Computer Security Incident Response Planning at Nuclear Facilities

IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES AND RELATED PUBLICATIONS

IAEA guidance on nuclear security issues relating to the prevention and detection of, and response to, criminal or intentional unauthorized acts involving, or directed at, nuclear material, other radioactive material, associated facilities or associated activities is provided in the **IAEA Nuclear Security Series**. Publications in this series are consistent with, and complement, international nuclear security instruments, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

Publications in the IAEA Nuclear Security Series are issued in the following categories:

- **Nuclear Security Fundamentals** specify the objective of a State's nuclear security regime and the essential elements of such a regime. They provide the basis for the Nuclear Security Recommendations.

- **Nuclear Security Recommendations** set out measures that States should take to achieve and maintain an effective national nuclear security regime consistent with the Nuclear Security Fundamentals.

- **Implementing Guides** provide guidance on the means by which States could implement the measures set out in the Nuclear Security Recommendations. As such, they focus on how to meet the recommendations relating to broad areas of nuclear security.

- **Technical Guidance** provides guidance on specific technical subjects to supplement the guidance set out in the Implementing Guides. They focus on details of how to implement the necessary measures.

Other publications on nuclear security, which do not contain IAEA guidance, are issued outside the IAEA Nuclear Security Series.

RELATED PUBLICATIONS

The IAEA also establishes standards of safety for protection of health and minimization of danger to life and property, which are issued in the **IAEA Safety Standards Series**.

The IAEA provides for the application of guidance and standards and makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Emergency Preparedness and Response** publications, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety and security related publications.

The **IAEA Nuclear Energy Series** comprises informational publications to encourage and assist research on, and the development and practical application of, nuclear energy for peaceful purposes. It includes reports and guides on the status of and advances in technology, and on experience, good practices and practical examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

COMPUTER SECURITY INCIDENT RESPONSE PLANNING AT NUCLEAR FACILITIES

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D’IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE’S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency’s Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is “to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world’’.

COMPUTER SECURITY INCIDENT RESPONSE PLANNING AT NUCLEAR FACILITIES

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2016

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

For further information on this publication, please contact:

Information Management Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Email: Official.Mail@iaea.org

COMPUTER SECURITY INCIDENT RESPONSE PLANNING AT NUCLEAR FACILITIES
IAEA-TDL-005
ISBN 978-92-0-104416-7
© IAEA, 2016

Printed by the IAEA in Austria
June 2016

FOREWORD

The aim of nuclear security is to prevent, detect and respond to malicious acts that involve nuclear material, other radioactive material or associated facilities and activities. Computers, computing systems and digital components play an increasingly important role in the management of sensitive information, nuclear safety, nuclear security, and material accountancy and control at these facilities. A compromise of computer systems could have a negative impact on nuclear security, both directly and indirectly, and could support malicious acts.

The IAEA Nuclear Security Series addresses nuclear security issues relating to the prevention and detection of, and response to, malicious acts involving nuclear material, other radioactive material, or associated facilities, including theft, sabotage, unauthorized access and illegal transfer. In support of the international consensus guidance issued in the IAEA Nuclear Security Series, the IAEA also produces other publications that provide additional expert advice on specific topics.

IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities, sets out guidance on establishing a computer security programme at a nuclear or radiological facility. Security is not solely a matter of prevention; it also involves detection and response. Each system owner or operator needs to have processes and contingency plans in place to detect and respond to computer security incidents that could potentially adversely impact systems used for physical protection, nuclear safety, and nuclear material accountancy and control, or that could lead to the unauthorized release of sensitive information.

The purpose of this publication is to assist Member States in developing comprehensive contingency plans for computer security incidents with the potential to impact nuclear security and/or nuclear safety. The publication provides an outline and suggestions for establishing a computer security incident response capability as part of a computer security programme, and considers the roles and responsibilities of the system owner, operator, competent authority and national technical authority in responding to a computer security incident with possible nuclear security repercussions.

This publication was prepared with the assistance of over twenty experts in two consultancy meetings and a series of external reviews, with input from more than from 12 Member States and international organizations.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

A nuclear security regime should ensure that there are systems and measures in place at all appropriate organizational levels to detect and assess nuclear security events and notify the relevant competent authorities[1] so that an appropriate response can be initiated. [1] The development of a national framework for managing the response to a nuclear security event is an important part of a national nuclear security regime.

It is increasingly recognized that computer security is a key component of nuclear security, presenting a unique set of challenges for facilities that handle nuclear and other radioactive material, and for associated activities such as transport. The primary concern is a malicious attack that directly or indirectly threatens the security of nuclear and/or radioactive materials.

The main aim of computer security is to prevent computer systems from being compromised, but organizations need to also be prepared to respond if an external or internal adversary succeeds in compromising their system. Facilities and State organizations need a contingency plan in place for nuclear security events that involve computer security incidents and the associated response. This plan has the aim to address isolating the danger, mitigating damage, notifying competent authorities and carrying out restoration processes.

Nuclear Security Series No. 13: Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [2] states that “Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber-attack, manipulation or falsification) consistent with the threat assessment or design basis threat.”

Protection is not solely a matter of prevention. It must also involve detection and response. Each system owner or operator needs processes and contingency plans in place to detect and respond to computer security incidents that might potentially impact systems used for physical protection, nuclear safety, and nuclear material accountancy and control, or that could lead to the unauthorized release of sensitive information, including information that might facilitate future attacks.

1.2. PURPOSE

The purpose of this publication is to assist Member States in developing comprehensive response plans for computer security incidents with the potential to adversely impact nuclear security and/or nuclear safety.

This publication supplements the existing literature by addressing the unique nature of nuclear and other radioactive material facilities and the unique security requirements associated with nuclear and other radioactive material. It provides guidance on the key elements for developing and implementing a comprehensive response to a computer security incident (i.e. cyber-attack) that may compromise or adversely impact nuclear security. It covers:

- Characterizing computer security incidents;
- Defining response policy, roles and responsibilities;
- Implementing the computer security incident response plan;

[1] Italicized terms are defined in the Glossary at the end of this publication.

- Computer security incident communication;
- Industrial control system considerations;
- Information system considerations;
- Physical protection system considerations;
- Nuclear security considerations.

