

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/>.

© ITU 2009

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Definitions	1
3.1	Terms and definitions for security incidents in general	1
3.2	Terms and definitions for telecommunications security incidents	2
4	Abbreviations.....	2
5	Concepts and issues of security incident management.....	3
5.1	Concepts of security incident management	3
5.2	Characteristics of telecommunications security incidents.....	6
5.3	Key issues of security incident management.....	6
6	Security incident management processes	9
6.1	Overview of security incident management processes.....	9
6.2	Relationship between security incident management and security management.....	12
7	Security incident management services.....	14
7.1	Overview	14
7.2	Service categories.....	14
7.3	Service descriptions.....	15
	Appendix I – An example of security incident severity rating	22
	Appendix II – An example of security incident report	24
	Bibliography.....	31

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

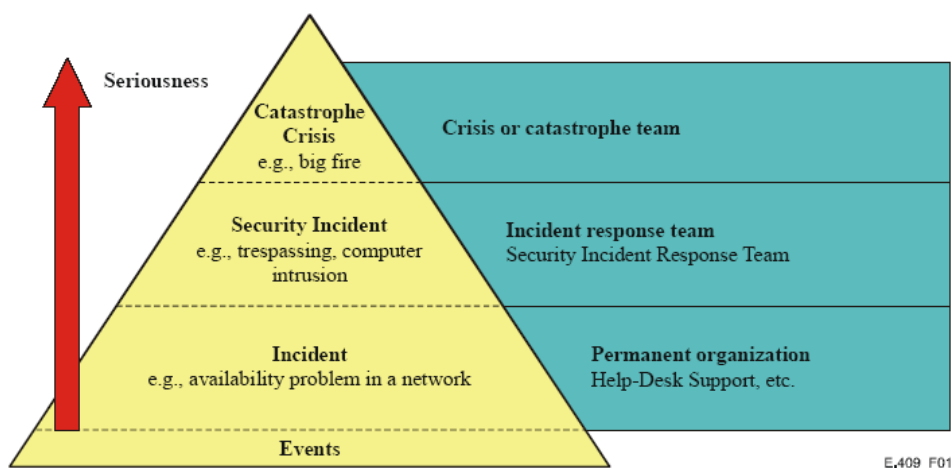
5 Concepts and issues of security incident management

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.



E.409_F01

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.

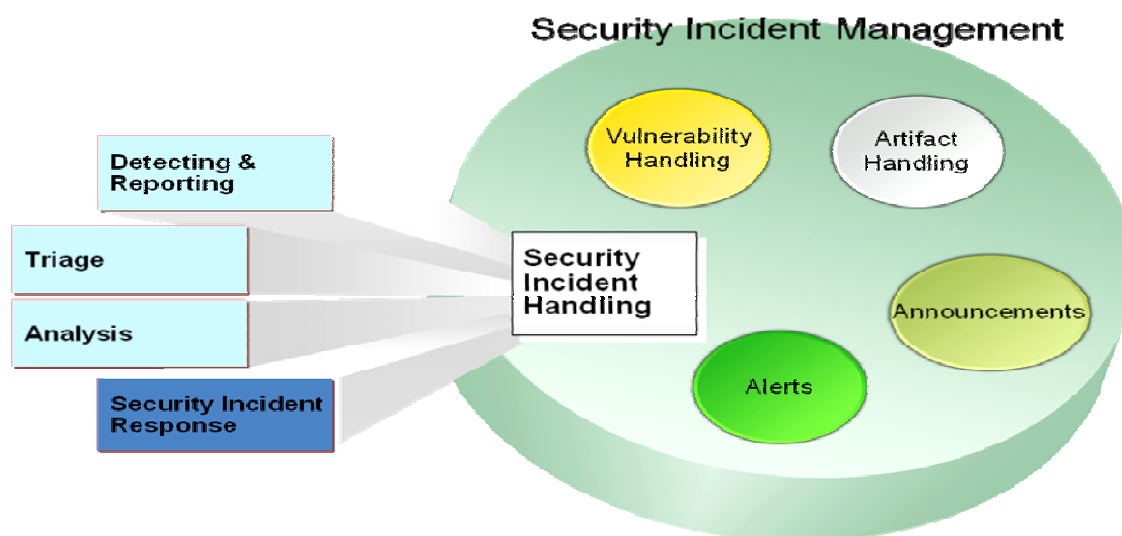


Figure 2 – Relationships among incident management, incident handling, and incident response (Modified from [b-CMU/SEI-TR-015])

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.