INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

E.409

(05/2004)

SERIES E: OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS

Network management – International network management

Incident organization and security incident handling: Guidelines for telecommunication organizations

ITU-T Recommendation E.409

ITU-T E-SERIES RECOMMENDATIONS

OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS

INTERNATIONAL OPERATION	
Definitions	E.100–E.103
General provisions concerning Administrations	E.104–E.119
General provisions concerning users	E.120–E.139
Operation of international telephone services	E.140–E.159
Numbering plan of the international telephone service	E.160–E.169
International routing plan	E.170–E.179
Tones in national signalling systems	E.180–E.189
Numbering plan of the international telephone service	E.190–E.199
Maritime mobile service and public land mobile service	E.200–E.229
OPERATIONAL PROVISIONS RELATING TO CHARGING AND ACCOUNTING IN THE INTERNATIONAL TELEPHONE SERVICE	
Charging in the international telephone service	E.230–E.249
Measuring and recording call durations for accounting purposes	E.260–E.269
UTILIZATION OF THE INTERNATIONAL TELEPHONE NETWORK FOR NON-TELEPHONY APPLICATIONS	
General	E.300–E.319
Phototelegraphy	E.320–E.329
ISDN PROVISIONS CONCERNING USERS	E.330–E.349
INTERNATIONAL ROUTING PLAN	E.350–E.399
NETWORK MANAGEMENT	
International service statistics	E.400–E.404
International network management	**E.405–E.419**
Checking the quality of the international telephone service	E.420–E.489
TRAFFIC ENGINEERING	
Measurement and recording of traffic	E.490–E.505
Forecasting of traffic	E.506–E.509
Determination of the number of circuits in manual operation	E.510–E.519
Determination of the number of circuits in automatic and semi-automatic operation	E.520–E.539
Grade of service	E.540–E.599
Definitions	E.600–E.649
Traffic engineering for IP-networks	E.650–E.699
ISDN traffic engineering	E.700–E.749
Mobile network traffic engineering	E.750–E.799
QUALITY OF TELECOMMUNICATION SERVICES: CONCEPTS, MODELS, OBJECTIVES AND DEPENDABILITY PLANNING	
Terms and definitions related to the quality of telecommunication services	E.800–E.809
Models for telecommunication services	E.810–E.844
Objectives for quality of service and related concepts of telecommunication services	E.845–E.859
Use of quality of service objectives for planning of telecommunication networks	E.860–E.879
Field data collection and evaluation on the performance of equipment, networks and services	E.880–E.899

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

ITU-T Recommendation E.409

Incident organization and security incident handling: Guidelines for telecommunication organizations

Summary

The purpose of this Recommendation is to analyse, structure and suggest a method for establishing an incident management organization within a telecommunication organization involved in the provision of international telecommunications, where the flow and structure of an incident are focused. The flow and the handling are useful in determining whether an event is to be classified as an event, an incident, a security incident or a crisis. The flow also covers the critical first decisions that have to be made.

Computer crime follows in the wake of the heavily increased use of computers in international telecommunications. Over the last years, computer crime has literally exploded, as confirmed by several international and national surveys. In the majority of countries, there are no exact figures on the number of computer break-ins or security incidents, especially those related to international telecommunications.

Most telecommunication organizations or companies do not have any specialized organization for handling Information and Communication Networks (ICN) security incidents (although they may have a general crisis team for handling crises of any type). When an ICN security incident occurs it is handled ad hoc, i.e., the person who detects an ICN security incident takes the responsibility to handle it as best as (s)he can. In some organizations the tendency is to forget and cover up ICN security incidents as they may affect production, availability and revenues.

Often, when an ICN security incident is detected, the person who detects it does not know who to report it to. This may result in the system or network's administrator deploying a workaround or quick fix just to get rid of the problem. They do not have the delegated authority, time or expertise to correct the system so that the ICN security incident does not recur. These are the main reasons why it is better to have a trained unit or group that can handle security incidents in a prompt and correct manner. Furthermore, many of the issues may be in areas as diverse as media relations, legal, law enforcement, market share, or financial.

When reporting or handling an incident, the use of different taxonomies leads to misunderstanding. This may, in turn, result in an ICN security incident getting neither the proper attention, nor the prompt handling, that is needed in order to stop, contain and prevent the incident from recurring. This may lead to serious consequences for the affected organization (victim).

To be able to succeed in incident handling and incident reporting, it is necessary to have an understanding of how incidents are detected, handled and resolved. By establishing a general structure for incidents (i.e., physical, administrative or organizational, and logical incidents) it is possible to obtain a general picture of the structure and flow of an incident. A uniform terminology is the base for a common understanding of words and terms.

Source

ITU-T Recommendation E.409 was approved on 28 May 2004 by ITU-T Study Group 2 (2001-2004) under the WTSA Resolution 1.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation E.409

Incident organization and security incident handling: Guidelines for telecommunication organizations

1 Introduction

1.1 Scope

The purpose of this Recommendation is to analyse, structure and suggest a method for establishing an incident management organization, within a telecommunication organization involved in the provision of international telecommunications, where the flow and structure of an incident are focused. The flow and the handling are useful in determining whether an event is to be classified as an event, an incident, a security incident or a crisis. The flow also covers the critical first decisions that have to be made.

This Recommendation provides an overview and framework that gives guidance for planning incident organization and security incident handling.

This Recommendation is generic in nature and does not identify or address requirements for specific networks.

This Recommendation is intended to facilitate international developments regarding telecommunication network security. Such developments would be facilitated if the requirements of this Recommendation could also be applied to the national Information and Communication Networks (ICN).

To be able to succeed in incident handling and incident reporting, an understanding of how incidents are detected, handled and resolved is necessary. By establishing a general structure for incidents (i.e., physical, administrative or organizational, and logical incidents) it is possible to obtain a general picture of the structure and flow of an incident. A uniform terminology is the base for a common understanding of words and terms.

When reporting or handling an incident, the use of different taxonomies leads to misunderstanding. This may, in turn, result in an ICN security incident getting neither the proper attention, nor the prompt handling, that is needed in order to stop, contain and prevent the incident from recurring. This may lead to serious consequences for the affected organization (victim).

This Recommendation describes the flow and the handling of an incident.

The definition of an incident varies among professions, organizations and people.

According to the general meaning of an incident, it may be anything from an erroneous backup, disruption of services, attack by a virus, to intrusion into computer systems.

1.2 Definitions

ISO 17799 mentions incident, security incident and information security incident.

Only the term "security incident" is defined as a "security breach, threat, weakness and malfunction that might have an impact on the security of organizational assets". Nowhere are the terms "incident" and "information security incident" explained. In this Recommendation, it is assumed that an incident is less severe than a security incident and that an information security incident is a particular type of security incident.

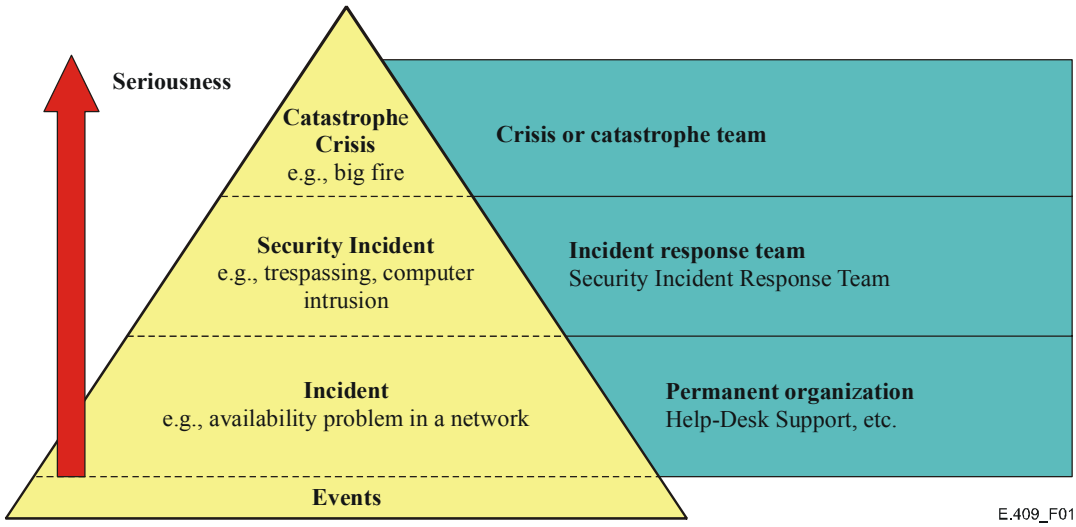

Figure 1/E.409 – The pyramid of events

Figure 1 shows the pyramid of events. At the bottom we find the event, followed by incident, security incident and at the top crisis and catastrophe. The closer to the top an event is, the more serious. In order to make use of a common and sound vocabulary regarding incident handling within the ICN area, this Recommendation defines the following terms:

1.2.1 **event**: An event is an observable occurrence which is not possible to (completely) predict or control.

1.2.2 **incident**: An event that might have led to an occurrence or an episode which is not serious.

1.2.3 **security incident**: A security incident is any adverse event whereby some aspect of security could be threatened.

1.2.4 **Information and Communication Networks (ICN) security incident**: Any real or suspected adverse event in relation to the security of ICN. This includes:

- Intrusion into ICN computer systems via the network;
- Occurrence of computer viruses;
- Probes for vulnerabilities via the network into a range of computer systems;
- PABX call leak-through;
- Any other undesired events arising from unauthorized internal or external actions.

1.2.5 **crisis**: 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 Continuency Plan (BCP) normally exists as well as a crisis management team to handle the situation.

1.3 Rationale

It is recommended that telecommunication organizations creating (computer security) incident response teams, as the first step, declare their use of taxonomy in order to avoid misunderstandings. Collaboration is much easier when using the same "language".

It is recommended that organizations use the term Incident and ICN Security Incident and define their own subdivisions according to the severity of the latter. In essence, an ICN security incident is any undesired, unauthorized event. This means that an ICN security incident includes computer intrusion, denial of service attack or a virus depending on the motivation, experiences and available

knowledgeable resources in the organization. In organizations that have created an effective virus fighting team, viruses may not be considered as ICN security incidents but rather as incidents.

An example, or template, of such a subdivision could be as follows:

–	Incidents	• Violating Internet Netiquette (Spamming, Abusive Content, etc.)
		• Violating security policies
		• Individual viruses
–	ICN Security Incidents	• Scans and probes
		• Computer intrusions
		• Computer sabotage and damage (availability attacks as bombing, DoS-attacks)
		• Malicious software (viruses, Trojans, worms, etc.)
		• Information theft and espionage
		• Impersonation

By using the same granularity and preciseness in terminology it is possible to gain experience in:

– guidance of the severity and scope;
– indication of the need for speed;
– effects of likely countermeasures;
– possible costs involved.

2 System description

2.1 Structure and flow

By establishing a general structure for incidents (i.e., physical, administrative or organizational, and logical incidents) a general picture of the structure and flow of an incident is obtained.

2.1.1 Protection principles

The protection mechanisms an organization implements should reflect the requirements of its ICN security policy or the equivalent, including legal aspects. The incident-handling-organization and its tasks shall support these requirements.

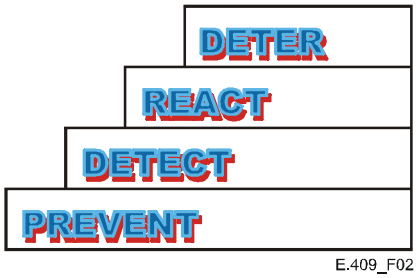

Figure 2/E.409 – Protection principles

Figure 2 shows that it is necessary to start at 'point zero'. An organization should implement all the steps involved in protective security mechanisms in order to obtain coherent protection.

The *preventive* protection mechanisms come first. When adequate preventive protection mechanisms are in place, implemented via physical or logical protection, it is then possible to identify and activate the *detecting* protection mechanisms.

The *detection* protection mechanisms could, in the simplest form be the checking of log files, logical or physical alarms, i.e., burglar alarms, fire alarms or other surveillance functions. One form of detection mechanism is the intrusion detection system (IDS).

Once an incident is detected, action should be taken. Such action usually comprises the following tasks:

- Stop an ongoing incident;
- Identify scope/scale of incident;
- Limit the damage;
- Take measures in order to investigate the course of events;
- Prevent the incident from recurring.

Actions necessary to stop and limit the incident (contain it) and prevent re-occurrence are performed by the permanent organization, i.e., helpdesk or support unit. If the incident escalates into a crisis, a specially trained crisis group performs the actions. Regarding investigation and analysis of the incident, it is recommended that the incident response team do this.

After all these three protection mechanisms are in place and functioning, there is a deterrent effect, i.e., the perpetrator knows there are functioning protection mechanisms and that detection and reaction to incidents are prompt. The deterrent effect can be increased by reacting to all incidents and by reporting any illegal incidents to law enforcement authorities.

2.1.2 Incident handling structure

In order to understand the role of incident handling and incident organization within the organization, it is recommended to use an incident handling structure. This structure shows an overview of the incident flow, describing the occurrence of an incident, actions/measures to contain the incident, recovery and follow-up.

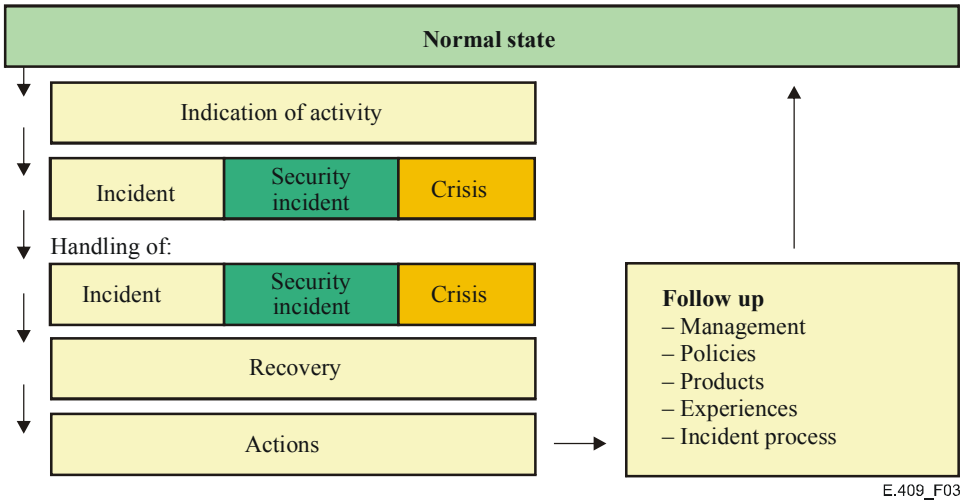

Figure 3/E.409 – The incident handling structure

The structure (see Figure 3) shows that all events, incidents, security incidents and crises arise from a normal state, i.e., normal functioning business.

When an indication of activity is detected that could lead to an incident or security incident, it is handled by the permanent organization as described below. The time between indication and occurred incident, or security incident, can be very short. The type of indication for an incident may be a virus on a single workstation, error in the network, etc. Regarding security incidents, indicators can be found in log files, firewall filters, etc. Indications could also be triggered alarms, indications from surveillance cameras, etc.

When an *incident or security incident occurs* it is assessed regarding its scope and consequences. An incident can escalate into a security incident or crisis. The permanent organization handles the incidents and the incident response team (CSIRT, Computer Incident Response Team) handles the security incidents. A specially formed crisis management group handles crises.

A CSIRT may constitute the entire security team of a telecommunication organization or may be totally distinct from such an organization's security team. Alternatively, although a telecommunication organization may not have a distinct CSIRT, this role may in fact be served implicitly by the organization's security team.

The *actions/measures* taken follow an established routine or a standard procedure. In case of severe security incidents or crises, the measures will be contingent with the scope and consequences of the incident. Measures are carried out by the security team or the incident response team.

During *recovery,* measures are taken in order to return to normal business. Depending on the occurred event, this could mean restarting computer or network systems, re-installation of programs, restoring of backups. Such measures may include resetting alarms, reconstruction of damaged property, etc.

While this work is being done, an assessment on whether the event should have a legal aftermath is also carried out. This may require a more thorough investigation and securing evidence, etc.

It is important to *follow-up* the work that occurred while handling incidents and security incidents, as well as crises. The purpose of the follow-up is to improve standard operations and procedures in order to prevent re-occurrence and minimize any consequences and costs.

The follow-up report can result in changes to incident processes, products and policies. The management is given a summary of the occurred incidents and security incidents, their scope, consequences and costs. This summary should also cover the efficiency of the incident-handling organization. A Lessons Learnt/Experiences file should be established to be able to compare different incidents in order to find more effective methods and practices in detecting and handling incidents and security incidents.

2.2 Incident flow

The flow of an incident or security incident is described below. This approach is founded on experiences and should be applicable to all telecommunication organizations and all types of incidents, as the flow is simple and general. The handling of an incident (incident flow) can be compared with actions taken in the case of an accident, a fire, etc. The starting point, or parameter, is that an event occurs which has implications for the organization.

2.2.1 The phases of crisis handling

In crisis management, a crisis is said to pass through three phases:

- **The pre-phase** occurs when there are indications that something might go wrong. In this phase, an organization should be on alert and raise its preparedness level.
- **The emergency phase** is when the crisis occurs. An emergency is always unexpected and ill-timed, and often occurs during non-business hours or weekends. As every crisis is different, it is important that the handling not be performed according to some standard routine that states every action to be taken regarding a defined threat. It is important to

know that crisis management is a matter of situational leadership and it is necessary to be able to improvise.

- **After phase**, or aftermath, is the phase that is crucial if the organization is going to resolve the crisis and survive. This phase consists of several other sub-phases such as psychological first aid, actions to get back to business, lessons learnt, etc.

2.2.2 The phases of incident handling

Incident handling is based on the emergency phase of crisis management. This phase has been supplemented with two additional phases, the *handling phase* and the *follow-up phase* (see Figure 4). These are described below.

The reason for not using the same phases as crisis management is that the pre-phase in crisis management covers the phases in incident handling, as a whole. Under normal circumstances, the handling of an incident does not reach crisis management level. If an incident should be transferred to crisis management, it means the incident has escalated into a crisis.

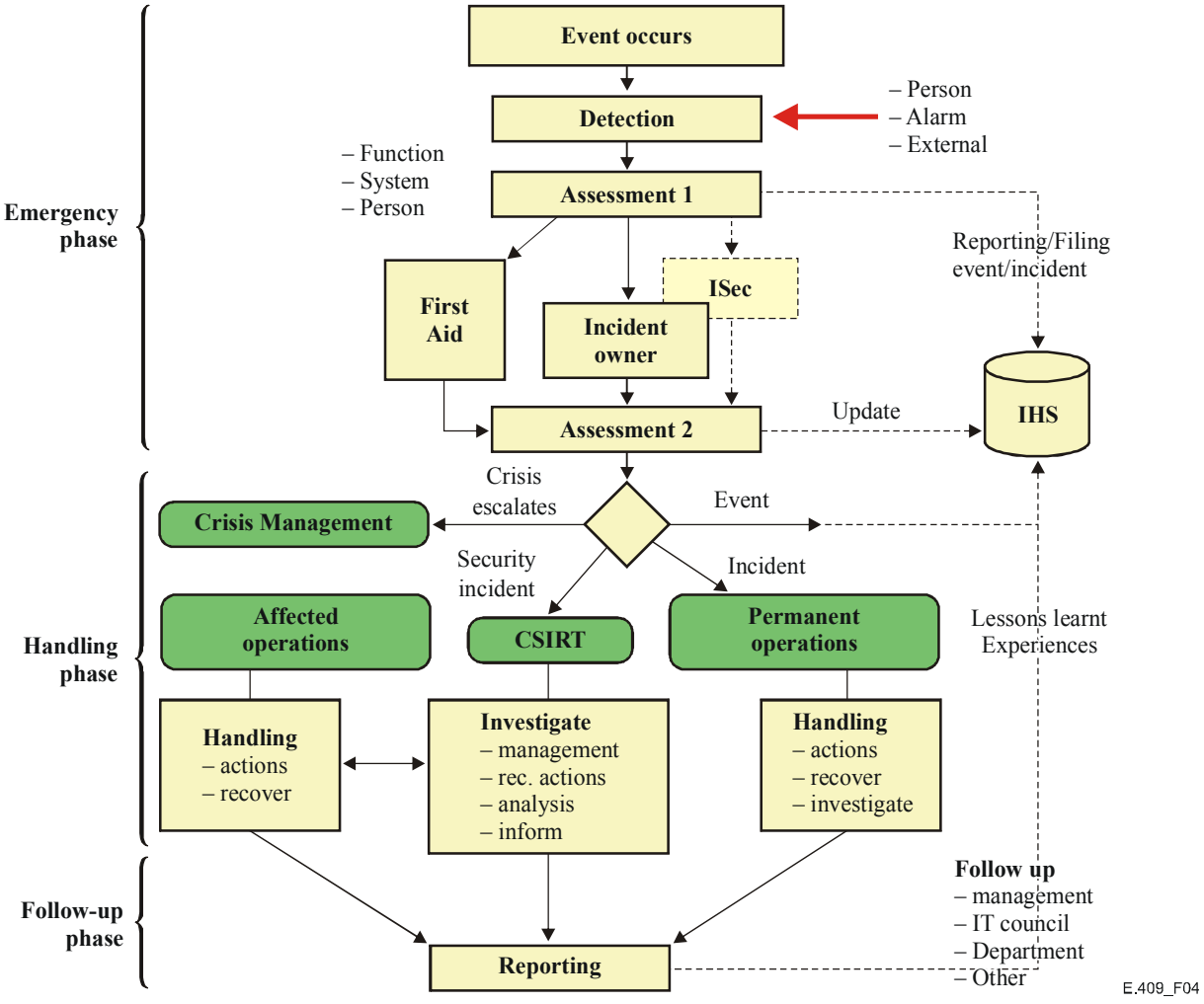

Figure 4/E.409 – Incident flow

The flow of an incident is presented below in the different phases.

2.2.2.1 Emergency phase

As shown in Figure 4, the emergency phase is the first one. This phase may be compared with an accident situation, i.e., during a traffic accident the first actions taken are often critical in terms of the final outcome. These actions have the most important consequences in terms of the outcome. The stages in the emergency phase are described in order (see Figure 5).

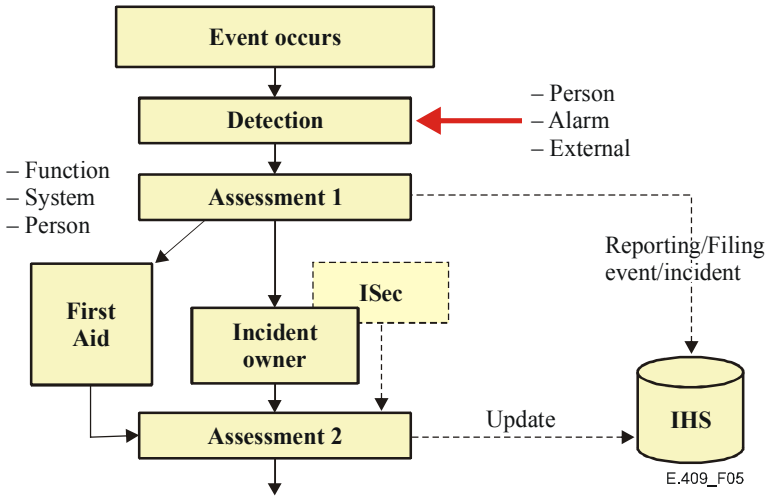

Figure 5/E.409 – The emergency phase

2.2.2.2 Detection

An event may be detected visually by an individual, i.e., by tracking an error message, reading a result file or by audit control. Visual detection might occur when the operator sees someone committing an intrusion or when someone detects a fire. An event could also be detected by a person who has a feeling that something is wrong, that something unusual is going on.

Logical alarms are situations that call for the attention of the end-user, operating personnel, security functions etc. A logical alarm could be an alarm triggered by the antiviral software, the audit subsystem or the firewall and intrusion detection system. An event could also trigger physical alarms such as fire alarms, burglar alarms, etc.

External detection occurs when someone not belonging to the organization detects the event. This could be, in the worst case, announced on the news, or a reporter who investigates sources, or contacts the organization to obtain a comment regarding an event the organization has not yet detected. It could also be the law enforcement authorities who notify the security department during the investigation of a crime, or a righteous citizen discovering an undesired feature of the telecommunication organization's website.

When an event is detected, an initial assessment of the situation must be made in order to confirm the category and seriousness. This is done by categorizing the events by type, i.e., is it an incident, a security incident, a crisis or just an event. After that, the scope and consequences have to be considered. Below is a simple classification, applied for ICN-security incidents only, to use when determining the seriousness of an incident or security incident.

This assessment can be made by the person who detects the event, who could also choose to report the detected event to a function, i.e., helpdesk, support or Information Security Department. When an event is reported to a function, it becomes the responsibility of that function. The functions that may receive a report of detection are also called Point-of-Contact (POC), and they are responsible for handling the situation. An alarm is normally automatically transferred to the responsible person, function or system. All reported events should be registered in an incident handling system (IHS).

A Point-of-Contact (POC) is a unit or a person to whom an event is reported. Sometimes, this is a unit or function such as the helpdesk, production control, Security or the Information Security Department (ISec). An event cannot be reported to the CSIRT as this is a virtual group that is formed at the time of a security incident. A security incident can be reported to the Information Security Department (ISec), which is responsible for the CSIRT, or any other POC where the correct assessment will be made and contact initiated with the responsible units.

• Class 4	Very serious	A security incident which has significant consequences for the organization, for example coordinated attacks, computer intrusions, theft of sensitive and confidential information, etc. A security incident which falls within this class requires significant countermeasures and results in significant damage.
• Class 3	Serious	A security incident which has consequences for the organization, for example computer sabotage, computer fraud, breach of integrity, misuse or exposure of corporate or customer information.
• Class 2	Less serious	A security incident, such as intrusion attempts, misuse of computing resources, etc. A security incident which falls within this class has less consequence, requires minor countermeasures and results in little damage.
• Class 1	No consequences	An incident which is handled by the permanent organization but may be escalated to a security incident, for example, scans, single viruses, abusive events, attacks directed to mail systems, etc. This class usually comprises incidents that affect the normal production. A security incident which falls into this class requires minor or no countermeasures and results in little or no damage.

An event is commonly reported to the helpdesk, especially when an end-user detects an event. End-users normally report all events and errors to the helpdesk. In other cases, the system administrator or operator may detect the event. The operational control centres for communications, system security and physical security might also detect the events as they receive alarms from logical and physical sensors or external sources.

All functions and units that might receive an alarm or indication of an event must be given instructions on how to act. This must be done to avoid events and alarms being neglected or incorrectly handled.

2.2.2.2.1 Assessment 1

This assessment is made by a person or function (POC) or system (IDS). In most cases, the assessment is made by the person receiving the alarm, or other information, about an event.

An event must be identified as belonging to one of five different categories:

- Crisis;
- Security incident;
- Incident;
- Event;
- False Alarm.

If an event cannot be categorized as above, it should be classified as an incident and handled by the permanent organization, i.e., helpdesk and support. Some events do not generate any actions as they are considered "user errors" or misinterpretations.

Moreover, the event must also be assessed in consideration of the effect it has on the organization or business. This "level of seriousness" is assessed according to the following four levels:

- Very serious consequences for the telecommunication organization;
- Serious consequences for the telecommunication organization;
- Some consequences for the telecommunication organization;
- No consequences for the telecommunication organization.

These assessments should be registered in the incident handling system (IHS).

In case of incidents, security incidents or crises, first aid must be given immediately. This includes the initial damage report, estimated consequences and an assessment as to whether or not there are any quick solutions that can be applied to limit the damage. This assessment is often performed by the person or function receiving the alarm or notification of the event.

Regarding incidents, the person or POC informs the affected departments and initiates measures. Taking into consideration the scope and consequences, this may also mean that experts are immediately involved. If it is a computer virus that has spread to one department only, the support function can handle this with standard operations.

At the same time, the helpdesk is *informed* regarding the event: what it is, which measures have been taken, and when the computer and network systems are back to normal. This is done to inform the people at the helpdesk, as they will be the ones to receive calls from end-users affected by the incident. They can inform the end-users that help is on the way. Another even more important reason is that if anyone else reports the same, or similar incident, the helpdesk knows who to inform about the new occurrence.

However, if a computer virus has spread, and is spreading to several departments, coordinated efforts must be undertaken to effectively limit the damage and eliminate the virus.

All *external inquiries* must be directed to the Information Security Department.

Before a decision is made regarding next steps or actions, the incident has to be handed over to the incident owner or the Information Security Department (ISec). The incident owner is the person who is responsible for the affected department, or the system owner of the system affected. The incident owner is the person who must assume responsibility for losses and costs.

If several departments are affected, the department with the biggest loss or costs is the incident owner. If the incident affects the infrastructure of the telecommunication organization, the corresponding department is responsible. If the incident owner cannot be determined, the Information Security Department (ISec) is considered the incident owner.

The incident owner has the authority over and responsibility for handling the incident.

2.2.2.2.2 Assessment 2

This assessment is made by the incident owner or the Information Security Department (ISec). The Information Security Department and CSIRT have expert knowledge in security and ICN security matters. They can be consulted for an assessment of the scope and consequences.

This assessment consists of a verification of the previous assessment regarding the classification of the incident (i.e., whether it is an event, incident, security incident or crisis). The incident owner decides if the incident has been correctly assessed or whether corrections need to be made. The incident owner also makes decisions regarding any further handling of the incident. This includes

the decision as to whether crisis management, CSIRT or the permanent organization should handle and investigate the incident.

The decision to inform support and the helpdesk is made by the incident owner. In some cases, it is better to postpone this decision until the incident leader and the incident response team are in place.

In cases where there is any doubt about whether the incident can be handled within the permanent organization, the contact person for CSIRT should be contacted. In case of a security incident, CSIRT must be contacted. Where appropriate, the Information Security Department can be contacted. During this work, the scope of the security incident will be made clear and a mutual assessment will be made as to whether crisis management should be called upon or not.

The record of the actual incident, registered in the incident handling system (IHS), is updated. Events without action should be registered as well. The purpose of registering all events is that an isolated event, or several events, may be related to other events, incidents or security incidents, although it is not evident at the time. If a security incident occurs, the connection between these events and the security incident may become clear.

After this phase, the security incident enters the handling phase.

2.2.2.2.3 Handling phase

During the handling phase, the actual handling of the event occurs. The event could be an incident, a security incident or a crisis. When entering this phase it earns "official" status and should be handled as follows.

During **crisis** or **escalation,** crisis management moves in and takes over the handling, according to established routines. The measures that are taken also follow established crisis routines and lead to the formation of the crisis management group. Crisis management, and the handling of a crisis are beyond the scope of this Recommendation.

An **incident** is handled by the permanent telecommunication organization, i.e., production control, support, security and surveillance, etc. An incident could consist of production errors and disturbances, visitors "on-the-loose", etc. The permanent organization handles the incidents by:

- Taking action to counteract the cause and effects of the incident and prevent it from recurring;
- Recovering in order to get back to business;
- Investigating what caused the incident and its consequences, and documenting performed actions.

It is suggested that production incidents be handled by the production support unit and the organization established for these events.

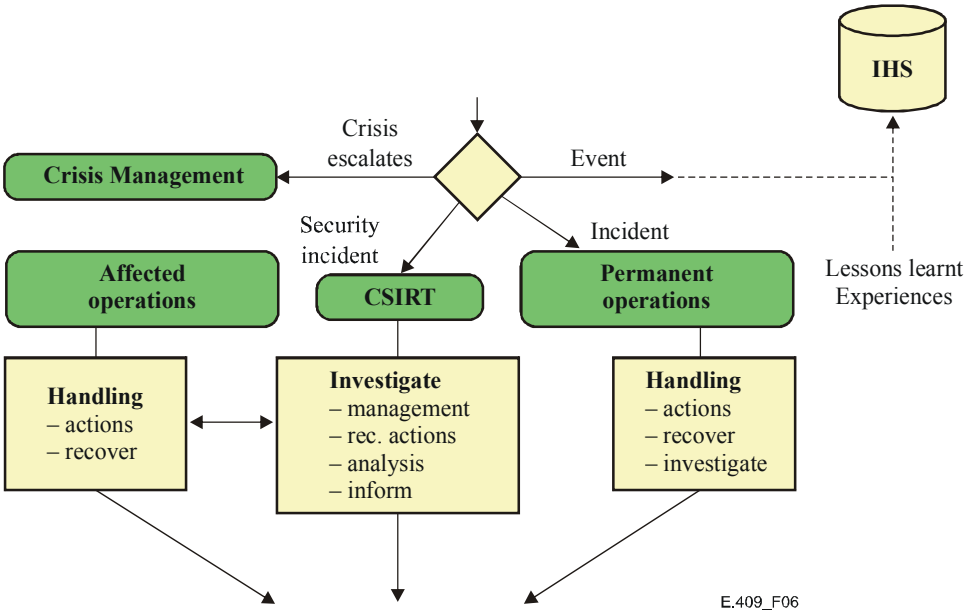

Figure 6/E.409 – The handling phase

When a **security incident** enters the handling phase, the handling is performed according to established routines.

The incident owner, in consultation with Information Security Department (ISec), initiates and builds the virtual and temporary incident response team, CSIRT. An incident leader is also selected. This may be any person from the affected support units, surveillance or Information Security Department (ISec). The incident response team, CSIRT, is formed with regard to the appropriate persons and skills.

CSIRT investigates the security incident, which means:

- Management and execution of the investigation work;
- Taking action to stop and limit the consequences of the security incident (containment). This is done together with the affected department. Normally, CSIRT acts like a support unit;
- Recover in order to get back to the business of telecommunications. This is done together with the affected department. Normally, CSIRT is a supporting unit;
- Analysis of the circumstances and the causes of the incident, its consequences and documentation of performed actions and costs;
- Information to involved parties, i.e., Information Security Department, helpdesk and support, etc.

These procedures may be far more detailed than the ones that are presented here, which can be used as a guideline.

The routine consists of five different steps:

1) Identification of incident type, scope and consequences;
2) Containment, i.e., stop the occurrence and limit the consequences of the security incident;
3) Eradication of the cause and prevention of re-occurrence;
4) Recovery to normal business;
5) Follow-up.

When CSIRT is formed, the "Identification" is a standard procedure in the briefing of the CSIRT members. They are also informed about the security incident, actual status, measures taken and precautions, etc.

2.2.2.2.4 Follow-up phase

In the follow-up phase, the crisis, security incident or incident has been resolved and the consequences are minimized. What remains is to assess the event and its handling, report to management, the Information Security Department, production controls etc.

The follow-up report should describe the detection of the incident, time lags between detection and (re)action, measures taken and their effectiveness and results. The report should also show shortcomings found in the original (ICN-) environment, deficiencies in handling and procedures. All this should be registered in a Lessons Learnt or Experiences file, which can be used to avoid making the same mistakes again. Both direct and indirect costs should be estimated.

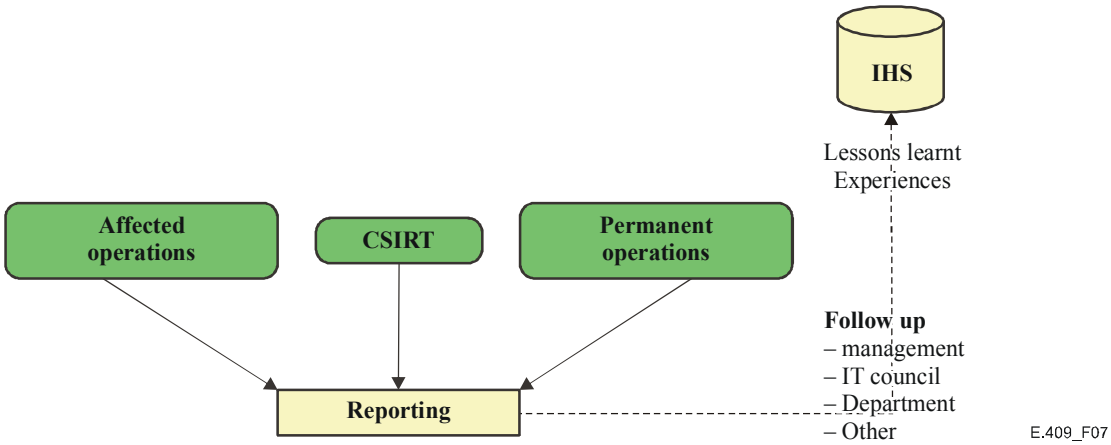

Figure 7/E.409 – Follow-up phase

During this phase the completion of the actual incident record is carried out in IHS. The Lessons Learnt or Experiences file should be established in order to overview and recall the experiences learnt during emergency, handling and follow-up phase.

3 Incident handling system

It is crucial to implement an incident handling system which keeps track of every detected and reported event, incident, security incident and crisis. By studying these files, it is possible to learn which types of events are more common, why they arise, how they are detected, their scope, consequences and costs. An important aspect is to register events that are not incidents, security incidents or crises. Although these events may not pose any threat when seen as isolated events, together they can tell us something about how incidents arise. Such events could reveal similarities to security incidents directed against the organization. Minor events which, seen individually, may look like an incorrect network request, may show a major scanning of the telecommunication organization's network, in particular, computer network and systems when viewed as a whole.

BIBLIOGRAPHY

- Excerpts from Master's Thesis in Incident Organization and Security Incident Handling, Jimmy Arvidsson, FIINA, 2001.
- CERT/CC (URL: http://www.cert.org) 2000-09-26.
- Federal Incident Response Capability (URL: http://www.fedcirc.llnl.gov) 2000-05-20.
- Internet Security Glossary; R. Shirey, GTE/BBN Technologies, May 2000.
- Informationssäkerhetshandbok, del 5 – Katastrofskydd för IT-verksamhet, v.2, Jan-Olof Andersson, JOA InfoSäk, 1999.
- Handbook for Computer Security Incident Response Teams (CSIRTs); Moira J. West-Brown, Dan Stikvoort, Klaus-Peter Kossakowski; Carnegie Mellons, Software Engineering Institute, 1998.
- Computer Security Incident Handling – Step by step, SANS Institute, NSWC, 1998.
- Intrusion Detection, Edward Amoroso, Intrusion.Net Books, 1998.
- Best Current Practice; Expectations for Computer Security Incident Response; N. Brownlee, The University of Auckland, E. Guttman, Sun Microsystems, June 1998.
- Computer Security Incident Handling Procedure, NSWC Dahlgren, October 1996.
- Computer Crime: A Crimefighter's Handbook, David Icove, Karl Seger and William – VonStorch, O'Reilly & Associates, 1995.
- An Analysis of Security Incidents On The Internet, 1989-1995, John Howard, CERT/CC (URL: http://www.cert.org/research/JHThesis/Start.html) 2000-05-20.
- Establishing a Computer Security Incident Response Capability (CSIRC), NIST, November 1991.
- "The Oxford Reference Dictionary"; Oxford University Press, 1986.
- A Common Language for Computer Security Incidents; John D. Howard and Thomas A. Longstaff; Sandia National Laboratories [Sandia Report: SAND98-8667].
- Intrusion Detection – Network Security Beyond The Firewall, Terry Escamilla.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
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	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
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 and open system communications
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, 2004