TECHNICAL REPORT

ISO/IEC TR 18044

First edition
2004-10-15

Information technology — Security techniques — Information security incident management

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

Reference number
ISO/IEC TR 18044:2004(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

ISO/IEC TR 18044, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

No typical information security policies or safeguards will guarantee total protection of information, information systems, services or networks. After safeguards have been implemented, residual weaknesses are likely to remain that may make information security ineffective and thus information security incidents possible, potentially with both direct and indirect adverse impacts on an organization's business operations. Further, inevitably new previously unidentified threats will occur. Insufficient preparation by an organization to deal with such incidents will make any actual response less effective, and potentially increase the degree of potential adverse business impact. Therefore it is essential for any organization that is serious about information security to have a structured and planned approach to:

- detect, report and assess information security incidents,
- respond to information security incidents, including by the activation of appropriate safeguards for the prevention and reduction of, and recovery from, impacts (for example in the support and business continuity planning areas),
- learn from information security incidents, institute preventive safeguards, and, over time, make improvements to the overall approach to information security incident management.

Information technology — Security techniques — Information security incident management

1 Scope

This Type 3 Technical Report (TR) provides advice and guidance on information security incident management for information security managers, and information system, service and network managers.

This TR contains 11 clauses and is organized in the following manner. Clause 1 describes the scope and is followed by a list of references in Clause 2 and terms and definitions in Clause 3. Clause 4 provides some background to information security incident management, and that is followed by a summary of the benefits and key issues in Clause 5. Examples of information security incidents and their causes are then provided in Clause 6. The planning and preparation for information security incident management, including document production, is then described in Clause 7. The operational use of the information security incident management scheme is described in Clause 8. The review phase of information security management, including the identification of lessons learnt and improvements to security and the information security incident management scheme, is described in Clause 9. The improvement phase, i.e. making identified improvements to security and the information security incident management scheme, is described in Clause 10. Finally, the TR concludes with a short summary in Clause 11. Annex A contains example information security event and incident report forms, and Annex B contains some example outline guidelines for assessing the adverse consequences of information security incidents, for inclusion in the reporting forms. The Annexes are followed by the Bibliography.

2 Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 13335-1:2004, *IT security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

ISO/IEC 17799:2000, *Information technology — Code of practice for information security management*

3 Terms and Definitions

For the purposes of this document the terms and definitions given in ISO/IEC 13335-1, ISO/IEC 17799 and the following apply.

3.1 Business continuity planning

Business continuity planning is the process to ensure that recovery of operations will be assured should any unexpected or unwanted incident occur that is capable of negatively impacting the continuity of essential business functions and supporting elements. The process should also ensure that recovery is achieved in the required priorities and timescales, and subsequently all business functions and supporting elements will be recovered back to normal.

The key elements of this process need to ensure that the necessary plans and facilities are put in place, and tested, and that they encompass information, business processes, information systems and services, voice and data communications, people and physical facilities.

3.2 Information security event

An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

3.3 Information security incident

An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. (Examples of information security incidents are shown in Clause 6.)

3.4 ISIRT (Information Security Incident Response Team)

An ISIRT is a team of appropriately skilled and trusted members of the organization, which will handle information security incidents during their lifecycle. At times this team may be supplemented by external experts, for example from a recognized computer incident response team or Computer Emergency Response Team (CERT).

3.5 Other

Also see the definitions in ISO/IEC JTC1 SC27 SD6, Glossary.

4 Background

4.1 Objectives

As a key part of any organization's overall information security strategy, it is essential to have in place a structured well-planned approach to the management of information security incidents.

The objectives of this approach are to ensure that:

- information security events can be detected and dealt with efficiently, in particular in identifying whether they need to be categorized as information security incidents or not,[1]
- identified information security incidents are assessed and responded to in the most appropriate and efficient manner,
- the adverse impacts of information security incidents on the organization and its business operations can be minimized by appropriate safeguards as part of the incident response, possibly in conjunction with relevant elements from a business continuity plan or plans,
- lessons can be quickly learnt from information security incidents and their management. This is to increase the chances of preventing future information security incidents occurring, improve the implementation and use of information security safeguards, and improve the overall information security incident management scheme.

4.2 Processes

To achieve the objectives outlined in Clause 4.1, information security incident management consists of four distinct processes:

- Plan and Prepare,
- Use,
- Review,
- Improve.

[1] It should be noted that information security events could be the result of accidental or intentional attempts to breach information security safeguards, but in most cases an information security event alone does not imply that an attempt has really been successful and therefore doesn't need to have any implications on confidentiality, integrity and/or availability, i.e. not all information security events will be categorized as information security incidents.

(It should be noted that these processes are similar to those reflected in the "Plan, Do, Check and Act' model in IS 9000 and IS 14000.)

A high level view of these processes is shown in Figure 1 below.

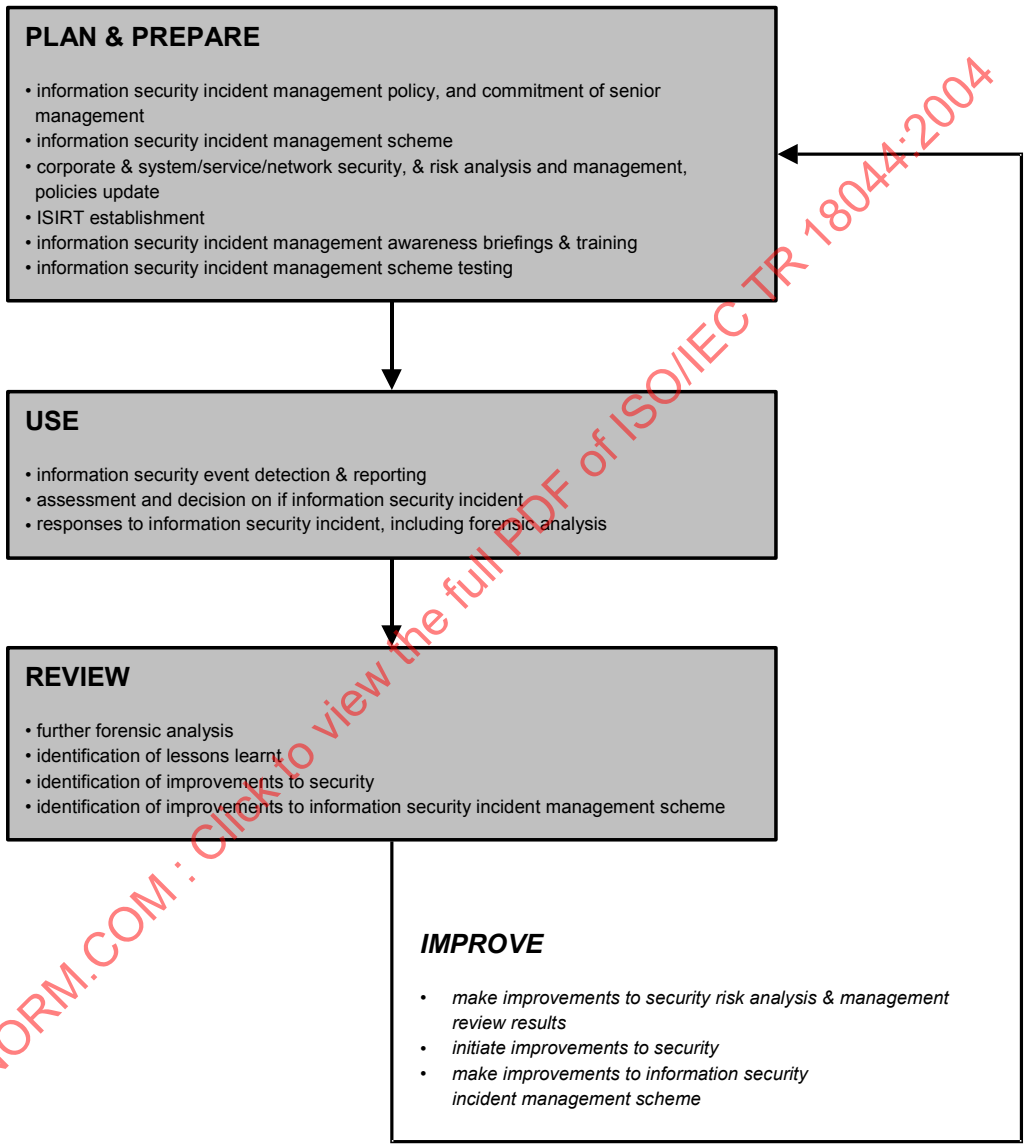

Figure 1- Information Security Incident Management Processes

4.2.1 Plan and Prepare

Effective information security incident management requires appropriate planning and preparation. For responses to information security incidents to be effective, the following actions are necessary:

- develop and document an information security incident management policy and gain visible commitment to that policy from all key stakeholders, particularly senior management,
- develop and comprehensively document an information security incident management scheme to support the information security incident management policy. Forms, procedures and support tools, for the detection, reporting, assessment and response to information security incidents, and details of the incident severity scale[2], should be encompassed within scheme documentation. (It should be noted that in some organizations, the scheme may be referred to as an information security incident response plan.),
- update information security and risk management policies at all levels, i.e. corporate-wide and for each system, service and network, with references to the information security incident management scheme,
- establish an appropriate information security incident management organizational structure, i.e. the Information Security Incident Response Team (ISIRT), with defined roles and responsibilities allocated to personnel who are available to enable an adequate response to all known types of information security incident. Within most organizations the ISIRT will be a virtual team, with a senior manager leading the team supported by groups of individuals specialized in particular topics, e.g. in the handling of malicious code attacks, who will be called upon depending on the type of incident concerned,
- make all organizational personnel aware through briefings and/or other mechanisms, of the existence of the information security incident management scheme, its benefits and how to report an information security event. Appropriate training should be provided to those personnel responsible for managing the information security incident management scheme, decision makers involved in determining whether information security events are incidents, and those individuals involved in the investigation of incidents,
- thoroughly test the information security incident management scheme.

The Plan and Prepare phase is further described in Clause 7.

4.2.2 Use

The following processes are necessary to make use of an information security incident management scheme:

- detecting and reporting the occurrence of information security events (by human or automatic means),
- collecting information associated with information security events, and assessing that information to determine what events are to be categorized as information security incidents,
- making responses to information security incidents:
  - immediately, in real-time or in near real-time,
  - where information security incidents are under control, conducting activities that may be required in slower time (for example, in facilitating full recovery from a disaster),
  - if information security incidents are not under control, instigating 'crisis' activities (for example, calling the fire brigade/department or activating a business continuity plan),
  - communicating the existence of information security incidents and any relevant details thereof to internal and external people and/or organizations. (This could include escalating for further assessments and/or decisions as required.),

[2] An incident severity scale to be used to 'grade' incidents should be established. This scale could, for example, be 'major' and 'minor', with, in any event, the decision based on the actual or projected adverse impacts on the organization's business operations.

- forensic analysis,
- properly logging all activities and decisions for further analysis,
- closing incidents on resolution.

The Use phase is further described in Clause 8.

4.2.3 Review

After information security incidents have been resolved/closed, the following review activities are necessary:

- conducting further forensic analysis, as required,
- identifying the lessons learnt from information security incidents,
- identifying improvements to information security safeguard implementation, as result of the lessons learnt, whether from one information security incident or many,
- identifying improvements to the information security incident management scheme as a whole, as a result of lessons learnt from quality assurance reviews of the approach (for example, from review of the effectiveness of the processes, procedures, the reporting forms and/or the organizational structure).

The Review phase is further described in Clause 9.

4.2.4 Improve

It is emphasized that the information security incident management processes are iterative, with regular improvements made to a number of information security elements over time. These improvements will be proposed on the basis of reviews of the data on information security incidents and the responses to them, as well as trends over time. This will include:

- revising the organization's existing information security risk analysis and management review results,
- making improvements to the information security incident management scheme and its documentation,
- initiating improvements to security, that may encompass the implementation of new and/or updated information security safeguards.

The Improve phase is further described in Clause 10.

5 Benefits and Key Issues

This clause provides information on the:

- benefits to be obtained from a good information security incident management scheme,
- key issues that need to be addressed to convince senior corporate management and those personnel who will report to and receive feedback from the scheme.

5.1 Benefits

Any organization using a structured approach to information security incident management may accrue significant benefits, which can be grouped under:

- improving information security,

- reducing adverse business impacts, for example disruption and financial loss, caused as a consequence of information security incidents,
- strengthening the information security incident prevention focus,
- strengthening of prioritization and evidence,
- contributing to budget and resource justifications,
- improving updates to risk analysis and management results,
- providing enhanced information security awareness and training program material,
- providing input to information security policy and related documentation reviews.

Each of these topics is introduced below.

5.1.1 Improving Security

A structured process for detecting, reporting, assessing and managing information security events and incidents enables rapid identification and response to any information security event or incident, thus improving overall security by helping to quickly identify and implement a consistent solution, providing a means of preventing future similar information security incidents.

5.1.2 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.

5.1.3 Strengthening Incident Prevention Focus

Using a structured approach to information security incident management can help to create a better focus on incident prevention within an organization. Analysis of incident related data will enable the identification of patterns and trends, thereby facilitating a more accurate focus on incident prevention and thus identification of appropriate actions to prevent incidents occurring.

5.1.4 Strengthening of Prioritization and Evidence

A structured approach to information security incident management will provide a solid basis for prioritization when conducting information security incident investigations.

If there are no clear procedures, there is a risk that investigation activities could be conducted in a reactive mode, responding to incidents as they occur and to the “loudest voice” of related management. This could prevent investigation activities from being directed where they are really needed and in the ideal priority.

Clear incident investigation procedures can 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. It should be recognized however, that there is a chance that the actions necessary to recover from an information security incident might jeopardize the integrity of any such collected evidence.

5.1.5 Budget and Resources

A well-defined and structured approach to information security incident management will help justify and simplify the allocation of budgets and resources within involved organizational units. Further, benefit will accrue for the information security incident management scheme itself, with the:

- use of less skilled staff to identify and filter out the false alarms,
- provision of better direction for the activities of skilled personnel,

- engagement of skilled personnel only for those processes where their skills are needed and only at the stage of the process where their contribution is needed.

In addition, a structured approach to information security incident management can include 'time stamping' so that it is possible to make 'quantitative' assessments of the organization's handling of security incidents. It should, for example, be possible to provide information on how long it takes to resolve incidents of different priorities and on different platforms. If there are bottlenecks in the information security incident management process, these should also be identifiable.

5.1.6 Information Security Risk Analysis and Management

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

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

- provision of data on frequencies of occurrence of the identified threat types.

The data gained on the adverse impacts on business operations from information security incidents will be useful in the business impact analysis. The data gained identifying the occurrence frequency of the various threat types will greatly aid the quality of the threat assessment. Similarly, the data gained on vulnerabilities will greatly aid the quality of future vulnerability assessments.

This data will greatly improve information security risk analysis and management review results.

5.1.7 Information Security Awareness

A structured approach to information security incident management will provide focused information for information security awareness programs. This focused information will provide a source of real example information capable of demonstrating that information security incidents do actually happen to the organization, and not always "to somebody else". It will also be possible to demonstrate the benefits associated with the rapid availability of solution information. Furthermore, such awareness helps to reduce a mistake or panic/confusion by an individual in the event of an information security incident.

5.1.8 Input to Information Security Policy Review

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

5.2 Key Issues

Feedback on the way information security incidents have been managed will assist personnel to ensure that their work remains focused on the real risks to the organization's systems, services and networks. This important feedback cannot be as effectively provided through dealing with information security incidents as they occur on an ad hoc basis. It can be more effectively provided through the use of a structured well-designed information security incident management scheme that uses a common framework for all parts of the organization. This framework should continually enable more comprehensive results to be produced from the scheme, and allow a solid base for the rapid identification of possible information security incident conditions to be represented before an information security incident occurs, sometimes called "alerts".

The management and audit of the information security management scheme should provide the basis for the trust necessary to facilitate widespread participation, and to allay any concerns about the preservation of anonymity, security and the availability of useful results. For example, management and operations personnel need to be confident that "alerts" will give timely, relevant, accurate, concise and complete information.

Organizations need to avoid potential problems in implementing information security incident management schemes, such a lack of useful results and concerns about privacy related issues. It is necessary to convince stakeholders that steps have been taken to prevent such problems occurring.

Thus, a number of key issues should be addressed to achieve a good information security incident management scheme, including:

- management commitment,
- awareness,
- legal and regulatory aspects,
- operational efficiency and quality,
- anonymity,
- confidentiality,
- credible operations,
- typology.

Each of these issues is discussed below.

5.2.1 Management Commitment

Ensuring continued management commitment is vital for the acceptance of a structured approach to information security incident management. Personnel need to recognize an incident and know what to do, and even understand the broad benefits of the approach to the organization. However, unless management is supportive, little will happen. The idea needs to be sold to management so that the organization commits to resourcing and maintaining an incident response capability.

5.2.2 Awareness

Another important issue for the acceptance of a structured approach to information security incident management is that of awareness. Whilst users should be required to participate, if they are not aware of how they and their part of the organization may benefit from participating in a structured approach to information security incident management, they are less likely to participate effectively in its operation.

Any information security incident management scheme should be accompanied with an awareness program definition document that includes details of the:

- benefits to be derived from the structured approach to information security incident management, both to the organization and to its personnel,
- incident information held in, and the outputs from, the information security event/incident database,
- strategy and mechanisms for an awareness program, that, depending on the organization, could be standalone or part of a broader information security awareness program.

5.2.3 Legal and Regulatory Aspects

The following legal and regulatory aspects of information security incident management should be addressed in the information security incident management policy and associated scheme.

- **Adequate Data Protection and Privacy of Personal Information is Provided.** In those countries where specific legislation exists that covers data confidentiality and integrity, it is often restricted to the control of personal data. As information security incidents need to be typically attributable to an individual, information of a personal nature may therefore need to be recorded and managed accordingly. A structured approach to information security incident management therefore needs to take into account the appropriate privacy protection. This may include:

  - those individuals with access to the personal data should, so far as is practical, not personally know the person(s) being investigated;
  - non-disclosure agreements should be signed by those individuals with access to the personal data prior to them being allowed access to it;
  - information should only be used for the express purpose for which it has been obtained, i.e. for information security incident investigation.

- **Appropriate Record Keeping is Maintained.** Some national laws require that companies maintain appropriate records of their activities for review in the annual organization audit process. Similar requirements exist with regard to government organizations. In certain countries organizations are required to report or to generate archives for law enforcement (e.g. regarding any case that may involve a serious crime or penetration of a sensitive government system).

- **Safeguards are in place to Ensure Fulfillment of Commercial Contractual Obligations.** Where there are binding requirements on the provision of an information security incident management service, for example covering required response times, an organization should ensure that appropriate information security is provided to ensure that such obligations can be met in all circumstances. (Related to this, if an organization contracts with an external party for support (see Clause 7.5.4), for example a CERT, then it should be ensured that all requirements, including response times, are included in the contract with the external party.)

- **Legal Issues related to Policies and Procedures are dealt with**. The policies and procedures associated with the information security incident management scheme should be checked for potential legal and regulatory issues, for example if there are statements about disciplinary and/or legal action taken against those causing incidents. In some countries it not easy to terminate employment.

- **Disclaimers are Checked for Legal Validity.** All disclaimers regarding actions taken by the information incident management team, and any external support personnel, should be checked for legal validity.

- **Contracts with External Support Personnel cover all Required Aspects.** Contracts with any external support personnel, for example from a CERT, should be thoroughly checked regarding waivers on liability, non-disclosure, service availability, and the implications of incorrect advice.

- **Non-Disclosure Agreements are Enforceable**. Information security incident management team members may be required to sign non-disclosure agreements both when starting and leaving employment. In some countries, having signed non-disclosure agreements may not be effective in law; this should be checked.

- **Law Enforcement Requirements are Addressed**. The issues associated with the possibility that law enforcement agencies might legally request information from an information security incident management scheme need to be clear. It may be the case that clarity is required on the minimum level required by law at which incidents should be documented, and how long that documentation should be retained.

- **Liability Aspects are Clear.** The issues of potential liability, and related required safeguards to be in place, need to be clarified. Examples of events which may have associated liability issues are:
  - if an incident could affect another organization (for example, disclosure of shared information), and it is not notified in time and the other organization suffers an adverse impact,
  - if a new vulnerability in a product is discovered, and the vendor is not notified and a major related incident occurs later with major impact on one or more other organizations,
  - a report is not made where, in the particular country, organizations are required to report to or generate archives for law enforcement agencies regarding any case that may involve a serious crime, or penetration of a sensitive government system or part of the critical national infrastructure,
  - information is disclosed that seems to indicate that someone, or an organization, may be involved in an attack. This could damage the reputation and business of the person or organization involved.

  - information is disclosed that there may be a problem with a particular item of software and this is found not to be true.

- **Specific Regulatory Requirements are Addressed**. Where required by specific regulatory requirements, incidents should be reported to a designated body, for example as required in the nuclear power industry.
- **Prosecutions, or Internal Disciplinary Procedures, can be Successful**. The appropriate information security safeguards should be in place, including provably tamper-proof audit trails, to be able to successfully prosecute, or bring internal disciplinary procedures against, 'attackers', whether the attacks are technical or physical. In support of this, evidence will typically need to be collected in a manner that is admissible in the appropriate national courts of law or other disciplinary forum. It must be possible to show that:

  - records are complete and have not been tampered with in any way,
  - copies of electronic evidence are provably identical to the originals,
  - any IT system from which evidence has been gathered was operating correctly at the time the evidence was recorded.

- **Legal Aspects Associated with Monitoring Techniques are Addressed.** The implications of using monitoring techniques need to be addressed in the context of the relevant national legislation. The legality of different techniques will vary from country to country. For example, in some countries it is necessary to make people aware that monitoring of activities, including through surveillance techniques, takes place. Factors that need to be considered include who/what is being monitored, how they/it are being monitored, and when the monitoring is occurring. It should also be noted that monitoring/surveillance in the context of IDS is specifically discussed in TR 18043.

