11

When things go wrong: nonconformities and incidents

This chapter covers how to plan to deal effectively with failures in information security and how to use these experiences to improve your information security management system. It forms part of Stage 4 – Performance, Evaluation and Improvement in the Toolkit Route map.

Key topics

- **How to detect and recover when things go wrong**
- **How to reduce the impact of adverse events**
- **How learning from adverse events can improve information security**

11.1 Introduction

It is dangerous to assume that nothing will ever go wrong: information security is about managing the risk from adverse events, not eliminating them. Planning how to recover from failures is an important aspect of managing information security.

The ISO standards define two distinct types of failure:

- nonconformity: the nonfulfillment of a [known] requirement (ISO 19011)
- incident: an unexpected or unwanted event likely to compromise business operations (ISO/IEC 27000).

Organisations should take action to control and correct non-conformities, and respond to incidents to prevent recurrence.

Nonconformities may increase the likelihood of incidents, and incidents are one way in which that nonconformities are discovered. However not all incidents indicate the presence of nonconformities. A realistic ISMS will accept, and manage, a certain frequency and level of incidents (see Chapter 5, Risk assessment).

Both incidents and nonconformities require a prepared and timely response that remedies the immediate problem and learns lessons to reduce the likelihood of recurrence. Both involve identification, corrective action and analysis of root causes, which may follow similar processes. Both may (nonconformities must) lead to improvements in the ISMS.

A key difference is that, subject to audit requirements, the organisation will normally control the timescale on which it responds to a nonconformity, typically weeks or months. Incidents arise and evolve outside the organisation's control and require a technical response in minutes or hours. Incident response should link to the organisation's crisis communications plan (for example, see the final case study), and to business continuity and disaster recovery plans.

This chapter first considers how to address nonconformities, then incidents.

11.2 Nonconformities

11.2.1 Identifying nonconformities

Within an ISO/IEC 27001-aligned ISMS, there are two types of nonconformities:

- the documented management system deviates from the requirements of ISO/IEC 27001
- the implemented management system deviates from its documented state.

Nonconformities may result from not doing enough, or from doing too much (overkill). For example, blocking the use of USB sticks where a block has not been justified is a nonconformity; but so is identifying a need for such a block, documenting that it is in place, and then not implementing it.

Nonconformities are often found during an audit. A Stage 1 audit ("document review") may identify that the ISMS documentation does not contain what is required by the ISO standard; a Stage 2 ("conformance") audit may identify that the organisation's practice does not match its documentation. For example a required firewall might not have been installed or a password policy be being ignored.

Nonconformities may also be discovered outside the audit process, including through information security incidents or if staff have difficulty implementing or working within a prescribed control (see Chapter 6, Controls, for more advice). Organisations should ensure their processes can capture these nonconformities and that staff feel comfortable pointing them out.

11.2.2 Dealing with nonconformities

ISO/IEC 27001 requires organisations to deal with every nonconformity. A common, clearly-defined, process should be used, though different nonconformities may require different resources. Minor nonconformities may be resolved between the ISMS manager and the owner of the related business activity, while major ones require top management attention.

If an existing process, such as those which are part of ITIL service management or COBIT IT governance, is available and suitable to handle corrective actions, this should be used to simplify matters.

The process must ensure that each nonconformity is reviewed and appropriate corrective actions taken to deal with it and any consequences. Corrective actions may involve any part of the system, from a more accurate implementation of a required technical security control, better training for users in implementing it, to a change in the risk management process itself. Records of nonconformities and corrective actions must be kept.

The causes of nonconformities must also be reviewed, investigated and corrected. This may reveal wider issues across the ISMS, where a nonconformity may recur at different times or in different parts of the system. Wider corrective actions may be required if, for example, the ISMS has failed to identify a significant risk or selected an unsuitable control. Again, these conclusions must be documented and the required actions managed to completion.

Nonconformities should be used as a tool for the continual improvement of the organisation's information security (see Chapter 12, Continual improvement). It is important to remember that it is the organisation, not the individual, that is being assessed. Using nonconformities to assign blame will discourage correct behaviour among those involved in the ISMS.

11.3 Information security incidents

Any unwanted or unexpected event with a significant probability of threatening business operations or information security may constitute an incident. Incidents can affect information and its processing in any form: the compromise of a networked computer, the loss of a paper file or the inclusion of the wrong person in an information handling process may all be information security incidents.

Managing incidents effectively can significantly reduce their impact and so is a valuable way to enhance information security. For research and education organisations this reactive approach is particularly important since the wide range of legitimate users and activities makes strong preventive controls less appropriate (also see Chapter 6, Controls).

Information security incidents may also highlight areas needing improvement: for example identifying policies that are not followed, policies that are not effective, risks that have changed, or systems lacking necessary resources or skills. Reviewing incidents may also, of course, reveal the need for improvements to the incident management processes themselves.

Both outcomes require incident management to be planned, documented, resourced and recorded. The organisation must first define what it classes as an incident and plan its response.

11.3.1 The incident response policy and plan

The incident response policy is the basis for incident response activities. The policy defines what the organisation considers to be an incident, what incident response should achieve and how it is escalated, and the responsibilities and authorities of people within the organisation to make that happen.