1.3. SCOPE

This publication is intended for individuals or organizations involved in developing, implementing or executing contingency plans for computer security incidents with the potential to impact on nuclear security and/or nuclear safety. The guidance in this publication is applicable to:

- Competent authorities, including regulatory bodies;
- Management in facilities, companies and organizations involved in the use, storage or transport of nuclear material or other radioactive material;
- Operators and their staff;
- Contractors or other third parties working for the authorities, organizations or facility operators;
- Other entities that may play a role in the response to computer security incidents, including international and national law enforcement agencies;
- National and/or regional technical authorities such as Computer Emergency Response Team (CERT) organizations.

The guidance provided specifically relates to computer security incidents occurring or initiated at the operator, licensee, or supporting organizations such as vendor or maintenance support entities. However, this publication could be used by competent authorities and technical authorities to develop incident response processes and capabilities for incidents occurring or initiated within their respective organizations or locations.

The guidance may be adapted to meet the requirements of organizations and/or Member States in compliance with their national laws and regulations.

1.4. STRUCTURE

This publication is in five sections with eight associated annexes. The remaining sections are:

- Section 2. Concepts and Context: This section introduces the basic concepts used throughout the publication.
- Section 3. Policy, Roles and Responsibilities: This section sets out the policy, roles and responsibilities for preparing and implementing contingency plans.
- Section 4. Phases of an Incident Response: This details the computer incident response process, including the phases of the response.
- Section 5. Incident Analysis: This section discusses the multiple aspects of impact analysis required in a computer security incident and details the flow of activities during the response.

Eight annexes provide further information on:

- Incident indicators;
- Incident analysis guide;
- Special considerations for industrial control systems;
- Incident scenarios;
- Incident reporting;
- Evidence collection;
- Examples of technical characterizations;
- Example of a computer security incident response policy.

2. CONCEPTS AND CONTEXT

2.1. OVERVIEW

Nuclear facilities, other radioactive material facilities, associated facilities, organizations and activities, have a responsibility for the protection of sensitive information and sensitive information assets whose compromise could impact nuclear security. This includes the development of contingency and response plans as well as the requisite capabilities to address malicious acts including cyber-attacks.

In planning how to respond to computer security incidents, it is first necessary to understand and define what these are, and to identify when such incidents can result in a nuclear security event. This section clarifies the meaning of important terms used in this publication. It also applies the key concepts of computer security incident response planning to nuclear security.

The terms computer and computer system refer here to the computation, communication, instrumentation and control devices that make up functional elements of the nuclear facility. These include desktop computers, mainframe systems, servers and network devices, as well as lower level components such as embedded systems and programmable logic controllers (PLCs). [3]

A control system is a specific category of computing or networked system that responds to input signals from the process or an operator and generates output signals, thereby ensuring that the process continues to operate in the desired manner.

Control systems include the instrumentation and control (I&C) systems used in the operation of a nuclear power plant, a fuel cycle or storage facility to support a variety of functions. These are known by various names in the industry. In this document, the term industrial control systems (ICS) will be used. They include: supervisory control and data acquisition systems (SCADA), distributed control systems (DCS), and other control system configurations such as skid-mounted PLCs. [4]

A computer security incident is any event with actual or potential impact on a computer system or computer network. This also includes the act of violating an explicit or implied security policy.

The Council of Europe Convention on Cybercrime [5] categorizes computer security incidents in terms of offences against the confidentiality, integrity and availability of computer data and systems. These categories are:

1. Illegal access: Access without right to the whole or any part of a computer system.

2. Illegal interception: Interception by technical means, without right, of non-public transmissions of computer data to, from or within a computer system, including interception of electromagnetic emissions from a computer system that carry such computer data.

3. Data interference: Causing damage, deletion, deterioration, alteration or suppression of computer data without right.

4. System interference: Seriously hindering, without right, the functioning of a computer system by inputting, transmitting, damaging, deleting, causing deterioration of, altering or suppressing computer data.

5. Misuse of devices: The production, sale, procurement for use, import, distribution or otherwise making available of:

- A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences in categories 1 to 4 above;
- A computer password, access code, or similar data with which the whole or any part of a computer system can be accessed, with the intention of using it for committing any of the offences in categories 1 to 4 above.

Computer security incidents have the potential to jeopardize the confidentiality, integrity and availability (CIA) of a computer system and the data it processes, stores or transmits. A security incident might also be a violation — or the imminent threat of a violation — of an explicit or implied security policy, an acceptable use policy, or standard security practice. While certain adverse events (e.g. floods, fires, electrical outages and excessive heat) can cause a system outage, they are not the malicious acts of individuals or organizations and therefore are not considered to be computer security incidents.

A computer security incident becomes an information security incident or breach when it involves the actual or suspected compromise or loss of information or data. The most serious of these incidents involve sensitive information. Sensitive information is information whose unauthorized disclosure (or modification, alteration, destruction or denial of use) could compromise the security of a State, of facilities associated with nuclear or other radioactive material, or of nuclear programmes, or may otherwise assist in the carrying out of a malicious act against a nuclear site, facility, organization or transport. Examples of sensitive information include the physical protection regime at a nuclear facility, the location and transport of nuclear or other radioactive material, or details of an organization's personnel. The IAEA Nuclear Security Series No 23-G Security of Nuclear Information [6] discusses and provides examples of potentially sensitive information associated with nuclear and other radioactive material facilities.

A Nuclear Security Event is an event that has potential or actual implications for nuclear security. In today's digital age, the reality that a cyber-attack could impact nuclear security needs to be considered.

A Computer Security Incident Response Team (CSIRT) is a local team responsible for responding to computer security incidents within their own organization. The size, composition and capabilities of a CSIRT may vary greatly depending on the nature of the organization and the computing infrastructure.

In this publication, technical authority (TA) refers to an organization with specialized skills and resources for responding to computer security incidents. The TA is looked upon to supplement the internal computer security response capabilities of an organization in responding to events. The TA may be the organization called on to respond if a computer security incident exceeds the Design Basis Threat (DBT) as defined for cyber-attacks. This is discussed in Nuclear Security Series No 10 Development, Use and Maintenance of the Design Basis Threat [7].

A Computer Emergency Response Team (CERT) is an example of a technical authority whose sole purpose is to provide assistance and response capabilities when a computer security incident occurs. CERTs may exist at many levels (national, local or sector).

2.2. OVERVIEW OF COMPUTER SECURITY INCIDENT RESPONSE

Computer security incident response is not a single action but an approach that supports not only the detection of a computer security incident, but also mitigation and recovery from such an incident. It can be considered to encompass four phases: Preparation; Detection & Analysis; Containment, Eradication & Recovery; and Post-Incident Activity. Figure 1 shows the sequence of these phases. Each phase will be discussed in greater detail in Section 3.

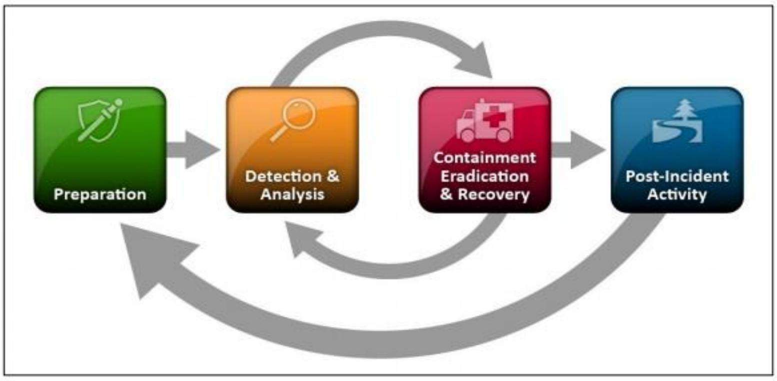


FIG. 1. Computer Security Incident Response Phases [8][2]

2.3. TIERS OF COMPUTER SECURITY INCIDENT RESPONSE

The complexity of cyber-attacks and their potential impact means that an important element in responding to computer security incidents is the structure that supports effective communication between operators, non-regulated organizations, competent authorities and technical authorities.

This structure may be multi-tiered, depending on the severity and nature of the incident. Figure 2 illustrates one possible structure used by some Member States. The first tier of response occurs at the incident location, such as an operator’s facility, an office of a non-regulated entity, or even a competent authority headquarters. The second tier represents a national, regional or sector capability that provides technical computer security incident response support beyond the capability of the response team, such as a technical authority, at the incident location. A CERT may provide this capability. The third tier is represented by the Competent Authorities whom may be involved depending on the nature of the incident and may include the regulator, law enforcement agencies, intelligence agencies, and/or others.

The following sections describe the responsibilities of these tiers of response. Although the term ‘operator’ is used, the same level of responsibilities could be applied as appropriate to non-regulated entities with responsibilities for nuclear security.

[2] Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States of America.

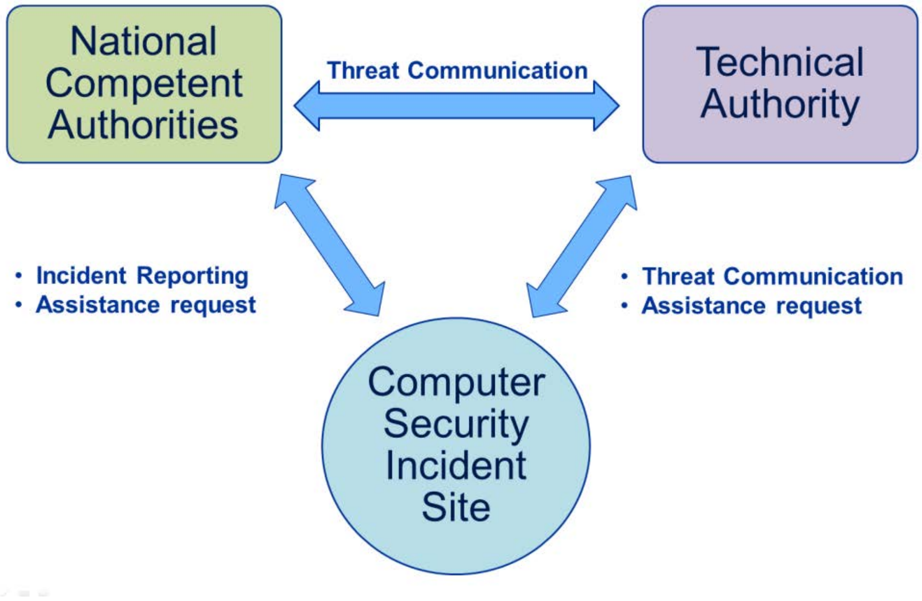


FIG. 2. Incident response communication pathways (tiered).

3. POLICY, ROLES AND RESPONSIBILITIES

3.1. OVERVIEW

It is crucial to develop policies, defined roles and responsibilities, and detailed procedures for a response to computer security incidents before an incident occurs. This section provides example guidance and recommendations on policy, roles and responsibilities for all tiers of the response including, but not limited to, the State (or international organizations), the technical authority, the competent authority and the operator.

3.2. COMPUTER SECURITY INCIDENT RESPONSE POLICIES

While policies will be highly individualized to each organization, most will include the same key elements regardless of whether the organization's computer security incident response capability is in-house or assigned to other competent authorities. Annex VIII provides a sample policy. Key policy elements include:

- A statement of management commitment;
- Policy objectives and purpose;
- The designation of a computer security incident response coordinator;
- The scope of the policy (i.e. to whom and what it applies and under what circumstances);
- A definition of computer security incidents and their consequences within the context of the organization;
- Organizational structure and the delineation of roles, responsibilities and levels of authority;
- Prioritization or severity ratings for computer security incidents;
- Reporting processes;
- Training and exercise requirements;
- An awareness programme;
- Team composition.