- **Acceptable Use Policy is Defined and Communicated.** Acceptable practice/use within the organization should be defined, documented and communicated to all intended users. (For example, users should be informed of the acceptable use policy and asked to provide written acknowledgement that they understand and accept that policy when they join an organization or are granted access to information systems.)

5.2.4 Operational Efficiency and Quality

The operational efficiency and quality of a structured approach to information security incident management relies on a number of factors, including obligation to notify incidents, quality of notification, ease of use, speed and training. Some of these factors relate to making sure that users are aware of the value of information security incident management and being motivated to report incidents. With regard to speed, the time people take to report an incident is not the only factor, but also the time it takes to process data and distribute processed information (especially in the case of alerts). Appropriate awareness and training programs should be complemented by 'hot line' support from information security incident management personnel, in order to minimize delays.

5.2.5 Anonymity

The issue of anonymity is fundamental to the success of information security incident management. Users should be convinced that the information they contribute on information security incidents is completely protected and, where necessary, sanitized such that there exists no way of associating it with their organization or part thereof unless with their full agreement.

The information security management scheme should address situations where it is important to ensure the anonymity of the person or party that reports potential information security incidents under specific circumstances. Each organization should have provisions that clearly illustrate the expectation of anonymity, or lack thereof, for persons or parties reporting a potential information security incident. The ISIRT may need to obtain additional information not initially relayed by the person or party who reported the incident. Furthermore, important information about the information security incident itself can be derived from who detects it first.

5.2.6 Confidentiality

An information security incident management scheme may contain sensitive information, and people involved in addressing incidents may be required to handle sensitive information. During processing either this information should be 'anonymized' or personnel with access to this information required to sign confidentiality agreements. If information security events are logged via a generalized problem management system, sensitive details may also have to be omitted.

Additionally, the information security incident management scheme should have provision for controlling the communication of incidents to external parties, including the media, business partners, customers, law enforcement organizations, and the general public.

5.2.7 Credible Operations

Any information security incident management team should be capable of efficiently satisfying the functional, financial, legal and political needs of the organization and be able to exercise organizational discretion when managing information security incidents. The function of the information security incident management team should also be independently audited to confirm that all business requirements are being satisfied effectively. Further, a good way of achieving another aspect of independence is to separate the incident response reporting chain from operational line management and to make a senior manager directly responsible for managing incident responses. Finance of the capability should also be segregated to avoid undue influence.

5.2.8 Typology

A common typology, reflecting the general structure of the information security incident management approach, will be one of the key factors to enable the provision of consistent results. The typology will, together with common metrics and a standard database structure, provide the capability to compare results, improve alert information and enable a more accurate view of the threats to, and vulnerabilities of, information systems.[3]

6 Examples of Information Security Incidents and their Causes

Information security incidents may be deliberate or accidental (e.g. caused by error or acts of nature), and may be caused by technical or physical means. Their consequences include such events as information being disclosed or modified in an unauthorized manner, destroyed or otherwise being made unavailable, or organizational assets being damaged or stolen. Information security events that are not reported, and determined to be incidents, cannot be investigated, nor can safeguards be taken to prevent any recurrence.

The following descriptions of selected example information security incidents, and their causes, are provided for *illustrative purposes only*. It is important to note that these examples are by no means exhaustive.

6.1 Denial of Service

Denial of service (DoS) is 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 incidents caused by technical means: resource elimination and resource starvation.

Some typical examples of deliberate technical DoS incidents include:

- 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 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).

Some technical DoS incidents may be caused accidentally, for example caused by operator mis-configuration or through incompatibility of application software, but others may be 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 mis-configured 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.

[3] It is not the purpose of this document to define a common typology. The reader is advised to refer to alternative sources for this information.

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,
- malfunctions of software or hardware.

6.2 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, understand the network topology surrounding it, and with whom the target routinely communicates,
- potential vulnerabilities in the target or its immediate network environment that could be exploited.

Typical examples of information gathering attacks by technical means include:

- 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 the related services (e.g. e-mail, FTP, Web, etc.) and the software version 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 hacking 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,
- misuse of information systems (e.g. contrary to law or organization policy),

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 mis-configured 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.

6.3 Unauthorized Access

This category of incidents includes those that do not fall into the first two categories. In general this category of incidents consists of actual unauthorized attempts to access or misuse a system, service or network. Some examples of technically stimulated 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,
- 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,
- poorly and/or mis-configured operating systems due to uncontrolled system changes, or malfunctions of software or hardware, with results similar to those described in the last bullet of clause 6.2 above.

7 Plan and Prepare

The information security incident management planning and preparation phase focuses on:

- documenting the information security event and incident reporting and handling policy, and associated scheme (including related procedures),
- getting the appropriate incident management organizational structure and personnel in place,
- instituting an awareness briefing and training program.

With this phase completed, an organization should be fully prepared to properly manage information security incidents.

7.1 Overview

For an efficient and effective information security incident management scheme to be put into operational use, a number of preparatory activities should be completed after the necessary planning. These preparatory activities include the:

- formulation and production of an information security incident management policy, and gaining senior management commitment to that policy (see also Clause 7.2 below),
- definition and documentation of a detailed information security incident management scheme (see also Clause 7.3 below). The topics for inclusion include:
  - an information security incident severity scale to be used to 'grade' incidents. As mentioned in Clause 4.2.1, this scale could be 'major' and 'minor', with, in any event, the decision based on the actual or projected adverse impacts on the organization's business operations,
  - information security event[4] and incident[5] reporting forms[6] (example forms are shown at Annex A), the related documented procedures and actions, with links to the normal procedures for the use of data and system, service and/or network backups, and business continuity plans,

[4] The form completed by the reporting person (i.e. not an information security incident management team person).

- operating procedures for the ISIRT, with documented responsibilities, and the allocation of roles to designated persons[7] to conduct various activities, for example including:
  - shut down an affected system, service and/or network, in certain circumstances agreed by prior arrangement with the relevant IT and/or business management,
  - leave an affected system, service and/or network, connected and running,
  - monitor data flowing from, to and within an affected system, service and/or network,
  - activate normal back-up and business continuity planning procedures and actions in line with the system, service and/or network security policy,
  - monitoring and maintaining the secure preservation of electronic evidence, in case it is required for legal prosecution or internal disciplinary action,
  - communication of information security incident details to internal and external people or organizations,
- testing the use of the information security incident management scheme, its processes and procedures (see also Clause 7.3.5 below),
- updating of corporate information security and risk analysis and management policies, and specific system, service or network information security policies, to include reference to information security incident management, and ensure that these policies are regularly reviewed in the context of output from the information security incident management scheme (see also Clause 7.4 below),
- establishment of the ISIRT, with an appropriate training program designed, developed and provided to its personnel (see also Clause 7.5 below),
- the technical and other means for supporting the information security incident management scheme (and thus the work of the ISIRT) (see also Clause 7.6 below),
- design and development of an information security incident management awareness program (see also Clause 7.7 below), followed by its delivery to all of an organization's personnel (and later repeated as personnel change).

The following clauses describe each of these activities, including the contents of each document required.

7.2 Information Security Incident Management Policy

7.2.1 Aim

The information security incident management policy is aimed at every person having legitimate access to an organization's information systems and related locations.

7.2.2 Audience

The information security incident management policy should be approved by a senior organization executive officer, with confirmed documented commitment from all of senior management. It should be made available for every employee

[5] The form used by the information security incident management personnel to build on the initially reported information on an information security event and keep a running record of the incident assessments etc. over time until the incident is fully resolved. At each stage the update is included in the information security event/incident database. The 'completed' form/information security event/incident database record is then used in post-incident resolution activities.

[6] If at all possible these forms should be electronic (e.g. in secure web page) form with linkage to the electronic information security event/incident database. In today's world, to operate a paper-based scheme would be time consuming and not the most efficient way of operating.)

[7] For smaller organizations, an individual may be allocated more than one role.

and contractor, and should also be addressed in information security awareness briefings and training (see also Clause 7.7 below).

7.2.3 Content

The information security incident management policy content should address the following topics:

- the importance of information security incident management to the organization, and senior management commitment to it and the related scheme,
- an overview of information security event detection, reporting and collection of relevant information, and how this information should be used to determine information security incidents. This overview should include a summary of possible types of information security event, how to report them, what to report, where and to whom, and including how to handle entirely new types of information security event,
- an overview of information security incident assessment, including a summary of who is responsible, what has to be done, notification, and escalation,
- a summary of the activities that follow confirmation that an information security event is an information security incident. This should cover:
  - immediate responses,
  - forensic analysis,
  - communications to involved personnel and relevant third parties,
  - consideration as to whether an information security incident is under control,
  - later responses,
  - 'crisis' instigation,
  - escalation criteria,
  - who is responsible,
- a reference to the need for ensuring that all activities are properly logged for later analysis, and that continual monitoring is conducted to ensure the secure preservation of electronic evidence, in case it is required for legal prosecution or internal disciplinary action,
- post information security incident resolution activities, including learning from, and improving the process, following information security incidents,
- details of where the scheme documentation, including of procedures, is held,
- an overview of the ISIRT, encompassing the following topics:
  - the ISIRT organizational structure, and the identity of key personnel, including who is responsible for:
    - briefing senior management on incidents,
    - dealing with enquiries, instigating follow up, etc.,
    - the link with the external organizations (when necessary),
  - the information security management charter that specifies what the ISIRT is to do and the authority under which it will do it. At minimum, the charter should include a mission statement, a definition of the ISIRT's scope, and details of the ISIRT's board level sponsor and its authority,

- the ISIRT mission statement that focuses on the team's core activities. In order to be considered an ISIRT, the team should support the assessing of, responding to, and managing of, information security incidents, to a successful conclusion. The goals and purposes of the team are especially important, and require clear, unambiguous definition,

- a definition of the scope of the ISIRT activity. Normally, the scope of an organization's ISIRT will cover all of the organization's information systems, services and networks. In other cases, an organization may, for whatever reason, require the scope to be less than that, in which case it should be clearly documented what is in, and what is out of, scope,

- the identity of sponsoring senior executive officer/board member/senior manager, who authorizes the actions of the ISIRT, and the levels of authority invested in the ISIRT. Knowing this will help all personnel in the organization to understand the background and set-up of the ISIRT, and it is vital information for building trust in the ISIRT. It should be noted that before this detail is promulgated, it should be checked from a legal perspective. In some circumstances, disclosure of a team's authority may expose it to claims of liability,

- an overview of the information security incident management awareness and training program,

- a summary of the legal and regulatory aspects that have to be addressed (see also Clause 5.2.3).

7.3 Information Security Incident Management Scheme

7.3.1 Aim

The aim of an information security incident management scheme is to provide detailed documentation describing the processes and procedures for dealing with incidents and the communication of such incidents. The information security incident management scheme comes into effect whenever an information security event is detected. It is used as a guide for:

- responding to information security events,

- determining whether information security events become information security incidents,

- managing information security incidents to a conclusion,

- identifying lessons learnt, and any improvements to the scheme and/or security in general that are required,

- making identified improvements.

7.3.2 Audience

The information security incident management scheme is addressed at all of an organization's personnel, thus covering those responsible for:

- detecting and reporting information security events, which could be anyone in an organization, whether permanent or contracted,

- assessing and responding to information security events and information security incidents, and involved in the post-incident resolution phase of learning and as necessary improving information security and the information security incident management scheme itself. These include members of the operations support group (or similar team), the ISIRT, management, public relations personnel and legal representatives.

It should also take into account any third party users, and information security incidents and associated vulnerabilities reported from third party organizations and government and commercial information security incident and vulnerability information provision organizations.

7.3.3 Content

The content of the information security incident management scheme documentation should include:

- an overview of the information security incident management policy,
- an overview of the whole information security incident management scheme,
- the detailed processes and procedures[8], and information on the related tools and scales, associated with:
  - Plan and Prepare:
    - detecting and reporting the occurrence of information security events (by human or automatic means),
    - collecting the information on information security events,
    - conducting assessments of information security events (including escalation as required), using the agreed event/incident severity scale, and determining whether they become re-categorized as information security incidents,
  - Use (when information security incidents are confirmed):
    - communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations,
    - in accordance with the analysis and confirmed severity scale rating, instituting immediate responses, which could include the activation of recovery procedures, and /or issuing communications to relevant involved personnel,
    - conducting forensic analysis, as required and relative to the information security incident severity scale rating, and changing that scale rating as necessary,
    - deciding whether information security incidents are under control,
    - instituting any required further responses, including those that may be required in later time (for example, in facilitating full recovery from a disaster,
    - if information security incidents are not under control, instigating 'crisis' activities (for example, calling a fire brigade/department, or activating a business continuity plan),
    - escalating for further assessments and/or decisions as required,
    - ensuring that all activities are properly logged, for later analysis,
    - updating of the information security event/incident database,

    (The information security incident management scheme documentation should allow for information security incident responses both immediately and in the longer-term. All information security incidents will need an early assessment of the potential adverse impacts, both short and longer-term (for example, a major disaster could occur some time after an initial information security incident). Further, some responses may be necessary for information security incidents that are completely unforeseen, where ad hoc safeguards will be required. Even in this situation, the scheme documentation should encompass general guidelines on the steps that may be necessary.)
  - Review:

[8] The organization can decide if all procedures are included in the scheme documentation, or all or someare detailed in subsidiary documents.

  - conducting further forensic analysis, as required,
  - identifying and documenting the lessons learnt from information security incidents,
  - reviewing and identifying improvements to information security, as a result of the lessons learnt,
  - reviewing how effective the processes and procedures were in responding to, assessing and recovering from each information security incident, and identifying improvements to the information security incident management scheme as whole, as a result of lessons learnt),
  - updating of the information security event/incident database,
- Improve – based on the lessons learnt, making improvements to:
  - information security risk analysis and management results,
  - the information security incident management scheme (for example, to processes and procedures, the reporting form and/or organizational structure),
  - overall security, with the implementation of new and/or improved safeguards,

- details of the event/incident severity scale (for example, major or minor; or significant, urgent, minor, non-urgent) and associated guidance,
- guidance for deciding whether escalation is required during each relevant process, and to whom, and associated procedures. Anyone assessing an information security event or incident should be aware, based on the guidance provided in the information security incident management scheme documentation, when in normal circumstances it is necessary to escalate matters, and to whom. In addition, there will be unforeseen circumstances when this may be necessary. For example, a minor information security incident could evolve to significant or a 'crisis' situation if not handled properly or a minor information security incident not followed up in a week could become a major information security incident. The guidance should define information security event and incident types, escalation types and who can institute escalation,
- procedures to be followed to ensure that all activities are properly logged in the appropriate form, and that log analysis is conducted by designated personnel,
- procedures and mechanisms to ensure that the change control regime is maintained covering information security event and incident tracking, and information security incident report updates, and updates to the scheme itself,
- procedures for forensic analysis,
- procedures and guidance on using Intrusion Detection Systems (IDS), ensuring that associated legal and regulatory aspects have been addressed (see Clause 5.2.3). Guidance should include discussion of the advantages and disadvantages of undertaking attacker surveillance activities. Further information on IDS is contained in ISO/IEC TR 15947 – IT Intrusion Detection Framework, and ISO/IEC TR 18043 – Guidelines for the Selection, Deployment and Operation of Intrusion Detection Systems (IDS),
- the scheme organization structure,
- the terms of reference and responsibilities of the ISIRT as a whole, and of individual members,
- important contact information.

7.3.4 Procedures

Before being able to commence operation of the information security incident management scheme, it is important that documented and checked procedures are available. Each procedures document should indicate those responsible for its use and management, as appropriate from the operations support group and/or the ISIRT. Such procedures will include those for ensuring that electronic evidence is gathered and stored securely, and that its secure preservation is continually

monitored, in case it is required for legal prosecution or internal disciplinary action. Further, there should be documented procedures covering not just operations support group and ISIRT activities, but those involved in forensic analysis and 'crisis' activities – if not covered elsewhere (for example in a business continuity plan). Obviously the documented procedures should be entirely in line with the documented information security incident management policy and other information security incident management scheme documentation.

It is important to understand that not all procedures need be publicly available. For example, it is not desirable for all of an organization's personnel to understand the internal operation of an ISIRT in order to interact with it. The ISIRT should ensure that 'publicly available' guidance, including information resulting from information security incident analysis, is in readily available form, for example on the organization's Intranet. Furthermore, it may also be important to keep some details of the information security incident management scheme closely held to prevent the "insider" from tampering the investigation process. For example, if a bank employee who is embezzling funds is aware of some details of the scheme, he or she may be able to better hide their activities from investigators or otherwise hamper the detection and investigation of and recovery from an information security incident.

The content of operating procedures will depend on a number of criteria, especially related to the nature of known potential information security events and incidents and the types of information system assets that might be involved and their environment. Thus, an operating procedure could be related to a particular type of incident or indeed to type of product (for example firewalls, databases, operating systems, applications) or specific product. Each operating procedure should clearly identify the steps to be undertaken and by whom. It should reflect experience from external (for example government and commercial CERTs or similar, and suppliers) as well as from internal sources.

There will be operating procedures for dealing with types of information security events and information security incidents that are already known. There will also have to be operating procedures to be followed when an identified information security event or information security incident is not of any known type. In this case the following needs to be addressed:

- the reporting process for the handling of such 'exceptions',
- guidance on the timing for getting approval from management in order to avoid any delay of response,
- pre-authorized delegation of decision making without normal approval process.

7.3.5 Scheme Testing

Regular checking and testing of the information security incident management processes and procedures should be scheduled to highlight potential flaws and problems that may arise during the management of information security events and information security incidents. Any changes that arise from post response review should be subject to thorough checking and testing before going live.

7.4 Information Security and Risk Management Policies

7.4.1 Aim

The aim of including information security incident management content in the corporate information security and risk management policies, and specific system, service and network information security policies, is to:

- describe why information security incident management, particularly an information security incident reporting and handling scheme, is important,
- indicate senior management commitment to the need for proper preparation and response to information security incidents, i.e. to the information security incident management scheme,
- ensure consistency across the various policies,
- ensure planned, systematic and calm responses to information security incidents, thus minimizing the adverse impacts of incidents.

7.4.2 Content

Corporate information security and risk management policies, and specific system, service or network information security policies, should be updated so that they explicitly refer to a corporate information security incident management policy and associated scheme. The relevant sections should refer to the senior management commitment, and outline the:

- policy,
- scheme processes, and related infrastructure,
- requirements for detecting, reporting, assessing and managing incidents,

and clearly indicate those personnel responsible for authorizing and/or undertaking certain critical actions (e.g. taking an information system off-line or even shutting it down).

Further, policies should require that the appropriate review mechanisms are established to ensure that any information from the detection, monitoring and resolution of information security incidents is used as input to ensure the continuing effectiveness of the corporate information security and risk management, and specific system, service or network information security, policies.

7.5 Establishment of the ISIRT

7.5.1 Aim

The aim of establishing the ISIRT is to provide the organization with appropriate personnel for assessing, responding to and learning from information security incidents, and providing the necessary co-ordination, management, feedback and communication. An ISIRT can contribute to the reduction in physical and monetary damage, as well as the reduction of the damage to the organization's reputation that is sometimes associated with information security incidents.

7.5.2 Members and Structure

The appropriate size, structure and composition of the ISIRT should be appropriate for the size and structure of the organization. Although the ISIRT may constitute an isolated team or department, members may share other duties, which will encourage the input of members from a range of areas within the organization. As discussed in clauses 4.2.1 and 7.1, in many cases the ISIRT will be a virtual team led by a senior manager. The senior manager will be supported by individuals who are specialized in particular topics, for example in handling malicious code attacks, who will be called upon depending on the type of information security incident concerned. Depending on the size of the organization, a member may also fulfil more than one role within the ISIRT. The ISIRT may also comprise individuals from different parts of the organization (e.g., Business Operations, IT/Telecommunications, Audit, Human Resources and Marketing).

Team members should be accessible for contact, so the names and contact details of each member and their backup persons should be available within the organization. For example, the necessary details should be clearly indicated in the information security incident management scheme documentation, including any procedural documents, and the reporting forms, but not in policy statements.

The ISIRT manager should:

- have delegated authority to make immediate decisions on how to deal with an incident,
- usually have a separate line of reporting to senior management, separate from normal business operations,
- ensure that all ISIRT members have the required knowledge and skills levels, and that these continue to be maintained,
- assign investigation of each incident to the most appropriate member of his/her team.

7.5.3 Relationship with other Parts of the Organization

The ISIRT manager and members of his/her team must have a degree of authority to take the necessary actions deemed appropriate in response to an information security incident. However, actions that may have adverse effects on the overall organization, either financially or in terms of reputation, should be agreed with senior management. For this reason it is essential to detail in the information security incident management policy and the scheme the appropriate authority to which the ISIRT manager reports serious information security incidents.

Procedures and responsibilities for dealing with the media should also be agreed with senior management and documented. These procedures should specify:

- who in the organization will deal with media inquiries,
- how that part of the organization will interact with the ISIRT.

7.5.4 Relationship with External Parties

Relationships between the ISIRT and appropriate external parties need to be established. External parties may include:

- contracted external support personnel, for example from a CERT,
- external organizations' ISIRTs or computer incident response teams, or CERTs,
- law enforcement organizations,
- other emergency authorities (e.g. fire brigade/department),
- appropriate government organizations,
- legal personnel,
- public relations officials and/or members of the media,
- business partners,
- customers,
- the general public.

7.6 Technical and Other Support

Quick and effective responses to information security incidents will be more achievable when all necessary technical and other support means have been acquired, prepared and tested. This includes:

- access to details of the organization's assets (preferably with an up-to-date asset register) and information on their links to business functions,
- access to the documented business continuity strategy and related plans,
- documented and promulgated communications processes,
- the use of an electronic information security event/incident database and the technical means to populate and update the database quickly, analyze its information and facilitate responses (although it is recognized that there may occasionally be instances where manual records would still be required or used by an organization),
- adequate business continuity arrangements for the information security event/incident database.

The technical means used to populate and update the database quickly, analyze its information and facilitate responses to information security incidents should support:

- quick acquisition of information security event and incident reports,
- notification of previously selected personnel (as relevant external people) by appropriate means (for example electronic mail, fax, telephone, etc.), thus requiring the maintenance of a reliable contact database (which should be readily accessible, and should include paper and other backups), and the facility to transmit information to individuals in a secure fashion where appropriate,
- taking precautions commensurate with assessed risks for ensuring that electronic communication, whether Internet or non-Internet, cannot be eavesdropped while the system, service and/or network is under attack,
- taking precautions commensurate with assessed risks for ensuring that electronic communication, whether Internet or non-Internet, stays available while the system, service and/or network is under attack,
- ensuring the collection of all data about the information system, service and/or network, and all data processed,
- if commensurate with assessed risks, using cryptographic integrity control to help in determining whether and what parts of the system, service and/or network, and what data, were changed,
- facilitating the archiving and securing of collected information (for example, by applying digital signatures to logs and other evidence before off-line storage in read-only media such as CD or DVD ROM),
- enabling the preparation of printouts (e.g. of logs), including those showing the progress of an incident, and the resolution process and chain of custody,
- recovery of the information system, service and/or network to normal operation, with:
  - good backup procedures,
  - clean and reliable backups,
  - backup testing,
  - malicious code control,
  - original media with system and application software,
  - bootable media,
  - clean, reliable and up to date system and application patches,

  in line with the relevant business continuity plan(s).

An attacked information system, service or network may not function correctly. Thus as far as possible, and commensurate with the assessed risks, no technical means (software and hardware) that are necessary for responding to an information security incident should rely in their operations on the organization's 'mainstream' systems, services and/or networks. If it is possible, they should be fully independent.

All technical means should be carefully selected, correctly implemented and regularly tested (including testing of the backups made).

It should be noted that technical means described in this clause do not include technical means used to directly detect information security incidents and intrusions and to automatically notify appropriate persons. Such technical means are described in the Intrusion Detection Framework TR 15947 and in the Management of information and communications technology security (MICTS) TR 13335, particularly Part 2.

7.7 Awareness and Training

Information security incident management is a process that involves not only technical means but also people, and thus it should be supported by appropriately information security-aware and trained individuals within the organization.

The awareness and participation of all organization personnel is very important for the success of a structured information security incident management approach. For this reason, the role of information security incident management needs to be actively promoted as part of the corporate information security awareness and training program. The awareness program and related material should be available to all personnel, including new employees and, as relevant, third party users and contractors. There should be a specific training program for the operations support group, ISIRT members, and, as necessary, information security personnel and specific administrators. It should be noted that each group of people involved directly with the management of incidents may require different levels of training, depending on the type, frequency and criticality of their interaction with the information security incident management scheme.

The awareness briefings should encompass:

- the basics of how the information security incident management scheme works, including its scope and the security event and incident management 'workflow',
- how to report on information security events and incidents,
- as relevant, safeguards on confidentiality of sources,
- scheme service level agreements,
- notification of outcomes – under what circumstances sources will be advised,
- any constraints imposed by non-disclosure agreements,
- the authority of the information security incident management organization and its reporting line,
- who and how receive reports from the information security incident management scheme.

In some cases it may be desirable to specifically include awareness detail about information security incident management in other training programs (for example, personnel orientation programs or general corporate security awareness programs). This awareness approach may provide valuable context relevant to particular groups of people, and can improve training program effectiveness and efficiency.

Before the information security incident management scheme becomes operational, all relevant personnel need to become familiar with the procedures involved in the detection and reporting of information security events, and selected personnel need to become very knowledgeable about the subsequent processes. This should be followed up by regular awareness briefings and training courses. The training should be supported by specific exercises and testing for operations support group and ISIRT members, and information security personnel and specific administrators.

8 Use

8.1 Introduction

Information security incident management in operation comprises two main phases, the "Use" and "Review" phases, and these are followed by the "Improve" phase when any improvements identified as a result of lessons learnt are made. These phases and their associated processes were introduced in Clause 4.2. The "Use" phase is described in this clause, the "Review" phase in Clause 9, and the "Improve" phase is described in Clause 10.

The three phases, and related processes, are shown in Figure 2 below.

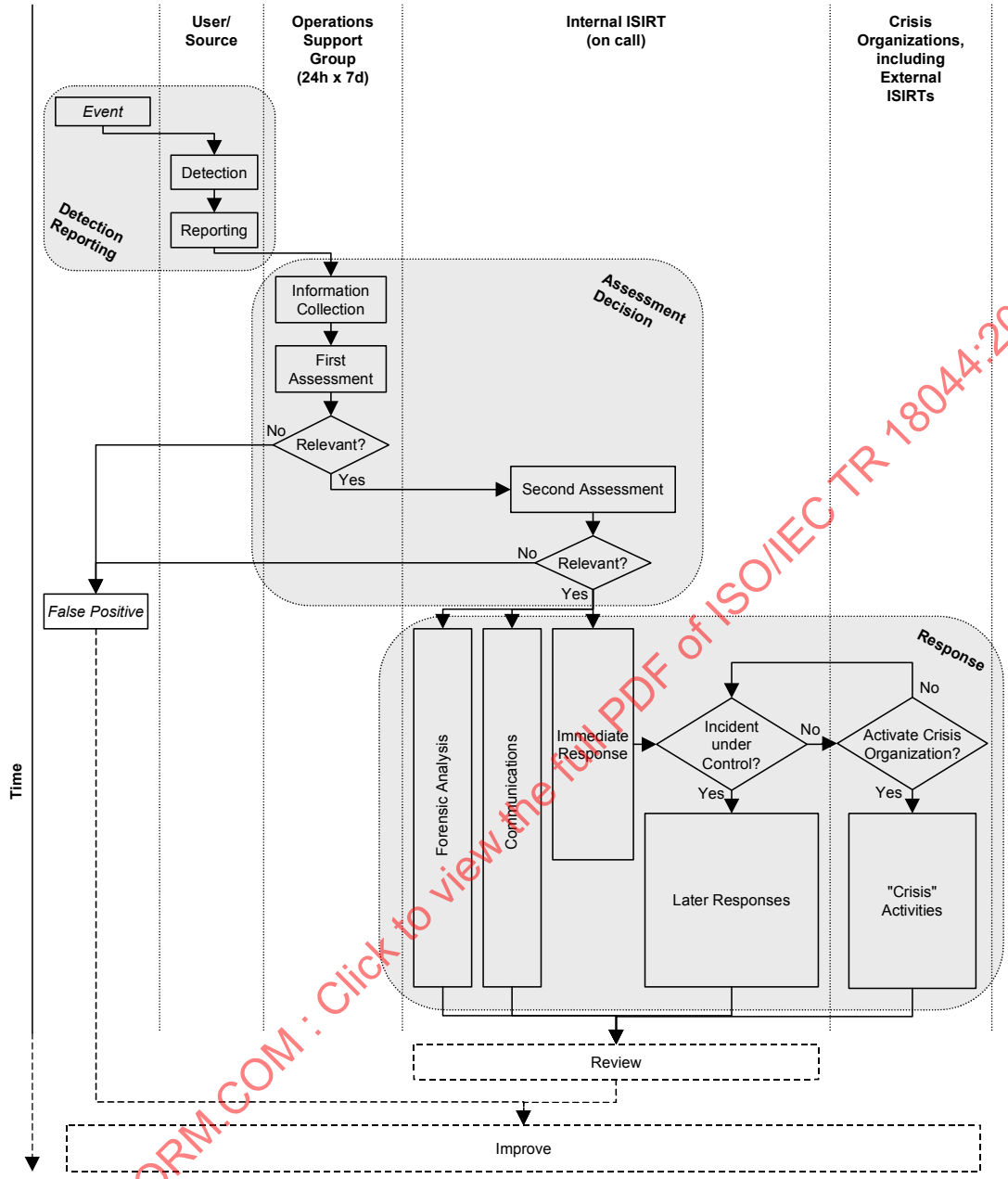

Figure 2 - Information Security Event and Incident Flow Diagram

8.2 Overview of Key Processes

In the Use phase, the key processes are the:

- detection of and reporting on the occurrence of an information security event, whether by one of the organization's personnel/customers or automatically (for example, by an alert from a firewall),
- collection of information on an information security event, and the conduct of the first assessment by the organization's operations support group personnel[9], who will determine whether the event is an information security incident or a false alarm has arisen,

[9] It is not to be normally expected that operations support group personnel will be security experts.

- conduct of the second assessment by the ISIRT, to firstly confirm that the event is an information security incident, and then, if it is, to instigate an immediate response as well as start necessary forensic analysis and communications activities,
- review by the ISIRT to determine if the information security incident is under control, and:
  - if it is, instigating any required later, further, responses, and ensuring all information is ready for post-incident review activities,
  - if it is not, instigating 'crisis' activities and involving the related personnel, for example the organization's business continuity manager and team,
- escalation, on an as required basis throughout the phase, for further assessments and/or decisions,
- ensuring that all involved, particularly the ISIRT, properly log all activities for later analysis,
- ensuring that electronic evidence is gathered and stored securely, and that its secure preservation is continually monitored, in case it is required for legal prosecution or internal disciplinary action,
- ensuring that the change control regime is maintained covering information security incident tracking and incident report updates, and thus that the information security event/incident database is kept up-to-date.

All information collected pertaining to an information security event or incident should be stored in the information security event/incident database managed by the ISIRT. The information reported during each process should be as complete as is possible at the time, to ensure as firm a base as there can be is available for the assessments and decisions made, and of course the actions taken.

Once an information security event has been detected and reported, the aims of the subsequent processes are:

- distributing the responsibility for incident management activities through an appropriate hierarchy of personnel, with assessment, decision making and actions involving both security and non-security personnel,
- providing formal procedures for each notified person to follow, including reviewing and amending the report made, assessing the damage, and notifying the relevant personnel (with the individual actions depending on the type and severity of the incident),
- using guidelines for thorough documentation of an information security event, and later if it becomes categorized as an information security incident, of the subsequent actions, and updating of the information security event/incident database.

Guidance on:

- information security event detection and reporting is provided in Clause 8.3,
- assessment and decision (as to whether an information security event is to be categorized as an information security incident) is provided in Clause 8.4,
- responses to information security incidents is provided in Clause 8.5, covering:
  - immediate responses,
  - review to determine if an information security incident is under control,
  - later responses,
  - 'crisis' activities,
  - forensic analysis,

- communications,
- commentary on escalation issues,
- activity logging.

8.3 Detection and Reporting

Information security events could be detected directly by a person or persons noticing something that gives cause for concern, whether technical, physical or procedural related. Detection could, for example, be from fire/smoke detectors or intruder (burglar) alarms, with the alerts notified to pre-designated locations for human action. Technical information security events could be detected by automatic means – for example, alerts made by audit trail analysis facilities, firewalls, intrusion detection systems, and anti-virus tools, in each case stimulated by pre-set parameters.

Whatever the source of the detection of an information security event, the person notified by automatic means, or directly noticing something unusual, is responsible for initiating the detection and reporting process. This could be any member of an organization's personnel, whether permanent or contracted personnel. The person should follow the procedures and use the information security event reporting form specified by the information security incident management scheme, to bring the information security event to the attention in the first instance to the operations support group, and management. Thus, it is essential that all personnel are well aware of, and have access to, the guidelines for reporting the different types of possible information security events, including the format of the information security event reporting form, and details of the personnel who should be notified on each occasion. (It is sensible that all personnel are at least also aware of the format of the information security incident reporting form, to aid their understanding of the scheme.)

How an information security event is handled will be dependent upon what it is, and the implications and repercussions which may flow from it. For many people, this will be a decision beyond their competence. Thus, the person reporting an information security event should complete the information security event reporting form with as much narrative and other information as is readily available at the time, liaising with his/her local manager as necessary. That form, preferably in electronic format (e.g. in an e-mail or web form submission), should be securely communicated to the designated operations support group (that should preferably provide a 24-hour service for 7 days per week), with a copy to the ISIRT manager. An example template for the information security event reporting form is shown in Annex A.

It is emphasized that not only accuracy but also timeliness is important in the content filled in the information security event reporting form. It is not good practice to delay the submission of a reporting form in order to improve the accuracy of its content. If the reporting person is not confident of the data in any field on the reporting form, it should be submitted with appropriate notation, and revisions communicated later. It should also be recognized that some electronic reporting mechanisms (e.g. e-mail) are themselves visible targets for attack.

When problems exist, or are considered to exist, with default electronic reporting mechanisms (e.g. e-mail), including when it is thought possible that the system is under attack and reporting forms could be read by unauthorized people, then alternative means of communication should be used. The alternative means could include in person, by telephone or text messaging. Such alternative means should be used particularly when it becomes evident early in an investigation that an information security event appears likely to be categorized as an information security incident, particularly one that may be significant.

It should be noted that whilst in most cases an information security event will have to be reported onwards for action by the operations support group, there may be occasions where an information security event can be handled locally, possibly with the help of local management. An information security event may be quickly determined as a false alarm, or it may be resolved to a satisfactory conclusion. In such cases a reporting form should be completed and forwarded to local management, and to the operations support group and to the ISIRT for recording purposes, i.e. into the information security event/incident database. In such circumstance, the person reporting closure of an information security event may be able to complete some of the information required for the information security incident reporting form – if this is the case then the information security incident reporting form should also be completed and forwarded.

8.4 Event/Incident Assessment and Decision

8.4.1 First Assessment and Initial Decision

The receiving person in the operations support group should acknowledge receipt of the completed information security event reporting form, enter it into the information security event/incident database, and review it. He/she should seek any clarification from the person reporting the information security event, and collect any further information required and known to be available, whether from the reporting person or elsewhere. Then, the operations support group person should conduct an assessment to determine whether the information security event should be categorized as an information security incident or is in fact a false alarm. If the information security event is determined to be a false alarm, the information security event reporting form should be completed and communicated to the ISIRT for addition to the information security event/incident database and review, and copied to the reporting person and his/her local manager.

Information and other evidence collected at this stage may need to be used at a future time for disciplinary or legal proceedings. The person or people undertaking the information collection and assessment tasks should be trained in the requirements for collection and preservation of evidence.

In addition to recording the date(s) and time(s) of actions, it is necessary to fully document:

- what was seen and done (including tools used) and why,
- the location of 'evidence',
- how evidence is archived (if applicable),
- how evidence verification was performed (if applicable),
- details of storage/safe custody of material and subsequent access to it.

If the information security event is determined as likely to be an information security incident, and if the operations support group person has the appropriate level of competence, further assessment may be conducted. This may result in required remedial actions, for example additional emergency safeguards being identified and referred for action to the appropriate person. It may be very evident that an information security event is determined to be an information security incident that is significant (using the organization's pre-determined severity scale), in which case the ISIRT manager should be informed directly. It may be very evident that a 'crisis' situation should be declared, and thus, for example, the business continuity manager notified for possible activation of a business continuity plan, with the ISIRT manager and senior management also informed. However, the most likely situation will be that the information security incident will need to be referred directly to the ISIRT for further assessment and action.

Whatever the next step is determined to be, the operations support group person should complete as much as is possible of the information security incident reporting form. An example template for an information security incident reporting form is shown in Annex A. The information security incident reporting form should contain narrative, and as far as is possible should confirm and describe:

- what the information security incident is,
- how it was caused – and by what or whom,
- what it affects or could affect,
- the impact or potential impact of the information security incident on the business of the organization,
- an indication as to whether the information security incident is deemed significant or not (using the organization's pre-determined severity scale),
- how it has been dealt with so far.

When considering the potential or actual adverse effects of an information security incident on the business of an organization, from:

- unauthorized disclosure of information,
- unauthorized modification of information,
- repudiation of information,
- unavailability of information and/or service,
- destruction of information and/or service,

the first step will be to consider which of a number of consequences is relevant.

Example categories are:

- Financial Loss/Disruption to Business Operations,
- Commercial and Economic Interests,
- Personal Information,
- Legal and Regulatory Obligations,
- Management and Business Operations,
- Loss of Goodwill.

For those considered relevant, the related category guideline should be used to establish the potential or actual impacts for entry into the information security incident report. Example guidelines are given in Annex B.

If an information security incident has been resolved, the report should include details of the safeguards that have been taken and any lessons learned (e.g. safeguards to be adopted to prevent re-occurrence or similar occurrences).

Once completed as far as is possible, the reporting form should then be referred to the ISIRT for entry into the information security event/incident database and review.

If an investigation is likely to be longer than one week, an interim report should be produced.

It is emphasized that the operations support group person assessing an information security incident should be aware, based on the guidance provided in the information security incident management scheme documentation:

- when it is necessary to escalate matters and to whom,
- that in all activities conducted by the operations support group, the documented change control procedures should be followed.

When problems exist, or are considered to exist, with default electronic reporting mechanisms (e.g. e-mail), including when it is thought possible that the system is under attack and reporting forms could be read by unauthorized people, then alternative means of reporting to the ISIRT manager should be used. Alternative means could include in person, by telephone or text messaging. Such alternative means should be used particularly when it appears that an information security incident is significant.

8.4.2 Second Assessment and Incident Confirmation

The second assessment, and confirmation or otherwise of the decision as to whether an information security event is to be categorized as an information security incident, should be the responsibility of the ISIRT. The receiving person in the ISIRT should:

- acknowledge receipt of the ‘information security incident reporting form, completed as far as is possible by the operations support group,

- enter the form into the information security event/incident database,
- seek any clarification from the operations support group,
- review the reporting form content,
- collect any further information required and known to be available, whether from the operations support group, the person who completed the information security event reporting form or elsewhere.

If there is still a degree of uncertainty as to the authenticity of the information security incident or the completeness of the reported information, the ISIRT member should conduct an assessment to determine whether the information security incident is real or in fact a false alarm. If the information security incident is determined to be a false alarm, the information security event report should be completed, added to the information security event/incident database and communicated to the ISIRT manager. Copies of the report should be sent to the operations support group, and the reporting person and his/her local manager.

If the information security incident is determined to be real, then the ISIRT member, involving colleagues as required, should conduct further assessment. The aim is to confirm as soon as possible:

- what the information security incident is, how it was caused – and by what or whom, what it affects or could affect, the impact or potential impact of the information security incident on the business of the organization, an indication as to whether the information security incident is deemed significant or not (using the organization's pre-determined severity scale),
- for deliberate human technical attack on an any information system, service and/or network, for example:
  - how deeply the system, service and/or network has been infiltrated, and what level of control the attacker has,
  - what data has been accessed by the attacker, possibly copied, altered or destroyed,
  - what software has been copied, altered or destroyed by the attacker,
- for deliberate human physical attack on an any information system, service and/or network hardware and/or physical location, for example:
  - what the direct and indirect effects of physical damage are (is physical access security non-existent?),
- for information security incidents not directly caused by human actions, the direct and indirect effects (for example, is physical access open because of a fire, is an information system vulnerable because of some software or communications line malfunction, or because of human error),
- how the information security incident has been dealt with so far.

When reviewing the potential or actual adverse effects of an information security incident on the business of an organization, from:

- unauthorized disclosure of information,
- unauthorized modification of information,
- repudiation of information,
- unavailability of information and/or service,
- destruction of information and/or service,

it will be necessary to confirm which of a number of consequences is relevant. Example categories are:

- Financial Loss/Disruption to Business Operations,

- Commercial and Economic Interests,
- Personal Information,
- Legal and Regulatory Obligations,
- Management and Business Operations,
- Loss of Goodwill.

For those considered relevant, the related category guideline should be used to establish the potential or actual impacts for entry into the information security incident report. Example guidelines are given in Annex B.

8.5 Responses

8.5.1 Immediate Responses

8.5.1.1 Overview

In the large majority of cases, the next activities for the ISIRT member will be to identify the immediate response actions to deal with the information security incident, record details on the information security incident form and within the information security event/incident database, and notify the required actions to the appropriate persons or groups. This may result in emergency safeguards (for example, cutting off/shutting down an affected information system, service and/or network, with the prior agreement of the relevant IT and/or business management), and/or additional permanent safeguards being identified, and notified for action to the appropriate person or group. If not already done so, the significance of the information security incident should be determined, using the organization's pre-determined severity scale, and if sufficiently significant appropriate senior management should be notified directly. If it evident that a 'crisis' situation should be declared, for example the business continuity manager should be notified for possible activation of a business continuity plan, with the ISIRT manager and senior management also informed.

8.5.1.2 Example Actions

As an example of relevant immediate response actions in the case of deliberate attack on an information system, service and/or network, it could be left connected to the Internet, or other network, to:

- allow for business critical applications to function correctly,
- collect as much information as possible about the attacker,

provided that the attacker does not know that he/she is under surveillance.

However, while undertaking such a decision the following factors need to be considered:

- the attacker may realize that he/she is being observed and may undertake actions that will cause further damage to the affected information system, service and/or network, and related data,
- the attacker could destroy the information that may be useful to track that person.

It is essential that it is technically possible to quickly and reliably cut-off and/or shut down the attacked information system, service and/or network, once a decision to do so has been taken. However, appropriate authentication means should be implemented so that unauthorized individuals could not undertake such action.

A further consideration is that the prevention of re-occurrence is usually of high priority, and it might well be concluded that the attacker has exposed a weakness which should be rectified, and the gains from tracking him/her do not justify the effort in doing so. This is especially relevant when the attacker is non-malicious and has caused little or no damage.

With regard to information security incidents that are caused by something other than deliberate attack, the source should be identified. It may be necessary to shut the information system, service and/or network down, or isolate the relevant part and shut it down (with the prior agreement of the relevant IT and/or business management), while safeguards are

implemented. This may take longer if the weakness is fundamental to the information system, service and/or network design, or if it is a critical weakness.

Another response activity may be to activate surveillance techniques (for example, 'honeypots' – see TR 18043). This should be on the basis of procedures documented for the information security incident management scheme.

Information that may be corrupted by the information security incident should be checked by the ISIRT member against backup records for modifications, deletions, or insertions of information. It may be necessary to check the integrity of the logs, as a deliberate attacker may have manipulated these logs to cover his/her tracks.

8.5.1.3 Incident Information Update

Whatever the next step is determined to be, the ISIRT member should update the information security incident report as much as is possible, add it to the information security event/incident database and notify the ISIRT manager and others as necessary. The update may cover further information on:

- what the information security incident is,
- how it was caused – and by what or whom,
- what it affects or could affect,
- the impact or potential impact of the information security incident on the business of the organization,
- changes to the indication as to whether the information security incident is deemed significant or not (using the organization's pre-determined severity scale),
- how it has been dealt with so far.

If an information security incident has been resolved, the report should include details of the safeguards that have been taken and any other lessons learned (e.g. further safeguards to be adopted to prevent re-occurrence or similar occurrences). The updated report should be added to the information security event/incident database, and notified to the ISIRT manager and others as required.

It is emphasized that the ISIRT is responsible for ensuring the secure retention of all information pertaining to an information security incident for further analysis, and potential legal evidential use. For example, for an IT oriented information security incident, after the initial discovery of the incident, all volatile data should be collected before the affected IT system, service and/or network is shut down, for a complete forensic investigation. Information to be collected includes contents of memory, cache and registers, and detail of any processes running, and:

- a full forensic duplication of the affected system, service and/or network, or a low level backup of logs and important files should be undertaken depending on the nature of the information security incident,
- logs from neighboring systems, services and networks, for example including from routers and firewalls, should be collected and reviewed,
- all information collected should be stored securely on read only media,
- two ore more persons should be present when forensic duplication is performed, to assert and certify that all activities have been carried out in accordance with relevant legislation and regulation,
- specifications and descriptions of the tools and commands used to perform the forensic duplication should be documented and stored together with the original media.

An ISIRT member will also be responsible, if it is possible at this stage, for facilitating the return of the affected facility (whether IT or otherwise) to a secure operational state that is not susceptible to a compromise by the same attack.

8.5.1.4 Further Activities

If an ISIRT member determines that an information security incident is real, then other important activities should be to:

- institute forensic analysis,
- inform those responsible for internal and external communications of the facts and proposals for what should be communicated, in what form and to whom.

Once an information security incident report has been completed as far as is possible, it should then be entered into the information security event/incident database and communicated to the ISIRT manager.

If an investigation is likely to be longer than a time period pre-agreed within the organization, an interim report should be produced.

The ISIRT member assessing an information security incident should be aware, based on the guidance provided in the information security incident management scheme documentation:

- when it is necessary to escalate matters and to whom,
- that in all activities conducted by the ISIRT, the documented change control procedures should be followed.

When problems exist, or are considered to exist, with normal communications facilities (e.g. e-mail), including when it is thought possible that the system is under attack, and:

- it is concluded that an information security incident is significant, and/or
- a 'crisis' situation has been determined,

as a fallback an information security incident should in the first instance be reported to the relevant people in person, by telephone or text messaging.

As deemed necessary, the ISIRT manager, in liaison with the organization's information security manager and the relevant board member/senior manager, should liaise with all related parties, both internal and external to the organization (see Clauses 7.5.3 and 7.5.4).

To ensure that the liaisons are organized quickly and are effective, it is necessary to establish a secure method of communication in advance, that does not wholly rely on the system, service and/or network that may be affected by the information security incident. These arrangements may include the nomination of backup advisors or representatives in the case of absence.

8.5.2 Incident Under Control?

After the ISIRT member has instigated the immediate responses, and as relevant forensic analysis and communications activities, a view needs to be quickly ascertained as to whether the information security incident is under control. If necessary, the ISIRT member may consult with colleagues, the ISIRT manager and/or other persons or groups.

If the information security incident is confirmed as being under control, then the ISIRT member should institute any required later responses, and forensic analysis and communications (see Clauses 8.5.3, 8.5.5 and 8.5.6 below), to bring the information security incident to a close and restore the affected information system to normal operations.

If the information security incident is confirmed as not being under control, then the ISIRT member should institute 'crisis activities' (see Clause 8.5.4 below).

8.5.3 Later Responses

Having determined that an information security incident is under control, and not to be subject to 'crisis' activities, then the ISIRT member should identify if and what further responses are required to deal with the information security incident. This could include restoring the affected information system(s), service(s) and/or network(s) back to normal operation. He/she should then record details on the information security incident reporting form and in the information security event/incident database, and notify those responsible for completing the related actions. Once those actions have

been successfully completed, details should be recorded on the information security incident reporting form and in the information security event/incident database, and then the information security incident should be closed and appropriate personnel notified.

Some responses will be directed at preventing information security incident re-occurrence or similar occurrence. For example, if it is determined that the cause of an information security incident is an IT hardware or software fault, without an available patch, then the supplier should be contacted immediately. If a known IT vulnerability was involved in an information security incident it should be patched with the relevant information security update. Any IT configuration related problems highlighted by the information security incident should be dealt with. Other measures to decrease the possibility of re-occurrence or similar occurrence of an IT information security incident may include changing system passwords and disabling unused services.

Another area of response activity may involve monitoring of the IT system, service and/or network. Following assessment of an information security incident, it may be appropriate that there should be additional monitoring safeguards in place to assist in detecting unusual and suspicious events that would be symptomatic of further information security incidents. Such monitoring may also reveal a greater depth to the information security incident, and identify other IT systems that were compromised.

It may well be necessary for activation of specific responses documented in the relevant business continuity plan. This could apply for both IT and non-IT related information security incidents. Such responses should include those for all business aspects, not just directly IT related but also key business function maintenance and later restoration – including, as relevant, of voice telecommunications, and personnel levels and physical facilities.

The last area of activity will be the restoration of the affected information system(s), service(s) and/or network(s) to normal operation. The restoration of an affected system(s), service(s) and/or network(s) to a secure operational state may be achieved through the application of patches for known vulnerabilities or by disabling an element that was the subject of the compromise. If due to the destruction of logs during an information security incident, the entire extent of the information security incident is unknown, then a complete system, service and/or network rebuild may be necessary. It may well be necessary for activation of parts of the relevant business continuity plan.

If an information security incident is non-IT related, for example caused by a fire, flood or bomb, then the recovery activities to be followed will be those documented in the relevant business continuity plan.

8.5.4 'Crisis' Activities

As discussed in Clause 8.5.2, it may be that when the ISIRT determines whether an information security incident is under control, the conclusion is that it is not under control and needs to be dealt with as a 'crisis' activity, using a pre-designated plan.

The best options for dealing with all possible types of information security incident that might affect availability/destruction and to some extent integrity of an information system, should have been identified in the organization's business continuity strategy. These options should be directly related to the organization's business priorities and related timescales for recovery, and thus the maximum acceptable outage time periods for IT, voice, people and accommodation. The strategy should have identified the required:

- preventive, resilience and business continuity support measures,
- organizational structure and responsibilities for managing business continuity planning,
- structure and outline content for the business continuity plan or plans.

The business continuity plan(s), and the safeguards put in place to support the activation of those plan(s), once tested satisfactorily, then form the basis for dealing with most 'crisis' activities once so designated.

Other types of possible 'crisis' activity include, but are not limited to, activation of:

- fire suppression facilities and evacuation procedures,
- flood prevention facilities and evacuation procedures,

- bomb ‘handling’ and related evacuation procedures,
- specialist information system fraud investigators,
- specialist technical attack investigators.

8.5.5 Forensic Analysis

Where identified by prior assessment as required for evidential purposes – de facto in the context of a significant information security incident, forensic analysis should be conducted by the ISIRT. It should involve the use of IT based investigative techniques and tools, supported by documented procedures, to review the designated information security incident(s) in more detail than has been the case hitherto in the information security incident management process. It should be conducted in a structured manner, and, as relevant, identify what may be used as evidence, whether for internal disciplinary procedures or legal actions.

The facilities needed for forensic analysis can be categorized into technical (e.g. audit tools, evidence recovery facilities), procedural, personnel and secure office facilities. Each forensic analysis activity should be fully documented, including as relevant photographs, audit trail analysis reports, data recovery logs. The proficiency of the person or people undertaking forensic analysis should be documented along with records of proficiency testing. Any other information that can demonstrate the objectivity and logical nature of analysis should also be documented. All records, of the information security incidents themselves, the forensic analysis activities, etc., and associated media, should be stored in a physically secure environment and controlled by procedures such that it cannot be accessed by unauthorized people nor altered or rendered unavailable. Forensic analysis IT based tools should comply with standards such that their accuracy cannot be legally challenged, as well as of course being kept up-to-date in line with technology changes. The ISIRT physical environment should provide demonstrable conditions that ensure the evidence is handled such that it cannot be challenged. Obviously enough personnel should be available, if necessary on an on-call basis, to be able to respond at any time.

Over time there will no doubt be requirements to review evidence in the context of a variety of information security incidents, including fraud, theft, and vandalism. Thus, to assist the ISIRT there will need to be available a number of IT based means and supporting procedures for uncovering information ‘hidden’ in an information system, service or network, including information that on first look appears to have been deleted, encrypted, or damaged. These means should address all known aspects associated with known types of information security incidents (and of course be documented in the ISIRT Procedures).

In today’s environment, forensic analysis will frequently need to encompass complex networked environments, where investigation will need to encompass an entire operating environment, including a multitude of servers – file, print, communications, e-mail etc., as well as remote access facilities. There are many tools available, including text search tools, drive imaging software and forensics suites. It is emphasized that the main focus of forensics analysis procedures is to ensure that evidence is kept intact and checked to ensure that it will stand up to any legal challenge, and that forensic analysis should be performed on an exact copy of the original data, to prevent the analysis work prejudicing the original media integrity.

The overall forensics analysis process should encompass, as relevant, the following activities:

- ensuring that the target system, service and/or network is protected during the forensic analysis from being rendered unavailable, altered or otherwise compromised, including by virus introduction, and that there are no or minimal effects on normal operations,
- prioritizing the ‘capture’ of ‘evidence’ i.e. proceeding from the most volatile to the least volatile (this will depend in large measure on the nature of the information security incident),
- identifying all relevant files on the subject system, service and/or network, including normal files, apparently (but not) deleted files, password or otherwise protected files, and encrypted files,
- recovering as much as is possible of discovered deleted files, and other data,
- uncovering IP addresses, host names, network routes and Web site information,

- extracting the contents of hidden, temporary and swap files used by both application and operating system software,
- accessing the contents of protected or encrypted files (unless prevented under law),
- analyzing all possibly relevant data found in special (and typically inaccessible) disc storage areas,
- analyzing file access, modification and creation times,
- analyzing system/service/network and application logs,
- determining the activity of users and/or applications on a system/service/network,
- analyzing e-mails for source information and content,
- performing file integrity checks to detect Trojan horse files and files not originally on the system,
- analyzing, if applicable, physical evidence, for example fingerprints, property damage, video surveillance, alarm system logs, pass card access logs, and interview witnesses,
- ensuring that extracted potential evidence is handled and stored in such a way that it cannot be damaged or rendered unusable, and that sensitive material cannot be seen by those not authorized. It is emphasized that evidence gathering should always be in accordance with the rules of the court or hearing in which the evidence may be presented,
- concluding on the reasons for the information security incident, the actions required and in what timeframe, with evidence including lists of relevant files included in an attachment to the main report,
- as required, providing expert support to any disciplinary or legal action.

The method(s) to be followed should be documented in the ISIRT Procedures.

The ISIRT should accommodate sufficient combinations of skills to provide wide coverage of technical knowledge (including of the tools and techniques likely to be used by deliberate attackers), analysis/investigative experience (including regarding the preservation of usable evidence), knowledge of relevant legislation and regulation implications, and ongoing knowledge of incident trends.

8.5.6 Communications

In many cases when an the information security incident has been confirmed by the ISIRT as real, there will be a need for certain people to be informed both internally (outside of normal ISIRT/management lines of communication) and externally – including the Press. This may need to occur at a number of stages, for example when an the information security incident is confirmed as real, when it is confirmed as under control, when it is designated for 'crisis' activities, when it is closed and when post incident review has been completed and conclusions reached.

To aid this activity when the need arises, it is very sensible practice to prepare certain information in advance such that it can be quickly adjusted to the circumstances of a particular information security incident and issued to the Press and/or other Media. If any information pertaining to information security incidents is be released to the Press it should be done in accordance with organization's information dissemination policy. Information to be released should be reviewed by the relevant parties, which may include senior management, public relations co-ordinators and information security personnel.

8.5.7 Escalation

There will be circumstances where matters will have to be escalated either to senior management, another group within the organization or persons or groups outside of the organization. This may be for a decision to be made on recommended actions to deal with an information security incident or for further assessment to determine what actions are required. This could be following the assessment processes described above in Clause 8.4, or indeed it could be during those processes if some major issue becomes evident early. Guidance should be available in the information security incident management scheme documentation for those who are likely at some point to need to escalate matters, i.e. operations support group and ISIRT members.

8.5.8 Activity Logging, and Change Control

It is emphasized that all involved in the reporting and management of an information security incident should properly log all activities for later analysis. This should be included with the information security incident reporting form and in the information security event/incident database, continually kept up-to-date throughout the cycle of an information security incident from first reporting form to completion of post incident review. This information should be retained provably secure and with an adequate back-up regime. Further, all changes made in the context of tracking an information security incident and updating the information security incident reporting form and the information security event/incident database should be under a formally accepted change control scheme.

9 Review

9.1 Introduction

Once an information security incident has been resolved and closure agreed, then there will be further forensic analysis conducted and a review to identify lessons and potential improvements to overall security and to the information security incident management scheme.

9.2 Further Forensic Analysis

It may be that once an incident has been resolved there is still a need for forensic analysis to identify evidence. This should be conducted by the ISIRT using the same toolset and procedures as suggested in Clause 8.5.5.

9.3 Lessons Learnt

Once an information security incident has been closed, it is important that the lessons to be learned from the handing of the information security incident are quickly identified and acted upon. The lessons could be in terms of:

- new or changed requirements for information security safeguards. These could be technical or non-technical (including physical) safeguards. Dependent on the lessons learned, these could include the need for rapid material updates for, and delivery of, security awareness briefings (for users as well as other personnel), and rapid revision and issue of security guidelines and/or standards,

- and/or changes to the information security incident management scheme and its processes, reporting forms and information security event/incident database.

Further, in this activity it is necessary to look beyond a single information security incident and check for trends/patterns which themselves may help identify the need for safeguards or approach changes. It is also sensible practice following an IT oriented information security incident, to conduct information security testing, particularly vulnerability assessment.

Thus, the data in the information security event/incident database should be analyzed on a regular basis in order to:

- identify trends/patterns,

- identify areas of concern,

- analyze where preventive action could be taken to reduce the likelihood of future incidents.

Relevant information acquired throughout the course of an information security incident should be channeled into the trend/pattern analysis. This can contribute significantly to the early identification of information security incidents and provide a warning of what further information security incidents may arise, based on previous experience and documented knowledge.

Use should also be made of information security incident and related vulnerability information received from government, commercial CERTs and suppliers.

Vulnerability assessment/security testing of an information system, service and/or network following an information security incident, should not be confined to only the information system, service and/or network, affected by the information security incident. It should be expanded to include any related information systems, services and/or networks. A complete vulnerability assessment is used to highlight the existence of the vulnerabilities exploited during

the information security incident on other information systems, services and/or networks and to ensure that no new vulnerabilities are introduced.

It is important to stress that vulnerability assessments should be conducted on a regular basis, and that the re-assessment of vulnerabilities after an information security incident has occurred should be part of this continuous assessment process (and not as a replacement).

Summary analyses of information security incidents should be produced for tabling at each meeting of the organization's management information security forum and/or other forum defined in the overall organizational information security policy.

9.4 Identification of Security Improvements

During review after an information security incident has been resolved, new or changed safeguards may be identified as being required. The recommendations and related safeguard requirements may be such that it is not feasible financially or operationally to implement them immediately, in which case they should feature in the longer-term aims of the organization. For example migration to a more secure robust firewall may not be financially feasible in the short term, but needed to be factored into an organization's long-term information security goals. (See also Clause 10.3 below.)

9.5 Identification of Scheme Improvements

Post-incident resolution, the ISIRT manager or a nominee should review all that has happened to assess and thus 'quantify' the effectiveness of the entire response to an information security incident. Such an analysis aims to determine which parts of the information security incident management scheme worked successfully and identify if any improvements are required.

An important aspect of post response analysis is to feed information and knowledge back into the information security incident management scheme. If of sufficient severity, a meeting of all the relevant parties should be scheduled shortly after an incident resolution while information is still fresh in people's minds. Factors to consider in such a meeting include the following:

- did the procedures outlined in the information security incident management scheme work as intended?
- are there any procedures or methods that would have aided in the detection of the incident?
- were any procedures or tools identified that would have been of assistance in the response process?
- were there any procedures that would have aided in recovering information systems following an incident identified?
- was the communication of the incident to all relevant parties effective throughout the detection, reporting and response process?

The results of the meeting should be documented and any agreed actions acted upon appropriately (see Clause 10.4 below).

10 Improve

10.1 Introduction

The "Improve" phase encompasses the implementation of the recommendations from the "Review" phase, i.e. for improvements to security risk analysis and management results, to security and to the information security incident management scheme. Each of these topics is addressed in the clauses below.

10.2 Security Risk Analysis and Management Improvement

Depending on the severity and impact of an information security incident, an assessment of information security risk analysis and management review results may be necessary to take into account new threats and vulnerabilities. As a

follow-on to the completion of an update information security risk analysis and management review, it may be necessary to introduce changed or new safeguards

10.3 Make Security Improvements

Following the recommendations made during the "Review" phase (see Clause 9.4 above), and analysis of a number of information security incidents, implementation of updated and/or new safeguards will need to be initiated. As discussed in clause 9.3 above, these could be technical (including physical) safeguards, and may include the need for rapid material updates for, and delivery of, security awareness briefings (for users as well as other personnel), and rapid revision and issue of security guidelines and/or standards. Further, an organization's information systems, services and networks should be subject to regular vulnerability assessments to aid in the identification of vulnerabilities and provide a process of continual system/service/network hardening.

In addition, whilst reviews of information security related procedures and documentation may be conducted in the immediate aftermath of an incident, it is more likely that this will be required as a later response. Following an information security incident, if relevant information security policies and procedures should be updated to take into account information gleaned and any problem issues identified during the course of the incident management process. It will be a long-term aim of the ISIRT, in conjunction with the organization's information security manager, to ensure that these information security policy and procedural updates are propagated throughout the organization.

10.4 Make Scheme Improvements

Areas identified for improvement to the information security incident management scheme (see Clause 9.5 above) should be reviewed and justified changes incorporated into an update of the scheme documentation. The changes to the information security incident management processes, procedures and the reporting forms should be subject to thorough checking and testing before going live.

10.5 Other Improvements

Other improvements may have been identified during the "Review" phase, for example changes in information security policies, standards and procedures, and changes to IT hardware and software configurations.

11 Summary

This Technical Report provides an overview of information security incident management, the benefits of adopting an information security incident management scheme, and the key issues associated with adopting such a scheme. Clear steps pertaining to planning and documenting an information security incident management policy and scheme are detailed along with the associated processes and procedures for managing information security incidents, and conducting post-incident resolution activities.

Annex A
(informative)

Example Information Security Event and Incident Report Forms

Information Security Event and Incident Reports

Notes for completion

The purpose of these forms - the information security event and incident report forms – is to provide information about an information security event, and then, if it is determined to be an information security incident, about the incident, to the appropriate people.

If you suspect that an information security event is in progress or may have occurred, particularly one which may cause substantial loss or damage to the organization's property or reputation, you should ***immediately*** complete and submit an information security event report form (see the first part of this Annex) in accordance with the procedures described in the organization's information security incident management scheme.

The information you provide will be used to initiate appropriate assessment, which will determine whether the event is to be categorized as an information security incident or not, and if it is any remedial measures necessary to prevent or limit any loss or damage. Given the potentially time-critical nature of this process, ***it is not essential to complete all fields in the reporting form at this time***.

If you are an operations support group member reviewing already completed/part-completed forms, then you will be required to take a view as to whether the event needs to be categorized as an information security incident. If an event is so categorized, you should complete the information security incident form with as much information as you are able and forward both the information security event and incident forms to the ISIRT. Whether the information security event is categorized as an incident or not, the information security event/incident database should be updated.

If you are an ISIRT member reviewing information security event and incident forms forwarded by an operations support group member, then the incident form should be then updated as the investigation progresses and related updates made to the information security event/incident database.

Please observe the following guidelines when completing the forms:

- if it is possible, the form should be completed and submitted electronically[10]. (When problems exist, or are considered to exist, with default electronic reporting mechanisms (e.g. e-mail), including when it is thought possible that the system is under attack and reporting forms could be read by unauthorized people, then alternative means of reporting should be used. Alternative means could include in person, by telephone or text messaging.),

- only provide information you know to be factual – do not speculate in order to complete fields. Where it is appropriate to provide information you cannot confirm, please clearly state that the information is unconfirmed, and what leads you to believe it may be true,

- you should provide your full contact details. It may be necessary to contact you – either very soon or at a later date – to obtain further information concerning your report,

If you later discover that any information you have provided is inaccurate, incomplete or misleading, you should amend and re-submit your report.

[10] If at all possible these forms should be electronic (e.g. in secure web page) form with linkage to the electronic information security event/incident database. In today's world, to operate a paper-based scheme would be time consuming and not the most efficient way of operating.

Information Security Event Report

Date of Event **Page 1 of 1**

Event Number:[11] **(If Applicable) Related Event and/or Incident Identity Numbers**:

REPORTING PERSON DETAILS

Name ..... **Address** .....

Organization ....

Telephone ..... **Email** .....

.....

INFORMATION SECURITY EVENT DESCRIPTION

Description of the Event:

- What Occurred
- How Occurred
- Why Occurred
- Components Affected
- Adverse Business Impacts
- Any Vulnerabilities Identified

INFORMATION SECURITY EVENT DETAILS

Date and Time the Event Occurred

Date and Time the Event was Discovered

Date and Time the Event was Reported

Is the Event Over? ***(tick as appropriate)*** **YES** ☐ **NO** ☐

If yes, Specify How Long the Event has Lasted in Days/Hours/Minutes

[11] *(Event numbers should be allocated by the organization's ISIRT Manager.)*