International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1056

(01/2009)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Security incident management guidelines for telecommunications organizations

Recommendation ITU-T X.1056

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	**X.1050–X.1069**
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1056

Security incident management guidelines for telecommunications organizations

Summary

Recommendation ITU-T X.1056 provides an overview of security incident management processes and services for telecommunication organizations. It provides concepts and key issues associated with security incident management. Since the telecommunication organizations need to have processes in place to not only handle incidents that do occur but to prevent incidents from re-occurring, five high-level processes are described along with the relationship to the security management. In addition, a list of services that a security incident management team can provide is suggested in terms of reactive, proactive, and security quality management services.

Source

Recommendation ITU-T X.1056 was approved on 13 January 2009 by ITU-T Study Group 17 (2009-2012) under Recommendation ITU-T A.8 procedures.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T X.1056

Security incident management guidelines for telecommunications organizations

1 Scope

This Recommendation seeks to assist telecommunication organizations in mitigating the risks from security incidents by providing practical guidance on how to respond to incidents effectively and efficiently. Telecommunication organizations are encouraged to tailor the recommended guidelines and solutions to meet their specific security or business requirements.

This Recommendation presents general security incident management guidelines that are independent of particular hardware platforms, operating systems, and applications to supportively provide detailed implementation guidelines in line with [ITU-T X.1051]. Specifically, it includes guidance on establishing an effective security incident management, but the primary focus of the Recommendation is on detecting, analysing, prioritizing, and responding incidents.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[ITU-T X.1051] Recommendation ITU-T X.1051 (2008) | ISO/IEC 27011:2008, *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*.

[ISO/IEC TR 18044] ISO/IEC TR 18044 (2004), *Information technology – Security techniques – Information security incident management*.

3 Definitions

3.1 Terms and definitions for security incidents in general

In order to make use of a common and sound vocabulary regarding security incident management for telecommunications organizations, this Recommendation follows the definitions in [ITU-T E.409] and [ISO/IEC TR 18044].

3.1.1 business continuity planning [ISO/IEC TR 18044]: 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.

3.1.2 crisis [ITU-T E.409]: A crisis is a state caused by an event, or the knowledge of a forthcoming event, that may cause severe negative consequences. During a crisis, one may, in best cases, have the possibility of taking measures to prevent the crisis from becoming a catastrophe. When a catastrophe occurs, a Business Continuity Plan (BCP) normally exists as well as a crisis management team to handle the situation.

3.1.3 event [ITU-T E.409]: An event is an observable occurrence which is not possible to (completely) predict or control.

3.1.4 incident [ITU-T E.409]: An event that might have led to an occurrence or an episode which is not serious.

3.1.5 incident handling: Incident handling is a service that involves all the processes or tasks associated with addressing an incident. Incident handling includes multiple functions such as detecting, reporting, triage, analysis and incident response.

3.1.6 incident management: Incident management encompasses the incident handling service and other proactive services that help prevent incidents by providing guidance against potential risks and threats.

3.1.7 ISIRT (Information Security Incident Response Team) [ISO/IEC TR 18044]: ISIRT is a team of appropriately skilled and trusted members of the organization, which will handle security incidents during their lifecycle. At times this team may be supplemented by external experts, for example from a recognized computer incident response team.

3.1.8 security incident [ITU-T E.409]: A security incident is any adverse event whereby some aspect of security could be threatened.

3.2 Terms and definitions for telecommunications security incidents

3.2.1 buffer overflow: A buffer overflow is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data, and may cause a process to crash or produce incorrect results. A buffer overflow can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits. Sufficient bounds checking by either programmer, compiler or runtime can prevent buffer overflows.

3.2.2 DoS/DDoS attack: A denial of service (DoS) attack or a distributed denial of service (DDoS) attack floods a network with an overwhelming amount of traffic, slowing its response time for legitimate traffic or causing it to halt completely. It generally consists of the concerted, malevolent efforts of a person or persons.

3.2.3 telecommunications security incident: Any real or suspected adverse event in relation to the security of telecommunications. This includes:

- intrusion into telecommunication systems via the network;
- occurrence of computer viruses;
- probes for vulnerabilities via the network into one or more computer systems;
- PABX call leak-through;
- any other undesired events arising from unauthorized internal or external actions.

4 Abbreviations

This Recommendation uses the following abbreviations:

DoS Denial of Service

DDoS Distributed Denial of Service

IDS Intrusion Detection Systems

ISIRT Information Security Incident Response Team

NGN Next Generation Network

5 Concepts and issues of security incident management

5.1 Concepts of security incident management

Security products throughout the organization scan systems and network traffic and report on potentially suspicious activity. Each report is termed a security event, and many thousands of events typically occur each day in organizations of moderate size. An event may be anything from a malformed or over-length network packet to a failed login on a computer. Determining whether any given event indicates trouble is difficult. Malformed packets can be malicious – potentially indicating a buffer overflow attack – or they can simply be innocent anomalies. Failed logins can signal an attempt to break into a system or they can be the result of simple typographical errors. Additional context is required to determine whether a problem exists and if so, what action is required. Focusing on event management without that additional context will result in poor coordination, time wasted on events that are "false positives", and operations that are reactive and unfocused.

A security incident is a set of one or more events or conditions that require action and closure in order to maintain an acceptable risk profile (see [b-ITU-T X.1055]). In the haystack of events, organizations have to find the "needles" that are the security incidents. Events may be isolated and disconnected, but security incidents add the context that enables security administrators to gain understanding and take action.

[ITU-T E.409] assumes that an incident is less severe than a security incident. Figure 1 shows the pyramid of events. At the bottom there are events, followed by incident, security incident and, at the top, crisis and catastrophe. The closer to the top an event is, the more serious it is.

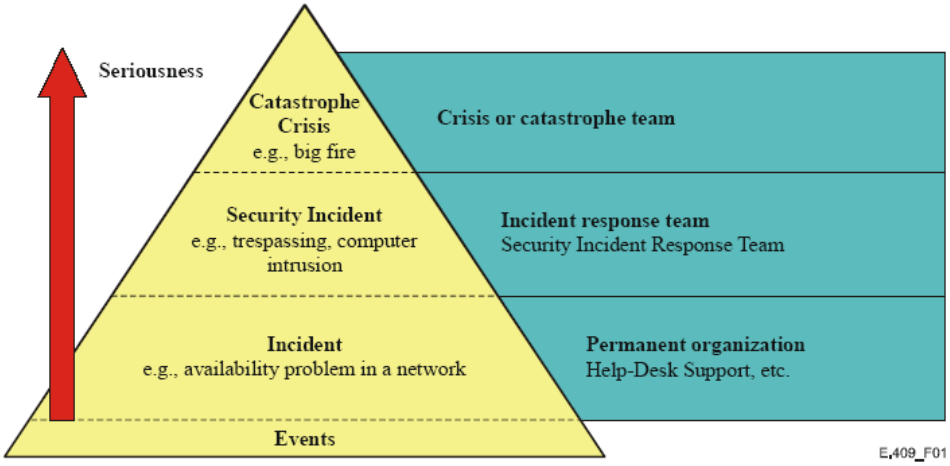

Figure 1 – Pyramid of events (see Figure 1 of [ITU-T E.409])

Defined in this way – as a set of events or conditions requiring response and closure – security incidents comprise more than the significant threats that jeopardize business and require intervention. They also include more mundane situations that occur on a daily basis and threaten the

business only if no action is taken. Examples of these routine situations include "low and slow" port scans and some varieties of email worms. Most organizations face thousands of instances of the latter types of threats, together with the higher profile blended threats like Code red, Nimda, and Klez.