3.2.1. State's responsibilities

An important component of a nuclear security regime is the State's responsibility to ensure that nuclear security systems and measures are in place at all appropriate organizational tiers (i.e. operator, CA, TA) for detecting and assessing nuclear security events and notifying the relevant competent authorities so that appropriate response actions can be initiated. This includes computer security incidents or threats that have actual or potential implications for nuclear security. The State's responsibility for computer security incident response may therefore include:

- Providing legislation for the security of computer assets at nuclear facilities and the security of nuclear sensitive information, including the criminalization of cyber-attacks on nuclear assets. Such legislation may directly address nuclear security or may be part of a larger security framework;

- Providing relevant computer threat information to the relevant authorities and operators. (This need not be through direct communication, but may be relayed via a competent authority.);
- Providing a national contingency resource to respond, if required, to cyber-attacks directed at nuclear material, other radioactive material, or associated facilities or activities;
- Consequence analysis and recovery operations as needed;
- Regularly performing assurance activities — such as national nuclear security exercises that include computer security incident scenarios — to identify and address issues and factors that may affect the capacity to provide an adequate computer security incident response;
- Specifying and coordinating relevant reporting activities to improve the management of computer security incidents;
- Developing, utilizing and maintaining the design basis threat (DBT) or threat assessment to include a computer threat component. The DBT or threat assessment is a key element in designing computer response capabilities for the operator and other authorities. The DBT may additionally define the criteria and designated resources for computer security incidents involving threats having capabilities that exceed the DBT [7].

3.2.2. Technical authority's responsibilities

A technical authority such as a Computer Emergency Response Team (CERT) delivers similar services to the operator's internal Computer Security Incident Response Team (CSIRT), but usually has a broader perspective and more extensive technical resources or services.

A formal agreement is recommended between the CERT (or other appropriate technical authorities) and the operator to support the response to computer security incidents, when required. This agreement would describe the relationship between the technical authority and operator, and may include:

- Defining the roles and responsibilities of the two organizations;
- Specifying conditions under which the operator will engage the technical authority;
- Specifying conditions under which the technical authority is advised to report threat information to the operator;
- Detailing the protection and confidentiality requirements for shared information;
- Specifying conditions under which the technical authority would share operator information with other entities;
- Detailing the availability and capability of technical authority resources and how the operator requests services;
- Specifying the role and availability of national advisory services for the communication of new threats or vulnerabilities.

3.2.3. Competent authority's responsibilities

Competent authorities, and specifically regulatory bodies, are responsible for establishing nuclear security regulations and requirements, and associated procedures for evaluating applications and granting authorizations or licenses. Specific responsibilities integral to the computer security incident handling process, include:

- Defining the expected operator response to a computer security incident and the criteria above which national resources will be provided to assist the operator;
- Defining information exchange, reporting and handling requirements for cyber-threat and incident information;
- Identifying and designating components of a computer security incident response for inclusion in contingency plans as appropriate. Providing guidance to the operator on the development of computer security plans, including computer security incident response;
- Conducting periodic reviews and assessment of the operator's computer security incident response plans;
- Designating a computer security coordinator within the competent authority who has adequate expertise to address computer security and computer security incidents. The computer security coordinator may be resident in the nuclear regulator or within another branch of the government; regardless of location, he or she must be clearly identified;
- Periodically conducting on-site inspections.

3.2.4. Operator's responsibilities

The ultimate responsibility for maintaining safe and secure operations lies with the operator. This includes the protection of nuclear and other radioactive materials. The operator is the first line of defence in the identification of a cyber-attack and the initial response. The operator's responsibilities with regards to computer security incident response include:

- Developing and maintaining computer security and computer security incident response capabilities to address threats consistent with the DBT or threat assessment;
- Carrying out computer risk analysis, including a vulnerability assessment. This may be included as part of a broader organizational risk analysis;
- Defining the set of digital systems and components accredited as performing important safety or security functions;
- Developing an Incident Response Policy (see Annex VIII for an example policy), Plan and Procedures for contingency and recovery operations;
- Designating a point of contact for computer security and a local Computer Security Incident Response Team;
- Providing initial characterization of a computer security incident;
- Providing notification of the incident as mandated;
- Providing incident documentation and assisting in the forensic process;
- Providing training and periodic exercises for incident response personnel.
- Engaging with the technical authority (e.g. the CERT) as needed;

— Sharing relevant incident information as appropriate;

— Complying with the regulations or guidelines issued by the CA.

3.3. THE COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

It is recommended that all organizations with nuclear security responsibilities, and which rely upon computers and computing systems, establish a Computer Security Incident Response Team (CSIRT). The goal is to create a multi-disciplined response capability to address the many facets and possible impacts of a computer security incident.

While the precise expertise required for the team will depend on the nature of the organization, its computer assets and the systems affected, expertise for the following areas is recommended:

— Computer security and computer security incident response.

> While the field of computer security is extensive, the computer security incident response process requires specific skills and training to respond to, analyse, and mitigate events impacting the confidentiality, integrity and availability of computer systems.

— Architectural, design and operational knowledge for deployed systems.

> An experienced designer, network, desktop and application architect needs to be engaged when planning the computer security incident response as their knowledge of the deployed systems will provide the type of insight needed to link into the incident security response process.

— Nuclear security.

> Nuclear material and other radioactive material and their associated facilities and activities present unique characteristics, constraints and security concerns. It is important that these are incorporated into the computer incident response process.

— Safety awareness as appropriate for the organization.

> The impact or potential impact on safety is one of the first considerations to be evaluated for a computer security incident. This is especially true when the computer security incident may have as its objective the theft, sabotage, unauthorized access or illegal transfer of — or other malicious act involving — nuclear material and other radioactive substances and their associated facilities.

— Communication: internal and external information exchange related to the incident.

> Communication is essential to the success of any computer security incident response. This includes communication within the organization and externally to partners and other agencies with relevant responsibilities.

Note that the composition of the CSIRT may evolve as the incident's nature and impact changes or becomes better understood. The CSIRT may be a component of the overall contingency or emergency response.

3.3.1. CSIRT organization

Computers are integrated across nearly all of an organization's operations, including business and information management systems and perhaps industrial control systems and physical protection systems. This section presents a notional computer security incident response organization covering all these areas. It is followed by an illustrative description of process flow that can be applied in a graded manner.

While each organization will structure their incident response roles in line to meet local needs, the following construct illustrates in a general way the mapping of role to function. Seven core roles or functions are identified within the computer security incident response process. These are Incident Response Management, Incident Response Coordination, Impact Analysis, Technical Assessment, Technical Support, Communications, and Incident Response Support / Extended Team Liaison. Organizational structures and specific titles may vary, but it is important that these functions are specified and assigned. Figure 4 illustrates a proposed organizational structure for these roles. This is just an example of one possible structure including associated roles that would ideally be based upon specific organizational needs.

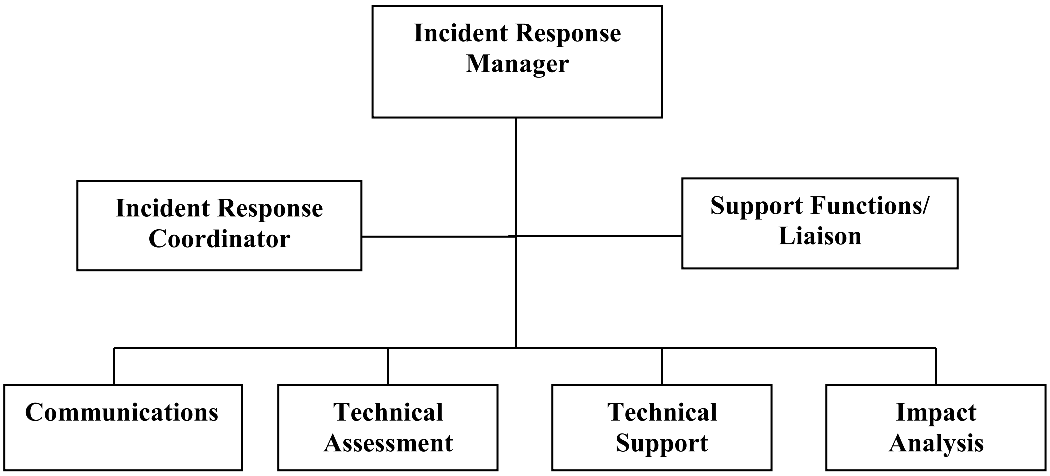

Incident Response Manager
Incident Response Coordinator
Support Functions/ Liaison
Communications
Technical Assessment
Technical Support
Impact Analysis

FIG. 3. A notional CSIRT organizational structure.

3.3.2. Incident Response Manager

The Incident Response Manager is a member of senior leadership who supervises the overall response to the computer security incident and acts as the direct interface to senior management. The Incident Response Manager role is not implemented for every incident, but only when the severity of the event requires escalation to the highest levels within the organization. In such cases, the Incident Response Manager assumes control of organization-wide response activities from the Incident Response Coordinator, who will still continue to manage activities local to the incident.

3.3.3. Incident Response Coordinator

The Incident Response Coordinator leads the response at the scene of the incident, supervising and managing activities. For incidents of escalation levels 0 and 1 (described below), the Incident Response Coordinator may act as the single point of coordination in the incident response. In the case of an escalation to a higher level, the Incident Response Coordinator will transfer overall incident management responsibilities to the Incident Response Manager but continue the role of local incident coordination.

3.3.4. Technical assessment role

The technical assessment role is generally composed of relevant subject matter experts (SMEs) who are assembled according to the type of event or incident. They have the role of monitoring all known sources for alerts or notifications of threats and then performing the technical evaluation to determine whether the incident has manifested itself within the organization, working with the Incident Response Coordinator on the initial escalation of the incident.

3.3.5. Impact analysis role

The impact analysis role is to assess the business impact to the organization as well as to determine whether the impact could also have an impact on plant or material operations. The impact analysis role works with the Incident Response Manager, the Incident Response Coordinator and any SMEs needed in order to gather enough information to decide which courses of action are necessary for containment and eradication of the threat.

3.3.6. Communications role

The communications role is responsible for ensuring that internal and external stakeholders are kept aware of the current state of the computer security incident. This includes technical communications about measures to be put into place to help mitigate the effect of the incident as well as ensuring that all external communication accurately reflects the state of the incident and actively engages the extended team for incident support.

3.3.7. Technical support role

Technical support refers to the larger set of technical computer resources that may be required in the response. These may include: specific system administrators, help desk staff, system owners, instrumentation and control engineers, and process control engineers. They work under the direction of the Incident Response Coordinator and are responsible for implementing the recommendations provided by the Technical Assessment Team.

3.4. THE COMPUTER SECURITY INCIDENT RESPONSE PLAN

The Computer Security Incident Response Plan and associated procedures describe the specific technical processes, techniques, checklists and forms used for a computer security an incident response. The plan needs to be comprehensive and detailed to ensure that the priorities of the organization are reflected in the response operations. Following standardized contingency response actions supports minimizing errors, particularly those that might be caused by the fast tempo and pressure of the incident response.

One primary function of the computer security incident response plan is to ensure the integrity and rapid recovery of essential system functions associated with safety, security, material accountancy and control, and emergency preparedness.

3.4.1. Elements of the Computer Security Incident Response Plan

While each computer security incident response plan will be customized according to the individual organization’s structure and needs, the following key elements are recommended:

— Senior management sponsorship, including the necessary approvals, authorities and resources to execute the plan.

> Senior management commitment is needed to provide the resourcing for a computer incident response capability and to ensure the organization’s commitment to the computer security incident response plan.

— Procedures for how to report computer security incidents.

Clear policies and procedures on incident reporting are necessary. These may include templates for the required information to be reported and a continually updated contact lists.

— A process for how and when to invoke the response plan components.

Invoking the response plan can be resource intensive and time consuming. Clearly defined thresholds are needed to address when the various parts of the response plan are engaged. Some aspects of the response plan, such as its preventative and investigative elements, may be engaged daily, while escalation criteria are needed for establishing a measured response to an incident and with a graded approach to action.

— Maximum allowed response time requirements for reporting, to include key points such as the initial notification, technical characterization and initial impact analysis.

The CSIRT commits to meeting response time requirements times for detection, reporting, notification and technical characterization of an incident. These tasks are often tough if the organization is confronting an unfamiliar computer security incident, but this provides an opportunity to reach out to other partner agencies for support to gain a better understanding of the type of incident or object and approach the maximum response times.

— Details of the CSIRT leadership and organization, including roles, responsibilities and contact details.

Clear lines of reporting and responsibility are critical to ensure the response element in the organization is never absent or waiting for a resource that has not been defined, assigned or made available.

— Responsibilities and monitoring processes for tracking the computer security incident.

Technical teams define the responsibilities and monitoring processes for tracking computer security incidents. They are also responsible for ensuring communication with staff whose systems or processes are impacted.

— Identification of essential sites, systems, assets and interdependencies.

The computer security incident response plan needs to identify sensitive digital assets and interdependencies and also to track how compensatory measures will be leveraged to protect these elements in the event that primary and secondary security measures become compromised.

— A clear escalation path and the authorization requirements for escalation.

Escalation management is a key process in a computer security incident response. Once the incident response process has been engaged, appropriate threshold criteria may be used to help ensure the appropriate level of incident involvement and management. Escalation processes may set out the escalation criteria, the escalation decision-making authority, and associated actions.

— A clear communication plan.

Communication of the computer security incident has multiple dimensions, each with strategic and tactical importance. An incident communication plan is not unique to a computer security incident, but it is important that any computer security incident response considers the communications needs. The communication plan may have the following components:

- The purpose and objective of the communication plan;
- Identification of the nature of expected communication within the response, describing how, what and to whom to communicate;
- A specification of when and how often to communicate.

Communications with the press corps may be necessary and desirable. It is better to be in control of the message than always to be responding to others.

— Contact information for all organizations referenced within the computer security incident response plan, including internal and external technical authorities and relevant competent authorities.

A computer security incident response plan needs to identify and provide the contact information for all people, roles and organizations that are essential for the implementation of the plan. In computer security incidents, time is a critical factor in the success of preventing further compromise and ensuring the safety of plant operations.

— Procedures and criteria to be met in order to close out computer security incidents.

Clear guidelines are needed to identify when a computer security incident can be considered closed.

— Procedures to request additional, possibly external resources (such as from Technical Authorities).

Alongside the escalation plans, procedures are needed to address how to engage and employ external resources.

— CSIRT training requirements.

The CSIRT needs periodic training to fulfil and maintain their core technical and administrative competencies. Team training may also be considered to ensure the team is making best use of the latest industry best practices for computer security incident response.

— Requirements for computer security exercises and metrics for evaluating the effectiveness of the response plan.

Alongside the training requirements, assurance activities such as training exercises and other evaluation methods along with metrics are needed to continually assess the effectiveness of the plan and CSIRT readiness.

— Requirements for the periodic review of the plan and response procedure.

Cyber-threats are dynamic in nature. The computer security incident response plan needs be reviewed periodically to help ensure that new threats and threat vectors are adequately addressed. This review may be comprehensive and take place annually, or it may be spread throughout the year, focusing on specific elements to break the task up and perhaps make it more manageable.

— Lessons learned.

The collection and sharing of lessons learned is an excellent component of continuous improvement.

Confidentiality of the computer security incident response plan and incident information needs to be carefully considered and appropriately handled.

3.5. OPERATOR PROCESSES AND PROCEDURES

The operator's computer security incident response processes and procedures need to consider the operational environment, potential threats, vulnerabilities and experience from previous incidents. The procedures also need to address minimization of the impact to systems with nuclear safety, security, material accountancy and control, and emergency preparedness functions.

The operator needs to consider the possible incident scenarios (see Annex IV) when developing procedures for response. The procedures may be developed to addresses situations such as:

- Malware infection, quarantine and removal;
- Suspected hacker infiltration;
- Denial of service (DoS) attacks;
- Distributed denial of service (DDoS) attacks;
- Isolation of a control system from other networks (if possible);
- Reconnection of a control system to other networks;
- Inability to view the status of system operation (loss of view);
- Inability to control system operation (loss of control);
- Insider attacks;
- Social media probes;
- Supply chain attack or compromise;
- Unauthorized network outbound traffic;
- Rapid reconfiguration to steady build;
- A leak or loss of sensitive information;
- Impairment of safety or special safety systems.

The above list is based upon known attack profiles and represents a starting point for developing procedures. The CSIRT is advised to develop its own set of procedures based on its own situation. Such procedures need to have a periodic review process to ensure their applicability and effectiveness.

In addition to procedures addressing specific types of situations, procedures are also needed to support operational processes that directly or indirectly support a computer security incident response. These procedures may be included in specific incident response guidance or may be incorporated as components within other operational procedures.

- Anti-virus and intrusion detection system signature updates.

  The management of known threats (malware, viruses, etc.) requires a methodical approach to anti-virus and intrusion detection, including multiple layers of protection (such as for the desktop or for networks) and an update plan for signatures.

— Security patching processes.

Managing security patches to mitigate known vulnerabilities may be considered. During incidents, patch installations may be required to prevent re-infection via the same vulnerability.

— System backup and recovery.

Regular system and data backups need to be planned as part of the continuity of operations plan. Additionally, periodic testing of recovery processes is needed to ensure that, during a computer security incident; systems can be rebuilt and recovered in a timely manner to known good configurations.

— Contingency processes to restrict and/or modify access control to support response, analysis and investigative processes, including the planning and setup of emergency user accounts.

During a computer security incident, it may become necessary to restrict access to systems, networks and facilities to certain users according to the scope of the investigation. To accomplish this efficiently requires technical measures to be in place before there is any additional damage, as well as administrative measures so that those who make the decision to restrict resources are clear on their authority and supported by management.

— Confirmation of correct system operation (i.e. a procedure for verifying that a system is operating as normal).

Defining the normal state of a system requires a list of testable controls and their range of normal operational limits. Testing these on a regular basis is a good way to understand system operation and to identify anomalous behaviours. The testing can be conducted by computer security operators and periodically by independent evaluators.

— Data integrity validation processes.

It is not sufficient to assume that every system that produces data is producing data that has not been altered. This is especially important for the ICS within a plant where these provide data on the physical operation of processes and/or components. These data may be verified periodically to understand and validate behaviours.

— Backup secondary systems or measures.

In the event of a system or component failure, systems or measures to compensate for this need to be identified with processes to ensure a transition from systems that may have been affected to secure and possibly redundant systems. Such processes may involve reverting to a secure system build or shifting to a backup facility. Compensatory measures or systems may also be needed to mitigate impact or recover lost function.

— Handling elevated computer threat conditions (a new vulnerability or an exploit applicable to plant systems).

An incident response includes the assessment process and adaptation to address changes in computer threat conditions. New vulnerability or exploits may be handled through the security patch process.

— Procedures for recertification or acceptance of the system prior to restart.

Before a component or process is brought back online in support of plant functions, some level of recertification may be needed. This ensures the integrity of the system and that it is indeed free from compromise and protected against the original incident. Additionally, some level of recertification may be required as a licensing constraint.

— Special procedures in response to impairment of safety or special safety systems.

In addition to the normal computer security incident response, an incident that impacts safety or special safety systems may require additional processes covered in other procedures. It is important to understand and define the interface between these procedures.

— Identifying and reporting suspected computer security incidents.

Although it may be difficult to identify compromise to a computer or associated faulty operation, clearly defined processes are needed to assist staff in identifying and reporting suspicious computer activity.

— Evidence collection[3].

Digital evidence is essential on many levels: for identifying the potential motives of the attacker, the identity of the perpetrators, the purpose of the malware, etc. Procedures are needed that address the collection of evidence and the preservation of the chain of custody in line with legal requirements. These procedures may also address environmental impacts such as humidity, temperature and shock to the digital device, packaging options, and transport and storage requirements. The collection and processing of digital evidence may be left to Competent Authorities, but it is essential that the system owners and the local CSIRT understand and support these processes.

The computer security incident response plan may identify law enforcement representatives to be contacted, the conditions under which computer security incidents needs to be reported to them, how the reporting is to be carried out, what evidence needs to be collected, and the evidence collection process to be used.

[3] Evidence Collection: The International Standard ISO/IEC 27037:2012(E) provides guidelines for specific activities in the identification, collection, acquisition and preservation of digital evidence that may be of evidential value. Any computer security incident responder must understand the fragile nature of computer-based digital evidence, which may be altered, tampered with or destroyed through improper handling or examination. During identification, collection, acquisition and preservation of potential digital evidence, it is necessary to follow an acceptable methodology to ensure the integrity and authenticity of the potential digital evidence. An acceptable methodology in obtaining digital evidence will contribute to its admissibility in legal and disciplinary actions. Additional information on digital evidence collection is found in Annex VI.

4. PHASES OF COMPUTER SECURITY INCIDENT RESPONSE

4.1. OVERVIEW

This section describes each phase of computer security incident response and the task responsibilities assigned to the operator, competent authority and technical authority. For many of the tasks, the responsibility is shared between more than one of these roles.

The response process consists of four interdependent phases: preparation; detection & analysis; containment, eradication & recovery; and post-incident activity. Often, multiple groups will be involved in the different aspects of the response. Collaboration and communication flow between these groups and from one phase to the next is essential for the rapid resolution of, and recovery from, the incident.

4.2. PREPARATION

The Preparation phase is made up of key planning functions. These include: establishing a policy that will inform the operational processes and clearly define the roles and responsibilities of all parties involved in the incident response process; drafting and implementing procedures to carry out the policy actions; and the identification of assets. It is important that the criteria for computer security incidents are clearly defined along with the associated response requirements. It is also essential that senior management has agreed these planning and response functions.

Additionally during the Preparation phase, the CSIRT(s) are encouraged to participate in security exercises, both separately and with other First Responder and Emergency Response Teams. Such exercises may include discussion and analysis of possible compromise scenarios, risk and impact assessments, ensuring staff awareness of the other incident response roles, and prioritization of recovery activities. Exercises are both an assurance activity and a means of identifying any deficiencies in the response activities.

The following table contains a list of tasks within the preparation phase of the computer security incident response process. Each task is assigned to one or more of: the operator (O), the competent authority (CA) or the technical authority (TA).

TABLE 1. PREPARATION PHASE TASKS

	Task	O	CA	TA	Comments
1.	Establish computer security incident response policy, including roles and responsibilities.	X	X	X	Roles and responsibilities need to include the relationship between organizations. The CA needs to have a computer security incident response policy.
2.	Designate the Computer Security Incident Response Team (CSIRT).	X	X		The operator and CA needs to designate the team in accordance with the established roles and responsibilities.
3.	Develop computer security incident response procedures.	X	X	X	It is advised that procedures include communication requirements and criteria for actions between organizations.
4.	Identify sensitive digital assets.	X			An understanding of these assets, their configuration, architecture, and data flow is essential for response and recovery.

	Task	O	CA	TA	Comments
5.	Identify risk, and define priorities for the response.	X			The operator is responsible for the identification of risk and prioritizing the response, calling on resources as needed.
6.	Identify the capabilities needed and any gaps in the computer security incident response.	X			The operator is responsible for identifying the capabilities needed and any gaps in the architecture or computer security plan that could hinder or prevent an adequate response.
7.	Identify the tools for use in a computer security incident response and ensure their availability.	X		X	The TA may provide a list of their recommended tools that support both computer defence capabilities and the preparation of artefacts for processing by the TA. It is advised that the operator identify and if possible qualify[4] tools for use in the computer security incident response process. Tools may support the collection of incident information and incident analysis.
8.	Ensure up-to-date and accurate architectural, data flow diagram, and configuration data are available to be accessed by the CSIRT.	X			The operator is responsible for the accuracy of all architectural diagrams including data flow and configuration data.
9.	Ensure the CSIRT undertakes security exercises (both separately and with other Emergency Response Teams).	X	X	X	Emergency response drills and exercises are desired to be conducted by the operator (and periodically involve the CA and TA) to validate the response procedures, including the requirements for communication between organizations.
10.	Discuss and analyse possible compromise scenarios that are consistent with the threat assessment or Design Basis threat.	X	X	X	It is advised that such discussions be a recurring task performed by the operator, CA and TA to ensure that new threat vectors are incorporated and compromise scenarios updated.
11.	Define computer security incident reporting criteria.		X	X	The CA and TA need to determine computer security incident criteria and thresholds as these will drive reporting requirements and define the instances when external consultation is recommended.
12.	Define and implement automatic and manual detection methods.	X	X	X	The CA and TA will provide guidance detection methods as part of good practices. The operator will determine which of these are critical to implement given the specificities of their facility infrastructure and sensitive digital assets.
13.	Conduct periodic reviews and assessment of the Operator's computer security incident response plans.	X	X		The operator and CA need to both conduct assessment activities associated with computer security incident responses.

