they saw or did – such as clicking on a link. Examine logs including your Active Directory, remote access and email.

Many incidents require more complex analysis which requires an expert's skill including:

- full host (disk/mobile/server) forensics
- network traffic and log analysis
- advanced malware analysis
- correlation of many different event, log and data sources.

[53] Plan: Your cyber incident response processes - NCSC.GOV.UK

[54] Atlassian Security Incident Management Process

[55] Plan: Your cyber incident response processes - NCSC.GOV.UK

Blueprint: Incident response (continued)

Containment, eradication and recovery

□ Contain

As soon as possible, contain the incident's impact to ensure critical services remain available to employees and customers if possible. This solution may be temporary and contain the issue for a few hours, days or weeks – in the best case scenario it's permanent.

□ Eradicate

You may need an expert to identify the attacking host and validate its IP address, block communication from the attacker and identify the threat actor to understand their mode of operation, search and block other communication channels they may be using. Other actions include the following:

- Quarantine particular devices/computers or parts of the network
- Reset administration and server accounts
- Block in and outbound activity and email
- Remove malicious files, cleaning machines' user profiles.[56]

□ Notify

Commence crisis management. Depending on the severity of the attack you will need to:

- Communicate information about the event to your executive, board and employees.
- Email or phone clients or customers who are data breach subjects immediately.
- Determine your legal or regulatory requirements.
- Inform regulators.
- Develop a media response.

Eradication must be successful before you can move to recovery – and this could involve monitoring and analysis for a period of time.

□ Start recovery

Once you're confident that your IT team or experts have removed the cyber threat or attacker from your systems, you can return to 'business as usual' while simultaneously carrying out your Business Continuity Plan into practice.

This will mean you can put clean systems and data back online. If the attack harmed your data or systems, you might have to go through a technical recovery stage as well and install offline backups, segregated for a period of time as online backups could also be infected. Some devices may require a total rebuild or reinstallation of the software after the incident.

□ Enact business continuity plan

To ensure that your business gets back to functioning as quickly as possible after a cyber attack or another disaster, put your business continuity plan into action.

[53] Plan: Your cyber incident response processes - NCSC.GOV.UK

[54] Atlassian Security Incident Management Process

[55] Plan: Your cyber incident response processes - NCSC.GOV.UK

[56] Plan: Your cyber incident response processes - NCSC.GOV.UK

Blueprint: Incident response (continued)

Post-incident activities

□	**Conduct a business impact assessment**	This will give you an idea of: • how much the event will have cost you • what your strengths and weaknesses are • how you can improve your response plans, roles and actions
		Reputational damage with existing and potential clients, as well as people in your supply chain, is more difficult to quantify at this early stage. Repair reputational damage by offering discounts or having extra employees (or employees diverted from other tasks) answer a hotline for queries from clients/customers. Inform your suppliers of the breach.[57]
□	**Learn from the experience**	Contact digital forensic experts so you have clear details of what happened and why so you can address that in your business remediation plan.

Lessons learned

Depending on the severity of the incident, ask senior management, board members, employees clients and customers the following questions and document the answers:

- What happened during the incident, and at what stages?
- How well did the incident response team deal with the incident? Were processes followed, and were they sufficient?
- What information was needed sooner?
- Were any wrong actions taken that caused damage or inhibited recovery?
- What could people do differently next time if the same incident occurred?
- Could they have shared information better with other organisations or other departments?
- What have we learned to prevent similar incidents in the future?
- What new precursors or indicators of similar incidents should we watch for in the future?
- What additional tools or resources are needed to help prevent or mitigate similar incidents?[58]

Use findings from these answers to learn valuable lessons from the cyber attack and feed into your cyber incident response plan, to change or improve the roles of management and employees, to beef up your staff training, to consult more experts and to improve your cyber security defence plan.

[57] Journal of Accountancy Helping clients build a cyberattack recovery plan

[58] US National Institute of Standards and Technology NIST SP 800-61