GUIDANCE

10 Steps to Cyber Security

Guidance on how organisations can protect themselves in cyberspace.

IN THIS GUIDANCE

PUBLISHED

11 May 2021

REVIEWED

11 May 2021

VERSION

1.0

WRITTEN FOR

Cyber security professionals

Incident management

Plan your response to cyber incidents in advance.

Incidents can have a huge impact on an organisation in terms of cost, productivity and reputation. However, good incident management will reduce the impact when they do happen. Being able to detect and quickly respond to incidents will help to prevent further damage,

reducing the financial and operational impact. Managing the incident whilst in the media spotlight will reduce the reputational impact. Finally, applying what you've learned in the aftermath of an incident will mean you are better prepared for any future incidents.

What are the benefits?

- **Effective incident management lessens the impact of a cyber incident**
- **A practised plan will help you make good decisions under the pressure of a real incident**
- **A well-managed response, with clear communication throughout, builds trust with shareholders and customers**
- **Learning from incidents identifies gaps and issues with your response capability**

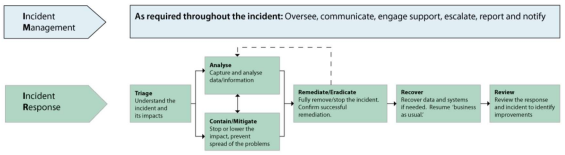
What should you do?

Prepare response plans and capability

- Ensure the right people are involved when drawing up your incident response plans. This is likely to include your IT security team, but will also include legal, HR and Public Relations staff, as well as suppliers and vendors. Senior management will need to support critical decisions and elements such as media handling for serious incidents.
- Ensure your incident response plan is linked to disaster recovery, business continuity and crisis management plans, and supported with the relevant capabilities. These come into play when an incident is serious enough to cause major disruption and/or damage to your business.
- Ensure everyone's roles and responsibilities are defined and understood and provide appropriate training. Appoint and empower specific individuals (or an incident response supplier) to handle incidents, and provide them with clear terms of reference to make decisions and manage any incident that

may occur. Ensure that the contact details of key personnel are readily available to use in the event of an incident. An example set of incident response team roles is given in the NCSC's guidance on Creating your Cyber Security Incident Response Team.

- Consider how you will detect incidents. Your response plans should align with all your methods of detection including logging and monitoring and reporting from staff, or suppliers and partners. Other third parties (such as organisations carrying out incident investigations or threat research) and occasionally government may also report incidents to you. All alerts should be sent to the team responsible for managing them, for assessment and triage.
- Establish your criteria for escalation to senior management and what needs to happen for you to scale up your response. Consider what is most important to **your specific organisation** to determine the severity of an incident, and how you should prioritise it.
- Ensure staff are aware of any playbooks you may have prepared for specific types of incident, and be ready to share these with any third parties which may need to be involved. It is vital that staff who can authorise critical decisions (such as taking a customer database or website offline) can be contacted. Consider identifying deputies should the primary contact not be available. The technical staff (i.e. those who will carry out such actions) must be aware of **who** can provide authorisation, and **how** and **when** to contact them. This applies to suppliers as well as in-house staff.
- Identify specific situations where the technical team can act autonomously, based on the highest business risks and where taking early containment action is likely to reduce the impact of particular incidents.
- Ensure your plan includes basic guidance on legal or regulatory reporting requirements based on the types and volumes of data your organisation holds, and an outline of your processes covering a full incident lifecycle. An example plan is shown below.



Practise your response plans

- Practising response plans ensures staff know how to respond in during an incident, and can also highlight any problem areas in your planned response . The NCSC's Exercise in a Box is a free online tool which helps organisations test and practise their response to different types of cyber attack, including everything you need for setting up, planning, delivery, and post-exercise activity.
- Practise restoring files from backups. After an incident ensure only clean data is copied back onto clean systems and networks.

Respond appropriately (and communicate clearly) during an incident

- Don't be drawn into over-reacting during the containment phase of an incident; you might need to gather more information before deciding on a suitable course of action. Over-reacting can cause more damage than the incident itself - in the case of targeted attacks, the attacker could react or bury themselves more deeply in your network. Consider the repercussions of any actions you may take, and discuss with colleagues.
- Communicate with your stakeholders and customers throughout an incident. Clear communication will help minimise the short term impact of an incident and will help build trust with your customers, reducing the long term impact of an incident.
- Keep a careful record of the incident response, decisions made, actions taken, data captured (or missing), as this will be incredibly useful for post-exercise reviews. This is especially true if you need to present evidence of your response to a regulatory body.

Incorporate lessons from incidents into organisational improvements

- Update your response plans after every incident. Use the incident to reflect on the security of your enterprise - understand how the incident happened and what could have prevented it. Post incident reviews should

feedback both into your response plans and wider organisation.

- Particularly consider if there was any information which would have significantly helped your response but which was difficult or impossible to obtain. Make a plan to gather this data ahead of any future attacks and add to your logging and monitoring strategy.
- Do not constrain yourself to only looking for what went wrong. Also consider which aspects of your response worked well, and why. This can give insights into how to improve future plans.

Learn More

Incident management
How to effectively detect, respond to and resolve cyber incidents.

Planning your response to Cyber Incidents
Advice for Board members on responding to cyber incidents.

← Logging and monitoring

Supply chain security →

Topics

Incident management
Operational security
Risk management

PUBLISHED
11 May 2021

REVIEWED
11 May 2021

VERSION
1.0

WRITTEN FOR
Cyber security professionals

Also see

Weekly Threat Report 23rd July 2021
The NCSC's weekly threat report is drawn from recent open source...
Report
23 July 2021

The first Certified Cyber Professional (CCP) Specialism is now live!

'Risk Management' is the first certifiable specialism under the...

Blog Post
8 July 2021

NCSC statement on Kaseya incident

The NCSC's official statement on the Kaseya cyber incident.

News
5 July 2021