Besides attacks, known system vulnerabilities or discovered policy violations are also security incidents that require a response in order to protect the business. When related events (e.g., attacks, vulnerabilities, and policy violations) are viewed together, the true nature (or type) of the security incident becomes evident. Changing from an event management to a security incident management approach allows technicians to understand:

- the scope: the number of systems affected;
- the impact: the degree to which each system is affected in terms of confidentiality, integrity and availability;
- the business criticality: the importance of the incident based on the business value of the impacted systems relative to other systems;
- the priority: the urgency of the required response relative to other incidents.

An incident-centric approach simplifies many of the otherwise complex and burdensome tasks of security management. Effective security incident management reduces the volume of data that requires monitoring and also allows response activities to be prioritized based on a unified view of the business impact of each incident.

Security incident management is proactive, controlled and consistent. In contrast, an event-centric approach ignores critical characteristics of incidents that are essential to an effective and complete response. Furthermore, relying solely on manual methods of identifying security incidents is impractical and increases the likelihood of poor response decisions.

In the early history of security incident management, the processes and functions performed by ISIRT members were primarily reactive in nature, focusing on incident handling; actions were taken to resolve or mitigate an incident when it occurred. As teams increased their capability and scope, they began to expand their activities to include more proactive efforts.

Figure 2 shows the relationship between security incident management, handling, and response. Security incident handling includes multiple functions such as detecting, reporting, triage, analysis, and incident response. Security incident management encompasses the incident handling service and other proactive services that help prevent incidents by providing guidance against potential risks and threats.

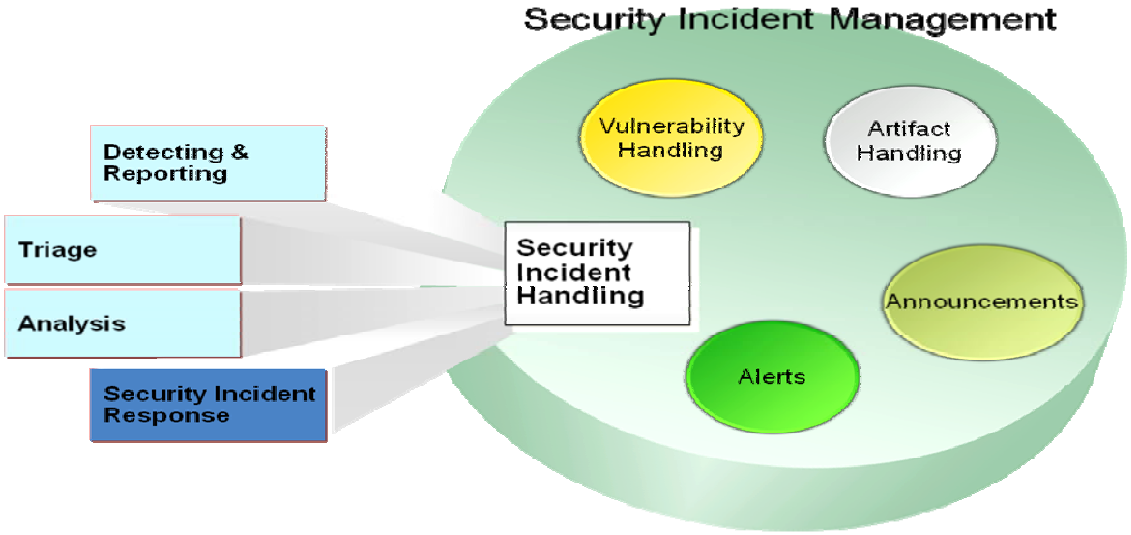

Figure 2 – Relationships among incident management, incident handling, and incident response (Modified from [b-CMU/SEI-TR-015])

As organizations become more complex and security incident management capabilities, such as ISIRTs, become more integrated into organizational business functions, it is clear that security incident management is not just the application of technology to resolve security events. It is also the development of a plan of action, a set of processes that are consistent, repeatable, of high quality, measurable, and understood within the constituency.

Therefore, the factors for the effective management of security incidents that need to be considered are as follows:

- integrate security incident management into the existing processes and organizational structures so that it enables, rather than hinders, critical business functions;
- strengthen and improve the capability of telecommunications organizations to effectively manage security events and thereby keep intact the availability, integrity, and confidentiality of an organization's system and critical assets, where required;
- support, complement, and link to any existing business continuity or disaster recovery plans where and when appropriate;
- support, complement, and provide input into existing business and IT policies that impact the security of an organization's infrastructure;
- implement a command and control structure, clearly defining responsibilities and accountability for decisions and actions;
- be part of an overall strategy to protect and secure critical business functions and assets;
- include the establishment of processes for:
  - notification and communication,
  - analysis and response,
  - collaboration and coordination,
  - maintenance and tracking of records.

5.2 Characteristics of telecommunications security incidents

Since the telecommunications service has the role of infrastructure for other applications, security incidents in telecommunications services might cause serious impact to the telecommunication service providers, as well as to the national economy. Security incidents in the context of telecommunication services can be described in terms of the following major characteristics:

- Telecommunications services are heavily dependent on various interconnected facilities, such as routers, switches, domain name servers, transmission relay systems, network management systems, etc. Therefore, telecommunications security incidents can occur at various equipments and incidents can propagate into other equipments rapidly through the network.
- In addition to telecommunications facilities, vulnerabilities in network protocols and topology can result in serious security incidents. In particular, convergence of wired and wireless networks into next generation networks (NGNs) can impose significant challenges to developing interoperable protocols.
- A major concern of telecommunications carriers is the prospect of security compromises causing network down-time, which can be extremely costly in terms of customer relations, lost revenue, and recovery costs. Deliberate attacks on the availability of the national telecommunication infrastructure can be viewed as a national security concern.
- Telecommunications management networks and systems are susceptible to hacker penetrations. A common motivation for such penetrations is theft of telecommunications services. Such theft can be engineered in various ways, such as invoking diagnostic functions, manipulating accounting records and altering provisioning databases, and eavesdropping on subscriber calls.
- In addition to external penetrations, carriers are concerned about security compromises from internal sources, such as invalid changes to network management databases by unauthorized personnel. Such occurrences may be accidental or deliberate.

5.3 Key issues of security incident management

A number of key issues should be addressed to achieve a good security incident management scheme (see [ISO/IEC TR 18044]), including:

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

Each of these issues is discussed below.

5.3.1 Management commitment

Ensuring continued management commitment is vital for the acceptance of a structured approach to 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 a security incident response capability.

5.3.2 Awareness

Another important issue to the acceptance of a structured approach to 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 security incident management, they are less likely to participate properly in its operation.

Thus any security incident management scheme should be accompanied by an awareness program which contains the following:

- benefits to be derived from the structured approach to security incident management, both to the organization as a whole and to users,
- incident information held in, and output from, the security 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.

5.3.3 Legal and regulatory aspects

The following legal and regulatory aspects of security incident management should be addressed in the security incident management policy and related documents such as guidelines.

- **Adequate data protection and privacy of personal information is provided**. In those countries where a specific legislation exists that covers data confidentiality and integrity, it is often restricted to the control of personal data. As security incidents need to be typically accountable to individuals, information of a personal nature may therefore need to be recorded and consequently need to be addressed. A structured approach to security incident management therefore needs to take into account the appropriate privacy protection.
- **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. It should be noted however, that a security incident report may not need to be made where, in the particular country, 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 fulfilment of commercial contractual obligations**. Where there are binding requirements on the provision of a security incident management service, for example covering required response times, an organization should ensure that appropriate security is provided to ensure that such obligations can be met in all circumstances. (Related to this, if an organization contracts with an external organization for support, for example a CERT, then it should be ensured that all requirements, including response times, are included in the contract with the external organization.)
- **Legal issues related to policies and procedures are dealt with**. The policies and procedures associated with the security incident management scheme should be checked for potential legal issues, for example if there are statements about disciplinary and/or legal action taken against those causing incidents.
- **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**. Security incident management team members may be required to sign non-disclosure agreements both when starting and leaving employment.
- **Law enforcement requirements are addressed**. The issues associated with the possibility that law enforcement agencies might legally request information from a security incident management team 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 need to be clarified.
- **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 security safeguards should be in place, including probably tamper-proof audit trails, to be able to successfully prosecute, or bring internal disciplinary procedures against, 'attackers', independently on whether the attack is 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 forums.
- **Legal aspects associated with monitoring techniques**. 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 use of specific 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 [b-ISO/IEC 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 it when they join an organization or are granted access to information systems.)

5.3.4 Operational efficiency and quality

The operational efficiency and quality of a structured approach to security incident management relies on a number of factors, including quality of notification, ease of use, speed, obligation to notify incidents, and training. Some of these factors relate to making sure that users are aware of the value of security incident management and are 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 security incident management personnel, in order to minimize delays.

5.3.5 Anonymity

The issue of anonymity is fundamental to the success of security incident management. Users should be convinced that the information they contribute on security incidents is completely protected and, where necessary, sanitized so 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 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 security incident. The ISIRT may need to obtain additional information not initially relayed by the person or party who reported the incident; furthermore, often important information about the security incident itself can be derived from who detects it first.

5.3.6 Confidentiality

A security incident management scheme may contain sensitive information, and people involved in addressing incidents may handle sensitive information. During processing either this information should be anonymized or personnel involved should be required to sign confidentiality agreements. When security incidents are logged in a generalized problem management system, sensitive details may also have to be omitted. Additionally, the security incident management scheme should have provisions for controlling the communication of the incident to external parties, including the media, business partners, customers, law enforcement, and the general public.

5.3.7 Credible operations

Any 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 a security incident. The function of the 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 official directly responsible for managing incident responses. Finance of the capability should also be segregated to avoid undue influence.

5.3.8 Typology

A common typology, reflecting the general structure of the 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. (It should be noted that it is not the purpose of this Recommendation to define a common typology; the reader is advised to refer to alternative sources for this information.)

6 Security incident management processes

6.1 Overview of security incident management processes

Telecommunications organizations need to have processes in place to not only handle security incidents that do occur but to prevent incidents from occurring or re-occurring. These include processes to:

- plan and implement a security incident management capability;
- secure and harden the organization's infrastructure to help prevent security incidents from occurring or to mitigate an ongoing incident;
- detect, triage, and respond to security incidents and events when they occur.

These basic processes form the five high-level processes in the security incident management model as specified in [b-CMU/SEI-TR-015]:

- Prepare/Sustain/Improve (Prepare), which includes sub-processes to:
  - plan and implement an initial security incident management or ISIRT capability;
  - sustain that capability;
  - improve an existing capability through lessons learned and evaluation;

  - perform a post-mortem review of security incident management actions when necessary;
  - transfer infrastructure process improvements from the post-mortem to the Protect process.
- Protect Infrastructure (Protect), which includes sub-processes to:
  - implement changes to the computing infrastructure to stop or mitigate an ongoing incident or to stop or mitigate the potential exploitation of a vulnerability in the hardware or software infrastructure;
  - implement infrastructure protection improvements resulting from post-mortem reviews or other process improvement mechanisms;
  - evaluate the computing infrastructure by performing such tasks as proactive scanning and network monitoring, and by performing security and risk evaluations;
  - transfer to the Detect process any information about ongoing incidents, discovered vulnerabilities, or other security-related events that were uncovered during the evaluation.
- Detect Events (Detect), which includes sub-processes to:
  - identify events and report those events;
  - receive the reports of events;
  - proactively monitor indicators such as network monitoring, IDS, or technology watch functions;
  - analyse the indicators being monitored (to determine any notable activity that might suggest malicious behaviour or identify risk and threats to the organization's infrastructure);
  - forward any suspicious or notable event information to the Triage process;
  - reassign events to areas outside of the security incident management process if applicable;
  - close any events that are not forwarded to the Triage process.
- Triage Events (Triage), which includes sub-processes to:
  - categorize and correlate events;
  - prioritize events;
  - assign events for handling or response;
  - pass on relevant data and information to the Respond process;
  - reassign events to areas outside of the security incident management process, if applicable;
  - close any events that are not forwarded to the Respond process or reassigned to other areas.
- Respond (Respond), which includes sub-processes to:
  - analyse the event;
  - plan a response strategy;
  - coordinate and provide technical, management, and legal response, which can involve actions to contain, resolve, or mitigate incidents and actions to repair and recover affected systems;
  - communicate with external parties;

– reassign events to areas outside of the security incident management process, if applicable;
– close response;
– pass lessons learned and incident data to the Prepare process for use in a post-mortem review.

The word "events" is chosen to describe the information and activity that are detected and triaged. The word "incident" is used once it has been determined that a true security incident has occurred. Although this may happen in the Detect or Triage processes, it is often not until the Respond process that something is validated as a true security incident. That is why the process names for "Detect Events" and "Triage Events" differ from "Respond."

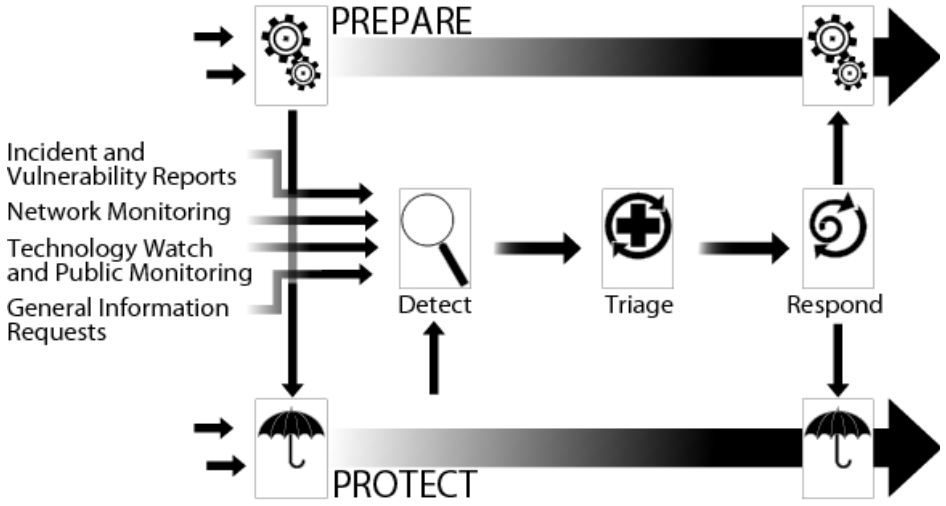

Figure 3 – Five high-level incident management processes (Source: [b-CMU/SEI-TR-015])