Different events may qualify as incidents ("business-affecting events") in different parts of the organisation; the desired response to an incident may also vary. In general the accidental destruction of a user's file is unlikely to constitute an incident, but the accidental destruction of a business-critical database almost certainly will. If the organisation's web server is compromised, the priority is likely to be to re-establish a secure web presence: if a server storing sensitive research data is compromised, the priority will be to find out what data may have been affected and how. The incident response policy may comprise a standard set of incident definitions and desired outcomes with variations covering areas with different requirements, consistent with the classification of information processed.

Once policy is set, an incident response plan should be developed to implement it. The plan will comprise processes, procedures and the systems and resources needed to implement them. These will themselves require preparation. The CERT Coordination Center's Mission Risk Diagnostic for Incident Management Capabilities provides a useful health check. Exercises are a good way to identify problems and to train incident responders to work together.

Case studies in this chapter include how one organisation developed its incident response policy and plan and two examples of incident response plans.

11.3.2 Responsibilities and authorities

Successful incident response requires coordination. Most incidents will involve working with others, both inside and outside the organisation, from technical staff, HR, legal and communications advisors, to network providers, regulators and law enforcement. Preparation must ensure that the required people, systems and services will be available when needed, even if this takes them away from normal duties. Defining specific roles and responsibilities in the incident response plan will considerably strengthen an organisation's capability to handle incidents.

Incident coordinators must be granted, or be able to quickly obtain, the authority to modify or suspend any of the organisation's activities until they are restored to a secure state. For example a compromised computer may need to be disconnected from the network, a suspect account have its access rights withdrawn, or a research activity suspended while the integrity of its data is checked.

11.3.3 Stages in incident response

Trust must be established before an incident, not during it.

Responding to an incident normally involves three stages: detection, analysis and response. Each is driven by the definitions and requirements of the incident response policy. After an incident, a review should take place to identify lessons that can be learned, including any changes to the ISMS that may be required.

Incidents may be detected directly, by someone noticing a security failure, or indirectly, by human or computer monitoring of computer logs or other records. The organisation should ensure it has the reporting and monitoring systems needed to detect the types of incident defined in the policy, and that these are known to and trusted by all those who may detect signs of an incident. Information gathered during security events and incidents is likely to be sensitive: a case study shows one organisation's policy for handling this material.

Successful incident management depends upon a critical resource – availability of the right people/roles to receive alerts, do the analysis, coordinate work, and carry out response activities. The organisation must have communication routes previously agreed, and tested – and contingency plans for those (frequent) cases where someone is unavailable.

Not all reported events will indicate incidents. An initial triage process determines whether a report, or group of reports, should be treated as an incident or whether another process, for example for faults or helpdesk enquiries, is appropriate. Those reports that are classed as incidents are likely to require further analysis to determine how best to restore the organisation to its desired operational state.

In complex incidents, the response stage may begin with containment to prevent the impact getting worse. This gives more time for the steps required to remove the incident's cause and, to the extent possible, investigate and mitigate its consequences. Both containment and response are likely to involve working with those having relevant expertise both inside and outside the organisation (see Chapter 8, Roles and competencies), as well as official communications channels to ensure that the right messages are getting out. All actions taken to respond to incidents should be recorded, to ensure the response is effective and to inform the subsequent review.

11.3.4 Review

Completed incidents are a major source of information about the organisation's information security, so should be reviewed to identify lessons that can be learned. Incident coordinators should review whether the response was successful and whether changes are needed to the incident response plan or its implementation.

They should also generate a report for the organisation's ISMS review process (see Chapter 12, Continual improvement). The detail in this report may vary. For routine incidents resolved successfully it may just summarise the number of incidents and the systems or units affected; but for serious or novel incidents, the report should include the root cause of the incident (to the extent that this can be determined), the impact on the organisation, and the controls that were, and were not, effective in managing it.

The final case study describes one organisation's response to a security incident affecting personal data.

Summary

- The ISMS should aim to manage the level and severity of adverse events, not to eliminate them
- The ISMS should contain plans to respond to, and learn from, these events
- Incident response requires trusted cooperation both within and outside the organisation; trust must be established in advance

Resources

Developing an information security incident response plan based on ISO/IEC 27035:2011 – University of Oxford

Example of an information security incident response scheme

Information security service: information security incident management process – UCL

Investigations and data access policies – University of York, case study

Data breach – case study

Reading list

ITIL
www.ucisa.ac.uk/ismt42
www.axelos.com/itil

COBIT
www.ucisa.ac.uk/ismt43
www.isaca.org/cobit

CERT-CC, Mission Risk Diagnostic for Incident Response Capabilities
www.ucisa.ac.uk/ismt44
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=91452

ENISA, CSIRT Exercises
www.ucisa.ac.uk/ismt45
www.enisa.europa.eu/activities/cert/support/exercise

NIST, Incident Response Exercises
www.ucisa.ac.uk/ismt46
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, Appendix A

Information Commissioner, Notification of Data Security Breaches to the Information Commissioner's Office
www.ucisa.ac.uk/ismt47
https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf

ENISA, Support for CSIRTs
www.ucisa.ac.uk/ismt48
www.enisa.europa.eu/activities/cert/support

Association of Chief Police Officers, Good Practice Guide for Digital Evidence
www.ucisa.ac.uk/ismt49
www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf