INTERNATIONAL STANDARD

ISO/IEC 27035-1

First edition
2016-11-01

Information technology — Security techniques — Information security incident management —

Part 1: Principles of incident management

Technologies de l'information — Techniques de sécurité — Gestion des incidents de sécurité de l'information —

Partie 1: Principes de la gestion des incidents

Reference number
ISO/IEC 27035-1:2016(E)

Contents

Page

3.2
incident response team
IRT
team of appropriately skilled and trusted members of the organization that handles incidents during their lifecycle

Note 1 to entry: CERT (Computer Emergency Response Team) and CSIRT (Computer Security Incident Response Team) are commonly used terms for IRT.

3.3
information security event
occurrence indicating a possible breach of information security or failure of controls

3.4
information security incident
one or multiple related and identified *information security events* (3.3) that can harm an organization's assets or compromise its operations

3.5
information security incident management
exercise of a consistent and effective approach to the handling of *information security incidents* (3.4)

3.6
incident handling
actions of detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents* (3.4)

3.7
incident response
actions taken to mitigate or resolve an *information security incident* (3.4), including those taken to protect and restore the normal operational conditions of an information system and the information stored in it

3.8
point of contact
PoC
defined organizational function or role serving as the coordinator or focal point of information concerning incident management activities

4 Overview

4.1 Basic concepts and principles

An information security event is an occurrence indicating a possible breach of information security or failure of controls. An information security incident is one or multiple related and identified information security events that meet established criteria and can harm an organization's assets or compromise its operations.

The occurrence of an information security event does not necessarily mean that an attack has been successful or that there are any implications on confidentiality, integrity or availability, i.e., not all information security events are classified as information security incidents.

Information security incidents can be deliberate (e.g. caused by malware or intentional breach of discipline) or accidental (e.g. caused by inadvertent human error or unavoidable acts of nature) and can be caused by technical (e.g. computer viruses) or non-technical (e.g. loss or theft of computers) means. Consequences can include the unauthorized disclosure, modification, destruction, or unavailability of information, or the damage or theft of organizational assets that contain information.

Annex B provides descriptions of selected example information security incidents and their causes for informative purposes only. It is important to note that these examples are by no means exhaustive.

A threat exploits vulnerabilities (weaknesses) in information systems, services, or networks, causing the occurrence of information security events and thus potentially causing incidents to information assets exposed by the vulnerabilities. Figure 1 shows the relationship of objects in an information security incident.

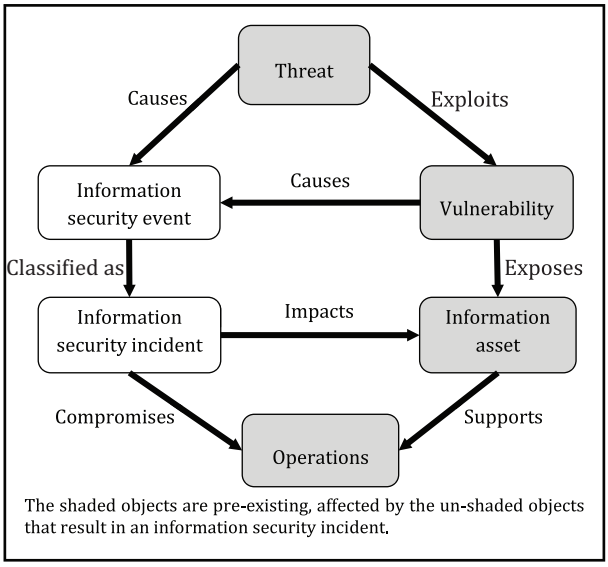

Figure 1 — Relationship of objects in an information security incident

Information sharing and coordination with external IRTs is an important consideration. Many incidents cross organizational boundaries and cannot be easily resolved by a single IRT. Information sharing and coordination relationships or partnerships with external IRTs can greatly enhance the ability to respond to and resolve incidents. For further detail about information sharing, see ISO/IEC 27010.

4.2 Objectives of incident management

As a key part of an organization's overall information security strategy, the organization should put controls and procedures in place to enable a structured well-planned approach to the management of information security incidents. From an organization's perspective, the prime objective is to avoid or contain the impact of information security incidents in order to minimize the direct and indirect damage to its operations caused by the incidents. Since damage to information assets can have a negative impact on operations, business and operational perspectives should have a major influence in determining more specific objectives for information security management.

More specific objectives of a structured well-planned approach to incident management should include the following:

a) information security events are detected and dealt with efficiently, in particular deciding when they should be classified as information security incidents;

b) identified information security incidents are assessed and responded to in the most appropriate and efficient manner;

c) the adverse effects of information security incidents on the organization and its operations are minimized by appropriate controls as part of incident response;

d) a link with relevant elements from crisis management and business continuity management through an escalation process is established;

e) information security vulnerabilities are assessed and dealt with appropriately to prevent or reduce incidents. This assessment can be done either by the IRT or other teams within the organization, depending on duty distribution;

f) lessons are learnt quickly from information security incidents, vulnerabilities and their management. This feedback mechanism is intended to increase the chances of preventing future information security incidents from occurring, improve the implementation and use of information security controls, and improve the overall information security incident management plan.

To help achieve these objectives, organizations should ensure that information security incidents are documented in a consistent manner, using appropriate standards for incident categorization, classification, and sharing, so that metrics can be derived from aggregated data over a period of time. This provides valuable information to aid the strategic decision making process when investing in information security controls. The information security incident management system should be able to share information with relevant external parties and IRTs.

Another objective associated with this part of ISO/IEC 27035 is to provide guidance to organizations that aim to meet the Information Security Management System (ISMS) requirements specified in ISO/IEC 27001 which are supported by guidance from ISO/IEC 27002. ISO/IEC 27001 includes requirements related to information security incident management. A table that cross-references information security incident management clauses in ISO/IEC 27001 and clauses in this part of ISO/IEC 27035 is provided in Annex C. ISMS relationships are also explained in Figure 2. This part of ISO/IEC 27035 can also support the requirements of information security management systems other than ISMS.

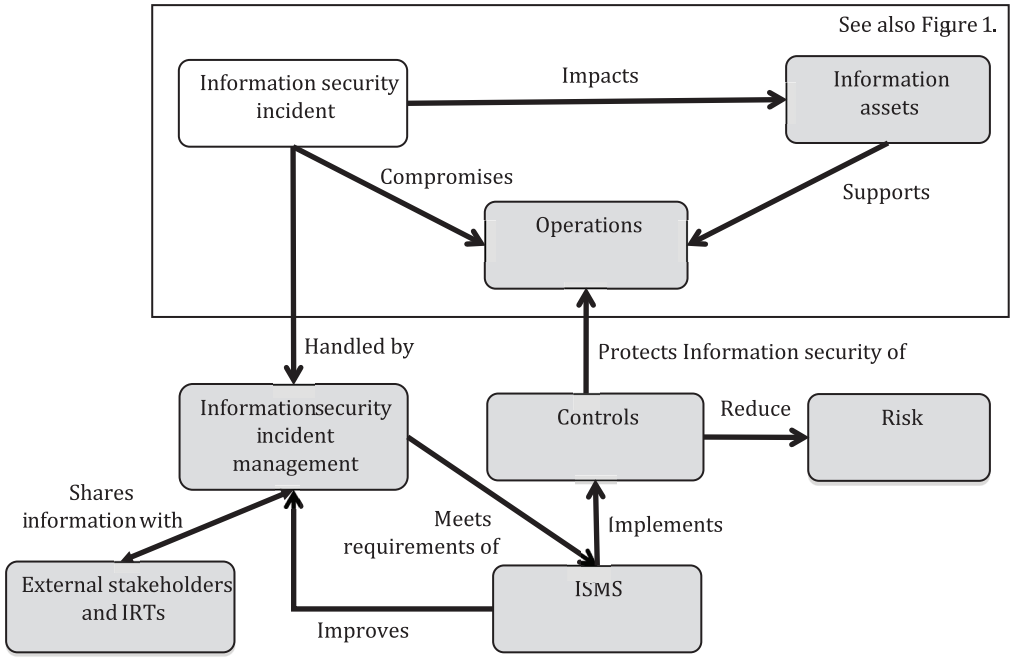

Figure 2 — Information security incident management in relation to ISMS and applied controls

4.3 Benefits of a structured approach

Using a structured approach to information security incident management can yield significant benefits, which can be grouped under the following topics.

a) Improving overall information security

A structured process for detection, reporting and assessment of and decision-making related to information security events and incidents will enable rapid identification and response. This will improve overall security by helping to quickly identify and implement a consistent solution, and thus provide a means of preventing future similar information security incidents. Furthermore, there will be benefits gained by metrics, sharing and aggregation. The credibility of the organization will be improved by the demonstration of its implementation of best practices with respect to information security incident management.

b) Reducing adverse business impacts

A structured approach to information security incident management can assist in reducing the level of potential adverse business impacts associated with information security incidents. These impacts can include immediate financial loss and longer-term loss arising from damaged reputation and credibility. For guidance on business impact analysis, see ISO/IEC 27005. For guidance on information and communication technology readiness for business continuity, see ISO/IEC 27031.

c) Strengthening the focus on information security incident prevention

Using a structured approach to information security incident management helps to create a better focus on incident prevention within an organization, including the development of methods to identify new threats and vulnerabilities. Analysis of incident-related data enables the identification of patterns and trends, thereby facilitating a more accurate focus on incident prevention and identification of appropriate actions to prevent further occurrence.

d) Improving prioritization

A structured approach to information security incident management will provide a solid basis for prioritization when conducting information security incident investigations, including the use of effective categorization and classification scales. If there are no clear procedures, there is a risk that investigation activities could be conducted in an overly reactive mode, responding to incidents as they occur and overlooking what activities should be handled with a higher priority.

e) Supporting evidence collection and investigation

If and when needed, clear incident investigation procedures will help to ensure that data collection and handling are evidentially sound and legally admissible. These are important considerations if legal prosecution or disciplinary action might follow. For more information on digital evidence and investigation, see the investigative standards in Annex A.

f) Contributing to budget and resource justifications

A well-defined and structured approach to information security incident management will help justify and simplify the allocation of budgets and resources for involved organizational units. Furthermore, benefit will accrue for the information security incident management plan itself, with the ability to better plan for the allocation of staff and resources.

One example of a way to control and optimize budget and resources is to add time tracking to information security incident management tasks to facilitate quantitative assessment of the organization's handling of information security incidents. It should be possible to provide information on how long it takes to resolve information security incidents of different priorities and on different platforms. If there are bottlenecks in the information security incident management process, these should also be identifiable.

g) Improving updates to information security risk assessment and management results

The use of a structured approach to information security incident management will facilitate:

— better collection of data for assisting in the identification and determination of the characteristics of the various threat types and associated vulnerabilities, and

— provision of data about frequencies of occurrence of the identified threat types.

The data collected about adverse impacts on business operations from information security incidents will be useful in business impact analysis. The data collected to identify the frequency of various threat types will improve the quality of a threat assessment. Similarly, the data collected on vulnerabilities will improve the quality of future vulnerability assessments. For guidance on information security risk assessment and management, see ISO/IEC 27005.

h) Providing enhanced information security awareness and training program material

A structured approach to information security incident management will enable an organization to collect experience and knowledge of how the organization handles incidents, which will be valuable material for an information security awareness program. An awareness program that includes lessons learnt from real experience will help reduce mistakes or confusion in future information security incidents.

i) Providing input to the information security policy and related documentation reviews

Data provided by an information security incident management plan could provide valuable input to reviews of the effectiveness and subsequent improvement of incident management security policies (and other related information security documents). This applies to topic-specific policies and other documents applicable both for organization-wide and for individual systems, services and networks.

4.4 Adaptability

The guidance provided by ISO/IEC 27035 (all parts) is extensive and, if adopted in full, could require significant resources to operate and manage. It is therefore important that an organization applying this guidance should retain a sense of perspective and ensure that the resources applied to information security incident management and the complexity of the mechanisms implemented are proportional to the following:

a) size, structure and business nature of an organization including key critical assets, processes, and data that should be protected;

b) scope of any information security management system for incident handling;

c) potential risk due to incidents;

d) the goals of the business.

An organization using this part of ISO/IEC 27035 should therefore adopt its guidance in a manner that is relevant to the scale and characteristics of its business.

5 Phases

5.1 Overview

To achieve the objectives outlined in 4.2, information security incident management consists of the following five distinct phases:

— Plan and Prepare (see 5.2);

— Detection and Reporting (see 5.3);

— Assessment and Decision (see 5.4);

— Responses (see 5.5);

— Lessons Learnt (see 5.6).

A high-level view of these phases is shown in Figure 3.

Some activities can occur in multiple phases or throughout the incident handling process. Such activities include the following:

— documentation of event and incident evidence and key information, response actions taken, and follow-up actions done as part of the incident handling process;

— coordination and communication between the involved parties;

— notification of significant incidents to management and other stakeholders;

— information sharing between stakeholders and internal and external collaborators such as vendors and other IRTs.

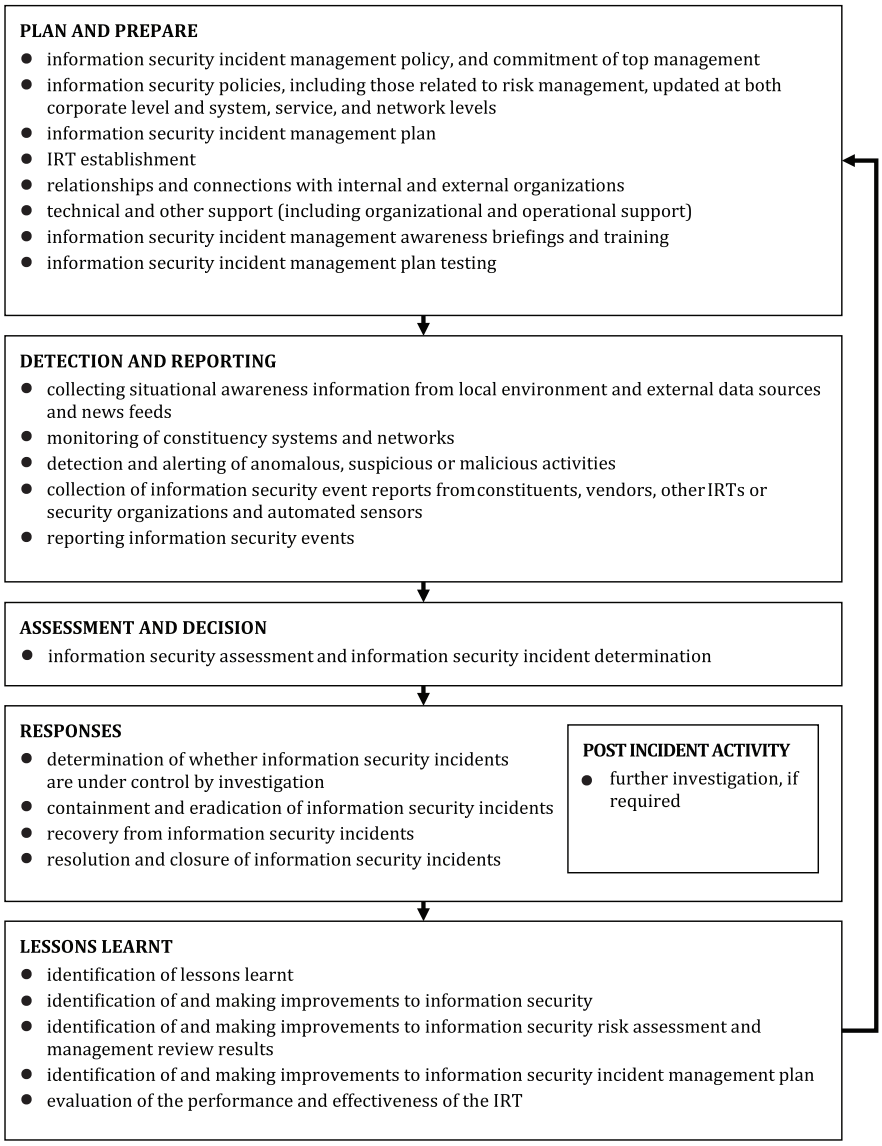

Figure 3 — Information security incident management phases

As noted in the Introduction, ISO/IEC 27035 is in two parts.

— ISO/IEC 27035-1 covers all five phases.

— ISO/IEC 27035-2 covers

  — Plan and Prepare, and

  — Lessons Learnt

Figure 4 shows the flow of information security events and incidents through information security incident management phases and related activities.

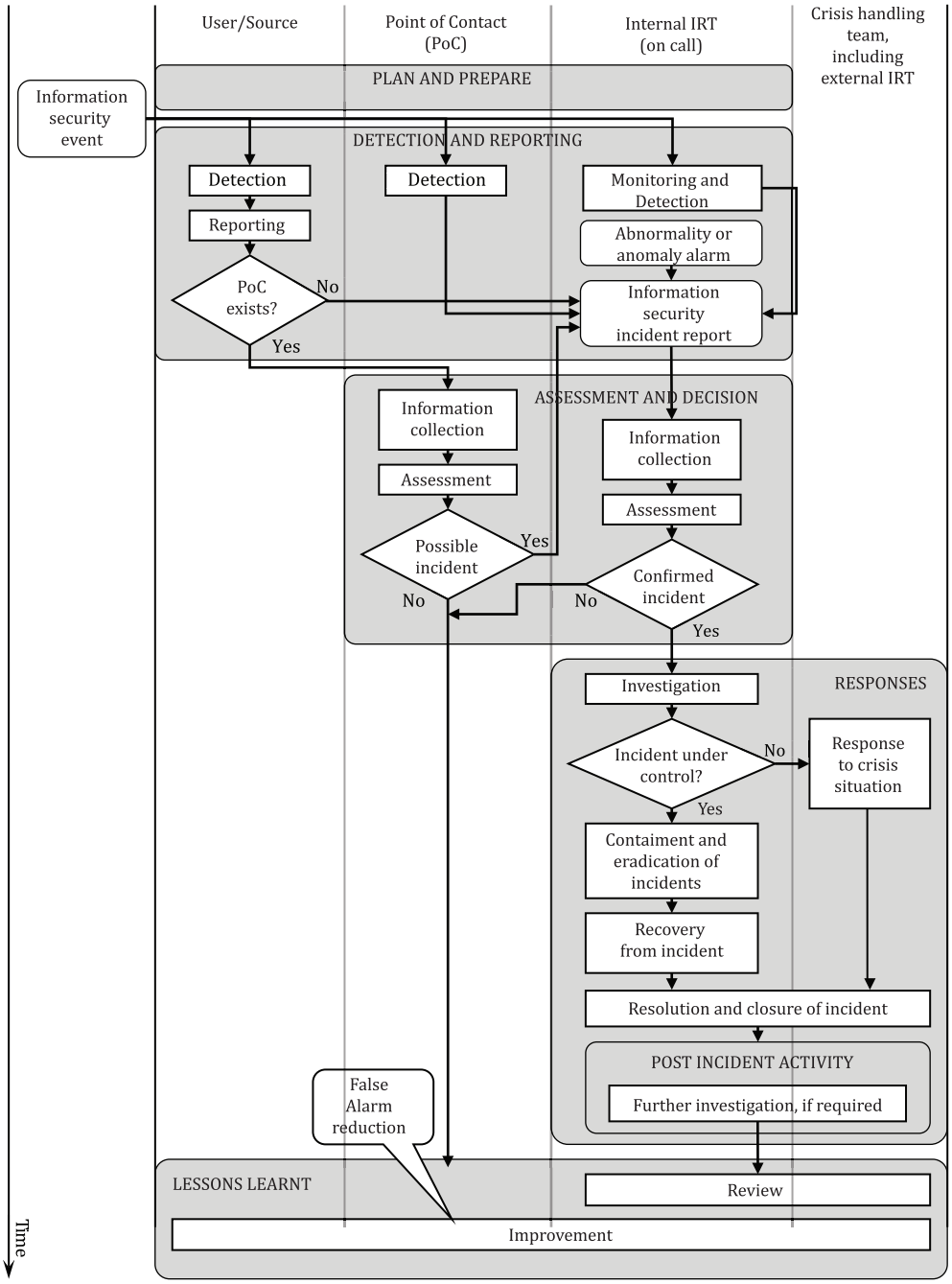

Figure 4 — Information security event and incident flow diagram

5.2 Plan and Prepare

Effective information security incident management requires appropriate planning and preparation. For an efficient and effective information security incident management plan to be put into operation, an organization should complete a number of preparatory activities, namely:

a) formulate and produce an information security incident management policy and gain top management commitment to that policy;

b) update information security policies, including those related to risk management, at a corporate level and specific system, service and network levels;

c) define and document a detailed information security incident management plan, including topics covering communications and information disclosure;

d) establish the IRT, with an appropriate training program designed, developed, and provided to its personnel;

e) establish and preserve appropriate relationships and connections with internal and external organizations that are directly involved in information security event, incident and vulnerability management;

f) establish, implement and operate technical, organizational and operational mechanisms to support the information security incident management plan and the work of the IRT. Develop and deploy necessary information systems to support the IRT, including an information security database. These mechanisms and systems are intended to prevent information security incident occurrences or reduce the likelihood of occurrences of information security incidents;

g) design and develop an awareness and training program for information security event, incident and vulnerability management;

h) test the use of the information security incident management plan, its processes and procedures.

With this phase completed, organizations should be fully prepared to properly manage information security incidents. ISO/IEC 27035-2 describes each of the activities listed above, including the contents of policy and planning documents.

5.3 Detection and Reporting

The second phase of information security incident management involves the detection of, collection of information associated with, and reporting on occurrences of information security events and the existence of information security vulnerabilities by manual or automatic means. In this phase, events and vulnerabilities might not yet be classified as information security incidents.

The reporting of security events in line with the organization's reporting policies enables later analysis if required.

For the Detection and Reporting phase, an organization should undertake the following key activities:

a) monitor and log system and network activity of constituency or parent organizations as appropriate;

b) detect and report the occurrence of an information security event or the existence of an information security vulnerability, whether manually by personnel or automatically;

c) collect information on an information security event or vulnerability;

d) collect situational awareness information from internal and external data sources including local system and network traffic and activity logs, news feeds concerning ongoing political, social, or economic activities that might impact incident activity, external feeds on incident trends, new attack vectors, current attack indicators and new mitigation strategies and technologies;

e) ensure that all activities, results and related decisions are properly logged for later analysis;

f) ensure that digital evidence is gathered and stored securely, and that its secure preservation is continually monitored, in case the evidence is required for legal prosecution or internal disciplinary action. For more detailed information on the identification, collection, acquisition and preservation of digital evidence, see the investigative standards in Annex A;

g) ensure that a change control regime is followed to enable information security event and vulnerability tracking and report updates, and to keep the information security database up-to-date;

h) escalate, on an as-needed basis throughout the phase, for further review or decisions.

All information collected pertaining to an information security event or vulnerability should be stored in the information security database managed by the IRT. The information reported during each activity should be as complete as possible at the time. This will support assessments, decisions and actions to be taken.

5.4 Assessment and Decision

The third phase of information security incident management involves the assessment of information associated with occurrences of information security events and the decision on whether to classify events as information security incidents.

Once an information security event has been detected and reported, the subsequent activities should be performed:

a) distribute the responsibility for information security incident management activities through an appropriate hierarchy of personnel with assessment, decision making and actions involving both security and non-security personnel;

b) provide formal procedures for each notified person to follow, including reviewing and amending reports, assessing damage, and notifying relevant personnel. Individual actions will depend on the type and severity of the incident;

c) use guidelines for thorough documentation of an information security event and the subsequent actions for an information security incident if the information security event becomes classified as an information security incident.

For the Assessment and Decision phase, an organization should perform the following key activities:

— collect information that can include testing, measuring, and other data gathering about the detection of an information security event. The type and amount of information collected will depend on the information security event that has occurred;

— conduct an assessment by the incident handler to determine whether the event is a possible or confirmed information security incident or a false alarm. A false alarm (i.e. a false positive) is an indication of a reported event that is found not to be real or of any consequence. If desired, the IRT can conduct a quality review to ensure that the incident handler correctly declared an incident;

— ensure that all parties involved, particularly the IRT, properly log all activities, results and related decisions for later analysis;

— ensure that the change control regime is maintained to cover information security incident tracking and incident report updates, and to keep the information security database up-to-date.

All information collected pertaining to an information security event, incident or vulnerability should be stored in the information security database managed by the IRT. The information reported during each activity should be as complete as possible at the time. This will support assessments, decisions and actions to be taken.

5.5 Responses

The fourth phase of information security incident management involves responding to information security incidents in accordance with the actions determined in the Assessment and Decision phase. Depending on the decisions, the responses could be made immediately, in real-time, or in near real-time, and some responses could involve information security investigation.

Once an information security incident has been confirmed and the responses determined, the subsequent activities should be undertaken:

a) distribute the responsibility for information security incident management activities through an appropriate hierarchy of personnel with decision making and actions, involving both security and non-security personnel as necessary;

b) provide formal procedures for each involved person to follow, including reviewing and amending the reports, re-assessing damage, and notifying the relevant personnel. Individual actions will depend on the type and severity of the incident;

c) use guidelines for thorough documentation of an information security incident and subsequent actions.

For the Responses phase, an organization should perform the following key activities:

— investigate incidents as required and relative to the information security incident classification scale rating. The scale should be changed as necessary. Investigation can include different kinds of analyses to provide a more in-depth understanding of incidents.

— review by the IRT to determine whether the information security incident is under control, and if so, perform the required response. If the incident is not under control or it is going to have a severe impact on the organization's operations, perform crisis response activities through escalation to the crisis handling function.

— assign internal resources and identify external resources in order to respond to an incident.

— escalate as needed throughout the phase for further assessments or decisions.

— ensure that all parties involved, particularly the IRT, properly log all activities for later analysis.

— ensure that digital evidence is gathered and stored provably securely, and that its secure preservation is continually monitored, in case the evidence is required for legal prosecution or internal disciplinary action. For more detailed information on the identification, collection, acquisition and preservation of digital evidence, see the investigative standards in Annex A.

— ensure that the change control regime is maintained to cover information security incident tracking and incident report updates, and to keep the information security database up-to-date.

— communicate the existence of the information security incident and share any relevant details (e.g. threat, attack, and vulnerability information) with other internal and external individuals or organizations, in accordance with organizational and IRT communication plans and information disclosure policies. It can be particularly important to notify asset owners (determined during the impact analysis) and internal and external organizations (e.g. other incident response teams, law enforcement agencies, Internet service providers, and information sharing organizations) that could assist with the management and resolution of the incident. Sharing information could also benefit other organizations since the same threats and attacks often affect multiple organizations. For further detail about information sharing, see ISO/IEC 27010.

— after recovery from an incident, a Post Incident Activity should be initiated depending on the nature and severity of the incident. This activity includes

  — investigation of the information pertaining to the incident,

  — investigation of other relevant sources such as involved personnel, and

  - summarized report of the investigation findings.

- once the incident has been resolved, it should be closed according to the requirements of the IRT or parent organization and all stakeholders should be notified.

All information collected pertaining to an information security event, incident, or vulnerability should be stored in the information security database managed by the IRT. The information reported during each activity should be as complete as possible at the time. This will support assessments, decisions and actions to be taken, including potential further analysis.

5.6 Lessons Learnt

The fifth phase of information security incident management occurs when information security incidents have been resolved. This phase involves learning lessons from how incidents (and vulnerabilities) have been handled.

For the Lessons Learnt phase, an organization should perform the following key activities:

a) identify the lessons learnt from information security incidents and vulnerabilities;

b) review, identify and make improvements to information security control implementation (new or updated controls), as well as information security incident management policy. Lessons can come from one or many information security incidents or reported security vulnerabilities. Improvements are aided by metrics fed into the organization's strategy on where to invest in information security controls;

c) review, identify and make improvements to the organization's existing information security risk assessment and management reviews;

d) review how effective the processes, procedures, reporting formats and organizational structure were in responding to, assessing and recovering from information security incidents and dealing with information security vulnerabilities. On the basis of the lessons learnt, identify and make improvements to the information security incident management plan and its documentation;

e) communicate and share the results of review within a trusted community (if the organization so wishes);

f) determine if the incident information, associated attack vectors and vulnerabilities may be shared with partner organizations to assist in preventing the same incidents from occurring in their environments. For more details, see ISO/IEC 27010 on information sharing;

g) perform a comprehensive evaluation of IRT performance and effectiveness on a periodic basis.

It is emphasized that information security incident management activities are iterative, and therefore an organization should make regular improvements to a number of information security elements over time. These improvements should be proposed on the basis of reviews of the data on information security incidents, responses, and reported information security vulnerabilities.

ISO/IEC 27035-2 describes in detail each of the activities listed above.

Annex B
(informative)

Examples of information security incidents and their causes

B.1 Attacks

B.1.1 Denial of Service

Denial of Service (DoS) and Distributed Denial of Service (DDoS) are a broad category of incidents with a common thread. Such incidents cause a system, service or network to fail to continue operating in its intended capacity, most often with complete denial of access to legitimate users. There are two main types of DoS/DDoS incidents caused by technical means: resource elimination and resource starvation.

Typical examples of deliberate technical DoS/DDoS incidents include the following:

— pinging network broadcast addresses in order to fill up network bandwidth with response traffic;

— sending data in an unexpected format to a system, service or network in an attempt to crash it, or disrupt its normal operation;

— opening up multiple authorized sessions with a particular system, service or network in an attempt to exhaust its resources (i.e. to slow it down, lock it up or crash it).

Such attacks are often performed through bots, a computer system running malware that is controlled via a botnet. A botnet is a central bot command and control network managed by humans. Botnet sizes can range from hundreds to millions of affected computers.

Some technical DoS incidents can be caused accidentally, for example, caused by operator misconfiguration or through incompatibility of application software, but most of the time, they are deliberate. Some technical DoS incidents are intentionally launched in order to crash a system or service, or take down a network, while others are merely the by-products of other malicious activity. For instance, some of the more common stealth scanning and identification techniques can cause older or misconfigured systems or services to crash when scanned. It should be noted that many deliberate technical DoS incidents are often executed anonymously (i.e. the source of the attack is “faked”), since they typically do not rely on the attacker receiving any information back from the network or system being attacked.

DoS incidents caused by non-technical means, resulting in loss of information, service and/or facilities, could be caused, for example, by

— breaches of physical security arrangements resulting in theft or wilful damage and destruction of equipment,

— accidental damage to hardware (and/or its location) by fire or water damage/flood,

— extreme environmental conditions, for example high operating temperatures (e.g. due to air conditioning failure),

— system malfunctions or overload,

— uncontrolled system changes, and

— malfunctions of software or hardware.

B.1.2 Unauthorized access

In general, this category of incidents consists of actual unauthorized attempts to access or misuse a system, service or network. Some examples of technical unauthorized access incidents include

— attempts to retrieve password files,

— buffer overflow attacks to attempt to gain privileged (e.g. system administrator) access to a target,

— exploitation of protocol vulnerabilities to hijack or misdirect legitimate network connections, and

— attempts to elevate privileges to resources or information beyond what a user or administrator already legitimately possesses.

Unauthorized access incidents caused by non-technical means, resulting in direct or indirect disclosure or modification of information, breaches of accountability or misuse of information systems, could be caused, for example, by

— breaches of physical security arrangements resulting in unauthorized access to information, and

— poorly and/or mis-configured operating systems due to uncontrolled system changes, or malfunctions of software or hardware.

B.1.3 Malware

Malware identifies a program or part of a program inserted into another program with the intent to modify its original behaviour, usually to perform malicious activities as information and identify theft, information and resource destruction, Denial of Service, spam, etc. Malware attacks could be divided into five categories: viruses, worms, Trojan horses, mobile code and blended. Whilst viruses are created to target any vulnerable infected system, other malware are also used to perform targeted attacks. This is sometimes performed by modifying existing malware and creating a variant that often is not recognized by malware detection technologies.

B.1.4 Abuse

This kind of incident occurs when a user violates an organization's information system security policies. Such incidents are not attacks in the strict sense of the word, but are often reported as incidents and should be managed by an IRT. Inappropriate usage could be

— downloading and installing hacking tools,

— using corporate e-mail for spam or promotion of personal business,

— using corporate resources to set up an unauthorized web site, and

— using peer-to peer activities to acquire or distribute pirated files (music, video, software).

B.2 Information gathering

In general terms, the information gathering category of incidents includes those activities associated with identifying potential targets and understanding the services running on those targets. This type of incident involves reconnaissance, with the goal being to identify the

— existence of a target, and to understand the network topology surrounding it, and with whom the target routinely communicates, and

— potential vulnerabilities in the target or its immediate network environment that could be exploited.

Typical examples of information gathering attacks by technical means include the following:

— dumping Domain Name System (DNS) records for the target's Internet domain (DNS zone transfer);

— pinging network addresses to find systems that are “alive”;

— probing the system to identify (e.g. fingerprint) the host operating system;

— scanning the available network ports on a system to identify network services (e.g. e-mail, File Transfer Protocol (FTP), web, etc.) and the software versions of those services;

— scanning for one or more known vulnerable services across a network address range (horizontal scanning).

In some cases, technical information gathering extends into unauthorized access if, for example, as part of searching for vulnerabilities, the attacker also attempts to gain unauthorized access. This commonly occurs with automated tools that not only search for vulnerabilities but also automatically attempt to exploit the vulnerable systems, services and/or networks that are found.

Information gathering incidents caused by non-technical means, resulting in

— direct or indirect disclosure or modification information,

— theft of intellectual property stored electronically,

— breaches of accountability, e.g. in account logging, and

— misuse of information systems (e.g. contrary to law or organization policy).

Information gathering incidents could be caused, for example, by

— breaches of physical security arrangements resulting in unauthorized access to information, and theft of data storage equipment that contains important data, for example encryption keys,

— poorly and/or misconfigured operating systems due to uncontrolled system changes, or malfunctions of software or hardware, resulting in internal or external personnel gaining access to information for which they have no authority, and

— social engineering, which is an act of manipulating people into performing actions or divulging confidential information, e.g. phishing.