The above diagram can be explained as follows:

- This diagram shows the Prepare and Protect processes as continuous ongoing processes. This is signified by the arrows going across the diagram and by having the icons for each at the beginning and end of the arrows. These processes involve putting into place all the necessary staff, technology, infrastructure, policies, and procedures for security incident management activities to occur in a timely, coordinated, and effective manner. The use of the arrows surrounding the Detect, Triage, and Respond processes show that Prepare and Protect support and enable the other processes.
- The small arrows coming into the Prepare and Protect process indicate requirements, policies, or rules that will govern the structure and function of these processes. These arrows also indicate incoming process improvement requests.
- The line that goes from the Prepare to the Protect process signifies a handoff between these two processes. In this case, the information passed is process improvement requests for changes in the computing infrastructure that result from a post-mortem review done in the Prepare process. These changes in the infrastructure, if implemented, will help harden and secure the infrastructure to help prevent similar incidents from happening and the same incident from re-occurring.
- The Detect, Triage, and Respond processes are shown in sequence as information coming into the Detect process is evaluated to determine if it is notable and needs to be passed on to the Triage process for further analysis and assessment. If in the Triage process the received

information (whether it is an incident report, a vulnerability report, a general information request, or a suspicious event) requires a response, it is passed on to the Respond process.

- The arrow going from Protect to Detect indicates the passage of any incident or vulnerability reports that may result from infrastructure evaluations. It is possible that during an evaluation, a vulnerability, ongoing incident, or remnant of a past incident is discovered. This information needs to be passed to the Detect process.
- The arrows going from the Respond process to the Prepare process signify the handoff of process improvements and corresponding incident data or respond actions and decisions where appropriate. The handoff from Respond to Prepare passes this information to the post-mortem review sub-process within the Prepare process.

6.2 Relationship between security incident management and security management

Since the security incident management scope includes processes for protecting infrastructures and detecting events using network monitoring and IDS, it is necessary to distinguish between security management and security incident management. The boundary between the two is open to interpretation and can be confusing. The dividing line often depends on the structure of an organization's security or incident management capabilities.

Security incident management should be viewed as an integral component of security management. Security management encompasses all of the tasks and actions necessary to secure and protect an organization's critical assets, and this is much broader in scope than security incident management. It involves aligning and prioritizing security actions based on the organization's mission and objectives and assessing security risks to achieving such objectives. Security management includes risk management, audit, access control, account management, asset management, physical security, security policies, configuration management, change and patch management, disaster recovery, and business continuity.

Security management applies risk management approaches to help choose the most effective course of action. Security incident management may use many of these capabilities in the performance of its objectives, such as patch management, configuration management, or security policies. Security incident management touches many of the other security functions, indicating the need for established channels of communication and collaboration. But security incident management is not responsible for establishing and maintaining these capabilities. Security management provides a framework within which the execution of security incident management processes occurs.

If the five high-level security incident management processes are examined, some of them are overlapped with security management in some fashion. Figure 4 shows how security incident management processes fit into the scope of security management.

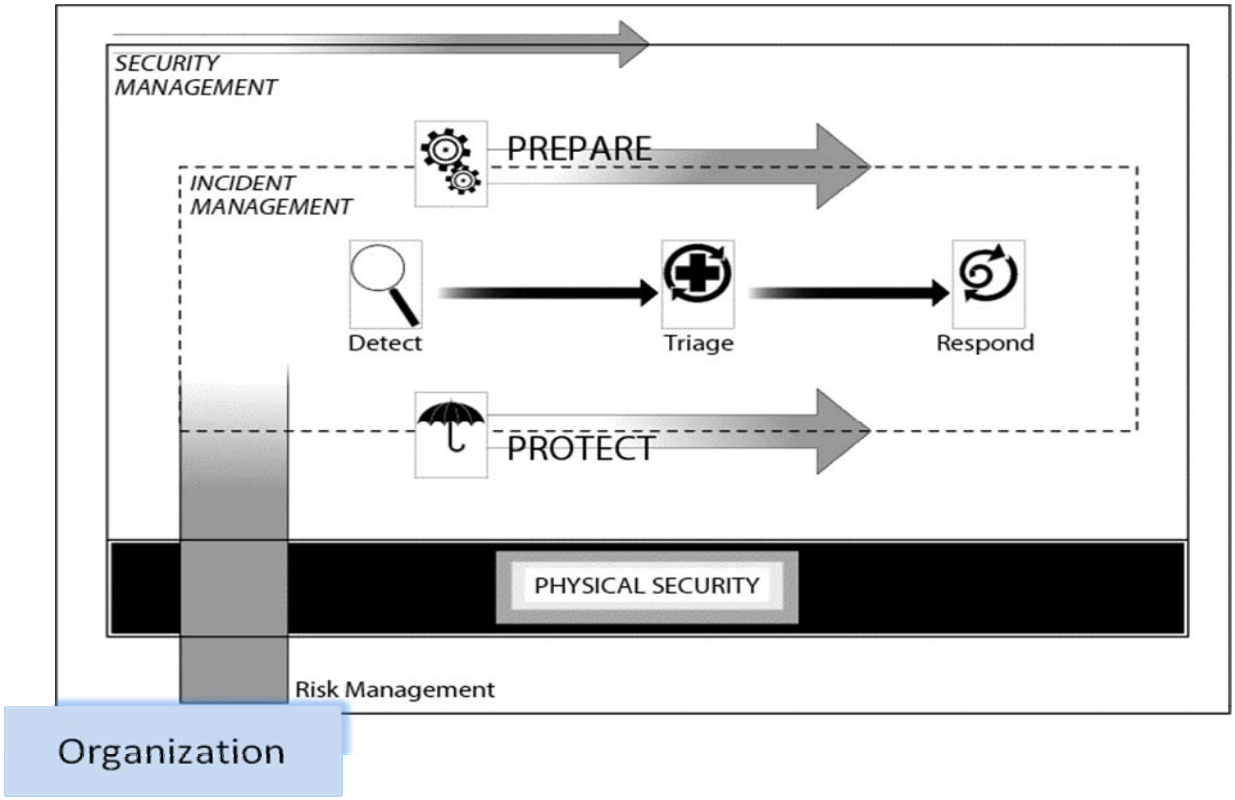

Figure 4 – Comparison of incident management and security management (Source: [b-CMU/SEI-TR-015])

In Figure 4, the arrows show that Prepare and Protect processes are included in both incident management and security management. The incident management Protect process addresses infrastructure changes in response to current computer security threats, while the security management Protect process addresses a wider range of protection activities, including those necessary to configure and secure a computing infrastructure and maintain and monitor those configurations. The Detect, Triage, and Respond processes are totally within the scope of incident management, with regard to the treatment of computer security events and incidents.

Security management exercises physical security and risk management capabilities to protect critical assets at the organizational level. Risk management also informs security incident management by balancing incident response actions with business drivers and organizational mission. Applying risk management during incident response helps determine what actions should be taken based on the criticality of the asset (information, system, network) that is under threat of attack. Not all assets are equivalent and not all response efforts are cost effective in light of the organizational mission. For example, if a telecommunications organization finds that its computer infrastructure is propagating a harmless virus, it may keep its infected systems up and running rather than shut down production to remove the virus. If the organizational mission is to keep production systems running and make money, then shutting them down could result in a higher risk (loss of revenue) than letting the virus propagate. Although this action may not be considered best practice, it reflects how tradeoffs may occur. Business and organizational drivers very often supersede recommended security and incident management actions.

This clause discusses the five high-level processes of incident management and how they relate to one another. This clause also discusses how this set of processes can be used to help create, sustain, and evaluate an incident management capability, which can be provided by ISIRT's services described in clause 7.

7 Security incident management services

7.1 Overview

One of the primary issues to be addressed in creating an ISIRT is deciding what services the ISIRT will provide to its organization. This process also involves naming and defining each provided service, which is not always an easy task. Experience has shown that there is often great confusion about the names used for ISIRT services. The purpose of this clause is to present a list of ISIRT services and their definitions based on [b-CMU/SEI HB-002]. Although this clause focuses on services provided by ISIRTs, many of these same services can also be provided by system, network, and security administrators who perform ad hoc incident handling as part of their normal administrative work when there is no established ISIRT.

ISIRT has to take great care in choosing the services it will offer. The set of services provided will determine the resources, skill sets, and partnerships the team will need in order to function properly. The selection of services should first and foremost support and enable the business goals of the telecommunications organizations.

7.2 Service categories

There are many services that an ISIRT can choose to offer. Each ISIRT is different and provides services based on the mission, purpose, and constituency of the team. ISIRT services can be grouped into three categories:

- **Reactive services**. These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core component of ISIRT work.
- **Proactive services**. These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future.
- **Security quality management services**. These services augment existing and well-established services that are independent of incident handling and traditionally performed by other areas of an organization such as the IT, audit, or training departments. If the ISIRT performs or assists with these services, the ISIRT's point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive but contribute indirectly to reducing the number of incidents.

The services are listed in Figure 5 and described in detail below.

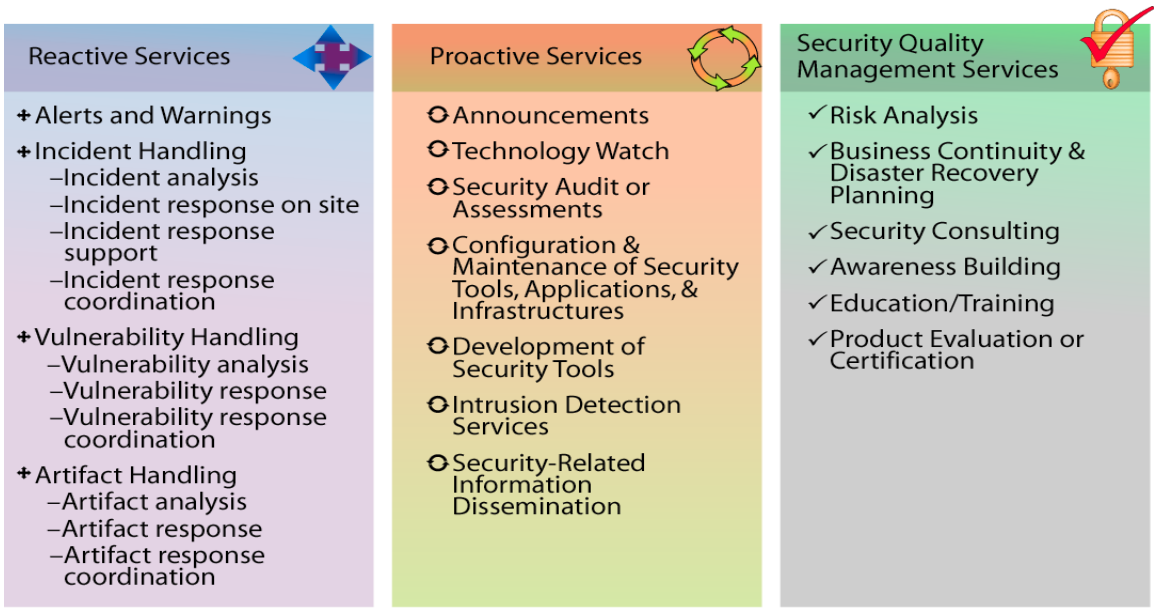

Figure 5 – List of common ISIRT services (Source: [b-CMU/SEI-TR-015])

It should be noted that some services have both a reactive and proactive side. For example, vulnerability handling can be done in response to the discovery of a software vulnerability that is being actively exploited. But it can also be done proactively by reviewing and testing code to determine where vulnerabilities exist, so the problems can be fixed before they are widely known or exploited.

7.3 Service descriptions

7.3.1 Reactive services

Reactive services are designed to respond to requests for assistance, reports of incidents from the ISIRT constituency, and any threats or attacks against ISIRT systems. Some services may be initiated by third-party notification or by viewing monitoring or intrusion detection systems (IDS) logs and alerts.

7.3.1.1 Alerts and warnings

This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action for dealing with the resulting problem. The alert, warning, or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected. Information may be created by the ISIRT or may be redistributed from vendors, other ISIRTs or security experts, or other parts of the constituency. Alerts and warnings can be categorized based on the severity of security incidents (see Appendix I).

7.3.1.2 Incident handling

Incident handling involves receiving, triaging, and responding to requests and reports, and analysing incidents and events. Particular response activities can include:

- taking action to protect systems and networks affected or threatened by intruder activity;
- providing solutions and mitigation strategies from relevant advisories or alerts;
- looking for intruder activity on other parts of the network;

- filtering network traffic;
- rebuilding systems;
- patching or repairing systems;
- developing other response or workaround strategies.

Since incident handling activities are implemented in various ways by different types of ISIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Incident analysis: There are many levels of incident analysis and many sub-services. Essentially, incident analysis is an examination of all available information and supporting evidence or artifacts related to an incident or event. It would be more efficient to analyse incidents if a standard template for security incident report is used (see Appendix II). The purpose of the analysis is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds. The ISIRT may use the results of vulnerability and artifact analysis (described below) to understand and provide the most complete and up-to-date analysis of what has happened on a specific system. The ISIRT correlates activity across incidents to determine any interrelations, trends, patterns, or intruder signatures. Two sub-services that may be done as part of incident analysis, depending on the mission, goals, and processes of the ISIRT, are:

- **Forensic evidence collection**: the collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise. This gathering of information and evidence has to be done in a way that documents a provable chain of custody that is admissible in a court of law under the rules of evidence. Tasks involved in forensic evidence collection include (but are not limited to) making a bit-image copy of the affected system's hard drive; checking for changes to the system such as new programs, files, services, and users; looking at running processes and open ports; and checking for Trojan horse programs and toolkits. ISIRT staff performing this function may also have to be prepared to act as expert witnesses in court proceedings.
- **Tracking or tracing**: the tracing of the origins of an intruder or identifying systems to which the intruder had access. This activity might involve tracking or tracing how the intruder entered the affected systems and related networks, which systems were used to gain access, where the attack originated, and what other systems and networks were used as part of the attack. It might also involve trying to determine the identity of the intruder. This work might be done alone but usually involves working with law enforcement personnel, Internet service providers, or other involved organizations.

Incident response on site: The ISIRT provides direct, on-site assistance to help constituents recover from an incident. The ISIRT itself physically analyses the affected systems and conducts the repair and recovery of the systems, instead of only providing incident response support by telephone or email (see below). This service involves all actions taken on a local level that are necessary if an incident is suspected or occurs. If the ISIRT is not located at the affected site, team members would travel to the site and perform the response. In other cases a local team may already be on site, providing incident response as part of its routine work. This is especially true if incident handling is provided as part of the normal job function of system, network, or security administrators in lieu of an established ISIRT.

Incident response support: The ISIRT assists and guides the victim(s) of the attack in recovering from an incident via phone, email, fax, or documentation. This can involve technical assistance in the interpretation of data collected, providing contact information, or relaying guidance on mitigation and recovery strategies. It does not involve direct, on-site incident response actions as

described above. The ISIRT instead provides guidance remotely so site personnel can perform the recovery themselves.

Incident response coordination: The ISIRT coordinates the response effort among parties involved in the incident. This usually includes the victim of the attack, other sites involved in the attack, and any sites requiring assistance in the analysis of the attack. It may also include the parties that provide IT support to the victim, such as Internet service providers, other ISIRTs, and system and network administrators at the site. The coordination work may involve collecting contact information, notifying sites of their potential involvement (as victim or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange and analysis. Part of the coordination work may involve notification and collaboration with an organization's legal counsel, human resources or public relations departments. It would also include coordination with law enforcement. This service does not involve direct, on-site incident response.

7.3.1.3 Vulnerability handling

Vulnerability handling involves receiving information and reports about hardware and software vulnerabilities; analysing the nature, mechanics, and effects of the vulnerabilities; and developing response strategies for detecting and repairing the vulnerabilities. Since vulnerability handling activities are implemented in various ways by different types of ISIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Vulnerability analysis: The ISIRT performs technical analysis and examination of vulnerabilities in hardware or software. This includes the verification of suspected vulnerabilities and the technical examination of the hardware or software vulnerability to determine where it is located and how it can be exploited. The analysis may include reviewing source code, using a debugger to determine where the vulnerability occurs, or trying to reproduce the problem on a test system.

Vulnerability response: This service involves determining the appropriate response to mitigate or fix vulnerabilities. This may involve developing or researching patches, fixes, and workarounds. It also involves notifying others of the mitigation strategy, possibly by creating and distributing advisories or alerts. This service can include installing patches, fixes, or workarounds.

Vulnerability response coordination: The ISIRT notifies the various parts of the organization or constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability. The ISIRT verifies that the vulnerability response strategy has been successfully implemented. This service can involve communicating with vendors, other ISIRTs, technical experts, constituent members, and the individuals or groups who initially discovered or reported the vulnerability. Activities include facilitating the analysis of a vulnerability or vulnerability report; coordinating the release schedules of corresponding documents, patches, or workarounds; and synthesizing technical analysis done by different parties. This service can also include maintaining a public or private archive or knowledge base of vulnerability information and corresponding response strategies.

7.3.1.4 Artifact handling

An artifact is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.

Artifact handling involves receiving information about and copies of artifacts that are used in intruder attacks, reconnaissance, and other unauthorized or disruptive activities. Once received, the artifact is reviewed. This includes analysing the nature, mechanics, version, and use of the artifacts; and developing (or suggesting) response strategies for detecting, removing, and defending against these artifacts. Since artifact handling activities are implemented in various ways by different types of ISIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Artifact analysis: The ISIRT performs a technical examination and analysis of any artifact found on a system. The analysis done might include identifying the file type and structure of the artifact, comparing a new artifact against existing artifacts or other versions of the same artifact to see similarities and differences, or reverse engineering or disassembling code to determine the purpose and function of the artifact.

Artifact response: This service involves determining the appropriate actions to detect and remove artifacts from a system, as well as actions to prevent artifacts from being installed. This may involve creating signatures that can be added to antivirus software or IDS.

Artifact response coordination: This service involves sharing and synthesizing analysis results and response strategies pertaining to an artifact with other researchers, ISIRTs, vendors, and other security experts. Activities include notifying others and synthesizing technical analysis from a variety of sources. Activities can also include maintaining a public or constituent archive of known artifacts and their impact and corresponding response strategies.

7.3.2 Proactive services

Proactive services are designed to improve the infrastructure and security processes of the constituency before any incident or event occurs or is detected. The main goals are to avoid incidents and to reduce their impact and scope when they do occur.

7.3.2.1 Announcements

This includes, but is not limited to, intrusion alerts, vulnerability warnings, and security advisories. Such announcements inform constituents about new developments with medium to long-term impact, such as newly found vulnerabilities or intruder tools. Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited.

7.3.2.2 Technology watch

The ISIRT monitors and observes new technical developments, intruder activities, and related trends to help identify future threats. Topics reviewed can be expanded to include legal and legislative rulings, social or political threats, and emerging technologies. This service involves reading security mailing lists, security web sites, and current news and journal articles in the fields of science, technology, politics, and government to extract information relevant to the security of the constituent systems and networks. This can include communicating with other parties that are authorities in these fields to ensure that the best and most accurate information or interpretation is obtained. The outcome of this service might be some type of announcement, guidelines, or newsletters focused at more medium- to long-term security issues.

7.3.2.3 Security audits or assessments

This service provides a detailed review and analysis of an organization's security infrastructure, based on the requirements defined by the organization or by other industry standards that apply. It can also involve a review of the organizational security practices. There are many different types of audits or assessments that can be provided, including:

- infrastructure review – manually reviewing the hardware and software configurations, routers, firewalls, servers, and desktop devices to ensure that they match the organizational or industry best practice security policies and standard configurations;

- best practice review – interviewing employees and system and network administrators to determine if their security practices match the defined organizational security policy or some specific industry standards;
- scanning – using vulnerability or virus scanners to determine which systems and networks are vulnerable;
- penetration testing – testing the security of a site by purposefully attacking its systems and networks.

Obtaining upper management approval is required before conducting such audits or assessments. Some of these approaches may be prohibited by organizational policy. Providing this service can include developing a common set of practices against which the audits or assessments are conducted, along with developing a required skill set or certification requirements for staff that perform the audits or assessments. This service could also be outsourced to a third party contractor or managed security service provider with the appropriate expertise in conducting audits or assessments.

7.3.2.4 Configuration and maintenance of security tools, applications, infrastructures, and services

This service identifies or provides appropriate guidance on how to securely configure and maintain tools, applications, and the general computing infrastructure used by the ISIRT constituency or the ISIRT itself. Besides providing guidance, the ISIRT may perform configuration updates and maintenance of security tools and services, such as IDS, network scanning or monitoring systems, filters, wrappers, firewalls, virtual private networks, or authentication mechanisms. The ISIRT may even provide these services as part of their main function. The ISIRT may also configure and maintain domain name servers and other servers, desktops, laptops, personal digital assistants, and other wireless devices according to security guidelines. This service includes escalating to management any issues or problems with configurations or the use of tools and applications that the ISIRT believes might leave a system vulnerable to attack.

7.3.2.5 Development of security tools

This service includes the development of any new, organization-specific tools that are required or desired by the ISIRT. This can include, for example, developing security patches for customized software used by the constituency or secured software distributions that can be used to rebuild compromised hosts. It can also include developing tools or scripts that extend the functionality of existing security tools, such as a new plug-in for a vulnerability or network scanner, scripts that facilitate the use of encryption technology, or automated patch distribution mechanisms.

7.3.2.6 Intrusion detection services

ISIRTs that perform this service review existing IDS logs, analyse and initiate a response for any events that meet their defined threshold, or forward any alerts according to a pre-defined service level agreement or escalation strategy. Intrusion detection and analysis of the associated security logs can be a daunting task – not only in determining where to locate the sensors in the environment, but collecting and then analysing the large amounts of data captured. In many cases, specialized tools or expertise is required to synthesize and interpret the information to identify false alarms, attacks, or network events and to implement strategies to eliminate or minimize such events. Some organizations choose to outsource this activity to others who have more expertise in performing these services, such as managed security service providers.

7.3.2.7 Security-related information dissemination

This service provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include:

- reporting guidelines and contact information for the ISIRT;

- archives of alerts, warnings, and other announcements;
- documentation about current best practices;
- general computer security guidance;
- policies, procedures, and checklists;
- patch development and distribution information;
- current statistics and trends in incident reporting;
- other information that can improve overall security practices.

This information can be developed and published by the ISIRT or by another part of the organization (IT, human resources, or media relations), and can include information from external resources such as other ISIRTs, vendors, and security experts.

7.3.3 Security quality management services

Services that fall into this category are not unique to incident handling or ISIRTs in particular. They are well-known, established services designed to improve the overall security of an organization. By leveraging the experiences gained in providing the reactive and proactive services described above, an ISIRT can bring unique perspectives to these quality management services that might not otherwise be available. These services are designed to incorporate feedback and lessons learned based on knowledge gained by responding to incidents, vulnerabilities, and attacks. Feeding such experiences into the established traditional services (described below) as part of a security quality management process can improve the long-term security efforts in telecommunications organizations.

Depending on organizational structures and responsibilities, an ISIRT may provide these services or participate as part of a larger organizational team effort.

The following descriptions explain how ISIRT expertise can benefit each of these security quality management services.

7.3.3.1 Risk analysis

ISIRTs may be able to add value to risk analysis and assessments. This can improve the organization's ability to assess real threats, provide realistic qualitative and quantitative assessments of the risks to information assets, and evaluate protection and response strategies. ISIRTs performing this service would conduct or assist with information security risk analysis activities for new systems and business processes or evaluate threats and attacks against constituent assets and systems.

7.3.3.2 Business continuity and disaster recovery planning

Based on past occurrences and future predictions of emerging incident or security trends, more and more incidents have the potential to result in serious degradation of business operations. Therefore, planning efforts should consider ISIRT experience in determining how best to respond to such incidents to ensure the continuity of business operations. ISIRTs performing this service are involved in business continuity and disaster recovery planning for events related to computer security threats and attacks.

7.3.3.3 Security consulting

ISIRTs can be used to provide advice and guidance on the best security practices to implement for constituents' business operations. An ISIRT providing this service is involved in preparing recommendations or identifying requirements for purchasing, installing, or securing new systems, network devices, software applications, or organization-wide business processes. This service includes providing guidance and assistance in developing organizational or constituency security policies. It can also involve providing testimony or advice to legislative or other government bodies.

7.3.3.4 Awareness building

ISIRTs may be able to identify where constituents require more information and guidance to better conform to accepted security practices and organizational security policies. This can reduce the occurrence of successful attacks and increase the probability that constituents will detect and report attacks, thereby decreasing recovery times and eliminating or minimizing losses. ISIRTs performing this service seek opportunities to increase security awareness through developing articles, posters, newsletters, web sites, or other informational resources that explain security best practices and provide advice on precautions to take. Activities may also include scheduling meetings and seminars to keep constituents up to date with ongoing security procedures and potential threats to organizational systems.

7.3.3.5 Education/training

This service involves providing information to constituents about computer security issues through seminars, workshops, courses, and tutorials. Topics might include incident reporting guidelines, appropriate response methods, incident response tools, incident prevention methods, and other information necessary to protect, detect, report, and respond to computer security incidents.

7.3.3.6 Product evaluation or certification

For this service, the ISIRT may conduct product evaluations on tools, applications, or other services to ensure the security of the products and their conformance to acceptable ISIRT or organizational security practices. Tools and applications reviewed can be open source or commercial products. This service can be provided as an evaluation or through a certification program, depending on the standards that are applied by the organization or by the ISIRT.

As a summary of the list of services described in the above clauses, whatever services an ISIRT chooses to offer, the parent organization has to ensure that the team has the necessary resources (people, technical expertise, equipment, and infrastructure) to provide a valued service to their constituents, or the ISIRT will not be successful and their constituents will not report incidents to them.

Appendix I

An example of security incident severity rating

(This appendix does not form an integral part of this Recommendation)

The following security incident severity rating is derived from the DHS's [b-US, DHS] rating, which specifies the five levels of severity. It can be modified to any levels appropriate to a specific telecommunications organization. Each level represents an increasing risk of security incidents. Beneath each threat condition of security incidents are some suggested protective measures, recognizing that ISIRTs are responsible for developing and implementing appropriate protective measures:

Low condition

This condition is declared when there is a low risk of security attacks. ISIRTs should consider the following general measures in addition to the organization-specific protective measures:

- refining and exercising as appropriate pre-planned protective measures;
- ensuring personnel receive proper training on protective measures; and
- institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to security attacks, and all reasonable measures are taken to mitigate these vulnerabilities.

Guarded condition

This condition is declared when there is a general risk of security attacks. In addition to the protective measures taken in the previous threat condition, ISIRTs should consider the following general measures in addition to the organization-specific protective measures:

- checking communications with designated emergency response or command locations;
- reviewing and updating emergency response procedures; and
- providing the public with any information that would strengthen its ability to act appropriately.

Elevated condition

An elevated condition is declared when there is a significant risk of security attacks. In addition to the protective measures taken in the previous threat conditions, ISIRTs should consider the following general measures in addition to the organization-specific protective measures:

- increasing surveillance of critical locations;
- coordinating emergency plans as appropriate with nearby jurisdictions;
- assessing whether the precise characteristics of the threat require the further refinement of preplanned protective measures; and
- implementing, as appropriate, contingency and emergency response plans.

High condition

A high condition is declared when there is a high risk of security attacks. In addition to the protective measures taken in the previous threat conditions, ISIRTs should consider the following general measures in addition to the organization-specific protective measures:

- coordinating necessary security efforts with national ISIRTs and law enforcement agencies;
- preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and

- restricting threatened facility access to essential personnel only.

Severe condition

A severe condition reflects a severe risk of security attacks. Under most circumstances, the protective measures for a severe condition are not intended to be sustained for substantial periods of time. In addition to the protective measures in the previous threat conditions, ISIRTs also should consider the following general measures in addition to the organization-specific protective measures:

- increasing or redirecting personnel to address critical emergency needs;
- assigning emergency response personnel and pre-positioning and mobilizing organization-wide ISIRT or crisis management team; and
- closing public and national infrastructure facilities.

Appendix II

An example of security incident report

(This appendix does not form an integral part of this Recommendation)

Instructions for completing the report

The purpose of these forms – the initial and full security incident report forms – is to provide information about a security incident, which may be either an actual or a suspected incident, to the appropriate people.

If you suspect that a security incident 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 initial incident report (see the first part of this appendix) in accordance with the procedures described in the organizations security incident management scheme.

The information you provide will be used to initiate appropriate assessment, which will determine whether the incident is real, 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 or ISIRT member reviewing already completed/partially-completed forms, then you will be completing the full incident report form.

Please observe the following guidelines when completing the forms:

- if it is possible, the form should be completed and submitted electronically;
- 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.

Initial Security incident report

Date of incident:
Incident number: **(If applicable) related incident identity numbers**:

REPORTING PERSON DETAILS

Name **Address**
Organization
Telephone **Email**

SECURITY INCIDENT DESCRIPTION

Description of the incident:

- What occurred
- How it occurred
- Why it occurred
- Components affected
- Adverse business impacts
- Any vulnerabilities identified

SECURITY INCIDENT DETAILS

Date and time the incident occurred
Date and time the incident was discovered
Date and time the incident was reported
Is the incident over? ***(tick as appropriate)*** **YES** ☐ **NO** ☐

If yes, specify how long the incident has lasted in days/hours/minutes

(Incident numbers should be allocated by the organization's ISIRT Manager.)

'Full' security incident report

Date of incident
Incident number: **(If applicable) related incident identity numbers**:

OPERATIONS SUPPORT GROUP MEMBER DETAILS
Name **Address**
Telephone **Email**

ISIRT MEMBER DETAILS
Name **Address**
Telephone **Email**

SECURITY INCIDENT DESCRIPTION
Further description of the incident:

- What occurred
- How it occurred
- Why it occurred
- Components affected
- Adverse business impacts
- Any vulnerabilities identified

SECURITY INCIDENT DETAILS
Date and time the incident occurred
Date and time the incident was discovered
Date and time the incident was reported
Is the incident over? ***(tick as appropriate)*** **YES** ☐ **NO** ☐

If yes, specify how long the incident has lasted in days/hours/minutes

(Incident numbers should be allocated by the organization's ISIRT Manager.)

TYPE OF SECURITY INCIDENT
(Tick one, then complete related section below)

Actual ☐ **Attempted** ☐ **Suspected** ☐

(One of) **Deliberate** *(indicate threat types involved)*

Theft (TH)	☐	**Hacking/Logical infiltration (HA)**	☐
Fraud (FR)	☐	**Misuse of resources (MI)**	☐
Sabotage/Physical damage (SA)	☐	**Other (OD)**	☐
Malicious code (VI) *Specify:*			

(One of) **Accidental** *(indicate threat types involved)*

Hardware failure (HF)	☐	**Other natural events (NE)**	☐
Software failure (SF) *Specify:*			
Communication failure (CF)	☐	**Loss of essential services (LE)**	☐
Fire (FI)/Staff shortage (SS)	☐		
Flood (FL)	☐	**Other (OA)** *Specify:*	

(One of) **Error** *(indicate threat types involved)*

Operations error (OE)	☐	**User error (UE)**	☐
Hardware maintenance error (HE)	☐	**Design error (DE)**	☐
Software maintenance error (SE)	☐	**Other (including genuine mistake) (OA)** *Specify:*	☐

Not known *(If not yet established whether incident was deliberate, accidental or error, tick here and if possible indicate the threat types involved using the above threat type abbreviations)*
Specify:

ASSETS AFFECTED

Assets affected (if any) *(Provide descriptions of the assets affected by or related to the incident, including serial, license and version numbers where relevant.)*

Information/Data ----------

Hardware ----------

Software ----------

Communications ----------

Documentation ----------

ADVERSE BUSINESS IMPACT/EFFECT OF INCIDENT

For each of the following indicate if relevant in the tick box, then against 'value' record the level(s) of adverse business impact , covering all parties affected by the incident, on a scale of 1 to 10 using the guidelines for the categories of: financial loss/Disruption to business operations (FD), commercial and economic interests (CE), personal information (PI), legal and regulatory obligations (LR), management and business operations (MO), and loss of goodwill (LG). Record the code letters for the applicable guidelines against 'Guideline', and if actual costs are known, enter these against 'cost'.

		VALUE	GUIDELINE(S)	COST
Breach of confidentiality ***(i.e. unauthorized disclosure)***	☐			
Breach of integrity ***(i.e. unauthorized modification)***	☐			
Breach of availability ***(i.e. unavailability)***	☐			
Breach of non-repudiation	☐			
Destruction	☐			

TOTAL RECOVERY COSTS FROM INCIDENT

(Where possible, the actual total costs of recovery for the incident as a whole should be shown, against 'value' using the 1 to 10 scale and against 'cost' in actuals.)	VALUE	GUIDELINES	COST

INCIDENT RESOLUTION

Incident investigation commenced date ----------

Incident investigator(s) names(s) ----------

Incident end date ----------

Impact end date ----------

Incident investigation completion date ----------

Reference and location of investigation report ----------

PERSON(S)/PERPETRATOR(S) INVOLVED
(One of)

Person (PE) ☐

Organized group (GR) ☐

Legally established organization/institution (OI) ☐

Accident (AC) ☐

No perpetrator (NP) ☐
e.g., natural elements, equipment failure, human error.

DESCRIPTION OF PERPETRATOR

ACTUAL OR PERCEIVED MOTIVATION

(One of) **Criminal/Financial gain (GC)** ☐

Political/Terrorism (PT) ☐

Pastime/Hacking (PH) ☐

Revenge (RE) ☐

Other (OM)
Specify:

ACTIONS TAKEN TO RESOLVE INCIDENT

(e.g., 'no action', 'in-house action', 'internal Investigation', 'external' investigation by ....)

ACTIONS PLANNED TO RESOLVE INCIDENT

(e.g., see above examples)

ACTIONS OUTSTANDING
(e.g., investigation is still required by other personnel)

CONCLUSION

(Tick to indicate that the incident is considered major or minor, and include a short narrative to justify the conclusion) **Major** ☐ **Minor** ☐

(indicate any other conclusions) ----------

INDIVIDUALS/ENTITIES NOTIFIED

(This detail is to be completed by the relevant person with security responsibilities, stating the actions required. If relevant, this may be adjusted by the organization's Information Security Manager)

Information security manager	☐	**ISIRT manager**	☐
Site manager (state which site)	☐	**Information systems manager**	☐
Report originator	☐	**Report originator's manager**	☐
Police	☐	**Other** *(e.g., help desk, human resources, management, internal audit, regulatory body, external CERT) specify:*	☐

INVOLVED INDIVIDUALS

ORIGINATOR	REVIEWER	REVIEWER
Signature	**Signature**	**Signature**
Name	**Name**	**Name**
Role	**Role**	**Role**
Date	**Date**	**Date**

Bibliography

[b-ITU-T X.1055] Recommendation ITU-T X.1055 (2008), *Risk management and risk profile guidelines for telecommunication organizations*.

[b-ISO/IEC 27002] ISO/IEC 27002 (2005), *Information Technology – Security Techniques – Code of practice for information security management.*
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297>

[b-ISO/IEC 18043] ISO/IEC 18043 (2006), *Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35394>

[b-NIST SP 800-61] NIST SP 800-61 (2004), *Computer security incident handling guide*.
<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

[b-CMU/SEI-TR-015] CMU/SEI-TR-015 (2004), *Defining incident management processes for CSIRTs*.
<http://www.sei.cmu.edu/publications/documents/04.reports/04tr015.html>

[b-CMU/SEI-HB-002] CMU/SEI-HB-002 (2003), *Handbook for computer security incident response teams (CSIRTs)*.
<http://www.sei.cmu.edu/publications/documents/03.reports/03hb002.html>

[b-CMU/SEI-TR-008] CMU/SEI-TR-008 (2007), *Incident management capability metrics*.
<http://www.sei.cmu.edu/publications/documents/07.reports/07tr008.html>

[b-US, DHS] US, *Department of Homeland Security, Security Severity Rating*.
<http://www.dhs.gov/xlibrary/assets/DHS_Daily_Report_2009-06-10.pdf>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009