National Cyber Security Centre

Guidance a part of GCHQ (/)

10 Steps: Incident Management

Created: 29 Sep 2015
Updated: 08 Aug 2016
Part of: 10 Steps to Cyber Security (/guidance/10-steps-cyber-security)
This section from within the NCSC's '10 Steps To Cyber Security' concerns Incident Management.

Summary

All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact.

What is the risk?

Security incidents will inevitably happen and they will vary in their level of impact. All incidents need to be managed effectively, particularly those serious enough to warrant invoking the organisation's business continuity or disaster recovery plans. Some incidents can, on further analysis, be indicative of more severe underlying problems.

If businesses fail to implement an incident management capability to detect, manage and analyse security incidents the following risks could be realised:

- **Managing business harm:** Failure to realise that an incident is happening or has occurred limits your ability to manage it effectively. This may lead to a much greater overall business impact, such as significant system outage, serious financial loss or erosion of customer confidence.

- **Continual disruption:** An organisation that fails to address the root cause of incidents (such as poor technology or weaknesses in the corporate security approach) could be exposed to repeated or continual compromise or disruption.

- **Failure to comply with legal and regulatory reporting requirements:** An incident resulting in the compromise of sensitive information covered by mandatory reporting requirements could lead to legal or regulatory penalties.

The organisation's business profile or role will determine the type and nature of incidents that could occur and the impact they might have, so a risk-based approach should be used to shape incident management plans.

How can the risk be managed?

Establish an incident response capability: Identify the funding and resources to develop, deliver and maintain an organisation-wide incident management capability. Resources could be in house or you might pre-establish a relationship with an specialist incident management company. This should address the full range of incidents that could occur and set out appropriate responses. The supporting policy, processes and plans should be risk based and cover any legal or regulatory reporting requirements.

Provide specialist training: The incident response team may need specialist knowledge and expertise across a number of technical (including forensic investigation) and non-technical areas. You should identify recognised sources (internal or external) of specialist incident management training and maintain the organisation's skill base.

Define the required roles and responsibilities: Appoint and empower specific individuals (or suppliers) 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.

Establish a data recovery capability: Data losses can occur and so a systematic approach to the backup of essential data should be implemented. Where physical backup media is used this should be held in a physically secure location, ideally offsite. The ability to recover archived data for operational use should be regularly tested.

Test the incident management plans: All plans supporting security incident management (including business continuity and disaster recover plans) should be regularly tested. The outcome of the tests should be used to inform the future development of the incident management plans.

Decide what information will be shared and with whom: For services or information bound by specific legal or regulatory reporting requirements you may have to report incidents. All internal and external reporting requirements should be clearly identified in the incident management plan.

Collect and analyse post-incident evidence: The preservation and analysis of the sequence of events that led up to the incident is critical to identify and remedy the root cause. The collected evidence could also potentially support any follow on disciplinary or legal action and the incident management policy should set out clear guidelines to follow.

Conduct a lessons learned review: Log the actions taken during an incident and review the performance of the incident management process post incident (or following a test) to see what aspects worked well and what could be improved. Review the organisational response and update any relevant policies or user training that could have prevented the incident from occurring.

User awareness: Users should be aware of their responsibilities and how they can report and respond to incidents. Users should be encouraged to report any security weaknesses or incident as soon as possible, without fear of recrimination.

Report criminal incidents to law enforcement: It is important that potential or actual cyber crime is reported to Action Fraud or other relevant law enforcement agency.

Learn more

Please visit our Incident management (/incident-management)pages.

Topics

Incident management(/topics/incident-management)
Cyber attacks(/topics/cyber-attacks)

Was this guidance helpful?

We need your feedback to improve this content.

Yes No