4.3. DETECTION AND ANALYSIS

During the Detection and Analysis phase, the CSIRT is responsible for determining the technical characterization of the incident. Detection activities include ensuring there is an adequate data monitoring infrastructure in place that supports the detection, collection and

[4] Tools certified as having satisfied equipment or software qualification requirements for the conditions relevant to its safety and security function(s). Qualified equipment containing software has been tested to ensure there is no adverse impact to the associated systems where these tools may be placed into service or use.

preservation of information related to an incident or potential incident. The CSIRT may use a test and evaluation environment for the analysis of incidents so as not to impact operational systems or damage potential forensics evidence.

One of the more difficult parts of the detection and analysis phase is determining which events are to be tracked as part of the computer security incident response process. Annex I of this document contains two lists of computer security incident indicators, and Annex IV contains incident scenarios that put the incident indicators into context.

Analysis activities may take place at many levels and may extend beyond the initial computer security incident response team and the initial technical characterization of the incident. Certain aspects of the analysis may require extensive time and effort. The priorities for the analysis could be:

1. Determining the potential impact of the incident on safety, security and emergency preparedness and identifying actions to place the organization or facility in a safe condition.

2. Identifying the extent of the incident to establish an adequate response.

3. Determining the potential damage from the incident in terms of potential information loss, physical damage to the facility, and public perception.

4. Determining the nature of the incident with regards to the attacker's intent and the ongoing threat.

5. Identifying the root cause of the incident and the efforts needed to prevent or mitigate future occurrences.

6. Identifying the source of the attack, the attacker and developing a profile of the attacker.

Section 4 provides additional guidance on the types of analysis that an incident might require. Annex II of this document contains an incident analysis guide and Annex VI an overview of the forensic collection process to support computer security incident analysis. This information will support the collective response of the CSIRT, the organizational leadership, and any external parties involved.

The following table lists tasks within the detection and analysis phase of the computer security incident response process in support of the creation of a *technical characterization* and damage assessment of the incident. Each task is assigned to one or more of: the operator (O), the competent authority (CA) or the technical authority (TA).

TABLE 2. DETECTION AND ANALYSIS TASKS

	Task	O	CA	TA	Comments
1.	Report computer security incidents or suspicious activities.	X	X		The CA may designate specific reporting requirements for computer events. This may detail the specific events that the operator is responsible for reporting.
2.	Ensure adequate data monitoring.	X	X		The operator is responsible for ensuring adequate data monitoring and the CA is responsible for the oversight of operator's compliance.
3.	Construct an adequate test and evaluation environment.	X		X	The operator is responsible for constructing an adequate test and evaluation environment drawing on the guidance of the TA when appropriate.

	Task	O	CA	TA	Comments
4.	Collect and preserve information.	X		X	The operator is responsible for the collection and preservation of information, drawing on the TA for guidance when appropriate.
5.	Analyse the cyber-threat and update the threat assessment.	X	X	X	The operator is responsible for updating and/or re-analysing threat assessments, drawing on the TA and CA for guidance when appropriate.
6.	Determine the potential impact on safety, security and emergency preparedness and identify immediate actions required to place the facility in a safe and secure condition	X			The operator is responsible for determining the potential impact of a computer security incident on safety, security and emergency preparedness.
7.	Determine which organizations to involve in the response.	X	X	X	The decision of who to involve or notify regarding the computer security incident may sometimes need to be a collective decision between the operator, CA and TA.
8.	Identify the root cause (which may be an ongoing process) and identify compensatory measures.	X		X	It is advised that the operator perform a root cause analysis with support from the TA, where appropriate.
9.	Determine infection boundaries and propagation paths.	X		X	The operator needs to determine infection boundaries and propagation with support from the TA, where appropriate.
10.	Evaluate similar systems for compromise.	X		X	The operator needs to evaluate whether similar systems have been compromised, with support from the TA, where appropriate.
11.	Evaluate other facilities for compromise.		X	X	If one facility is impacted, many others might also be compromised. Following a computer security incident, the CA and TA need to work with other facilities to assess whether they are infected or compromised as well.
12.	Develop a mitigation strategy.	X		X	The operator needs to develop a mitigation strategy for the computer security incident drawing upon the TA for guidance, when appropriate.

4.4. MITIGATION (CONTAINMENT, ERADICATION AND RECOVERY)

Given the cyclic and ongoing nature of the computer security incident response process, mitigation activities are ongoing and adapted as additional information is collected and analysed during the Detection and Analysis phase. The goals for mitigation are: (1) containment of the computer security incident, (2) eradication of any malware from the affected systems, and (3) recovery of system function, which may require other compensatory measures. Even if the compromised components or systems do not provide a critical safety or security function, they would still need to be checked and cleared to guard against the attack propagating to a component or system that does provide a critical safety or security function.

When planning a containment strategy, it is important to recognize that a number of components may be identified during the incident investigation as having been compromised. If any compromised component provides a critical safety or security function to the organization — such as contributing to the protection of sensitive digital assets, safe operation of the facility, or nuclear or other radioactive materials — it will be necessary to implement measures to ensure continued protection until the component can be brought back into operation. Such measures may include like-for-like replacement of a service (such as a backup firewall), isolation of safety components, systems, and architectures, or a stopgap measure such as a security guard who provides access control protection for part of a facility for example if the digital access control system become unavailable. It is the function that needs to be recovered, not necessarily the computer system itself.

An example of the three steps of mitigation — containment, eradication and recovery — would be when malware is discovered on a system. The first step would be to neutralize the possibility of propagation via any existing or new infection vectors. Next would be to determine whether additional measures such as security monitoring tools or updated signatures to existing tools may need to be deployed to protect and defend against re-infection. Finally, a system rebuild may be carried out, reinstalling the operating system and associated software from a trusted copy, and then recovering the system data from known good backups. For industrial control systems, this step may also include the installation of new equipment. Once the system is rebuilt, acceptance testing may be required to verify the operation and the integrity of the system.

The following table contains a list of tasks within the mitigation phase of the computer security incident response process that support the restoration of necessary systems and functions (and which may involve the use of compensatory measures). Each task is assigned to one or more of: the operator (O), competent authority (CA) or technical authority (TA).

TABLE 3. MITIGATION TASKS

	Task	O	CA	TA	Comments
1.	Ensure the facility (and/or system) is placed in a safe and secure condition.	X			The operator needs to take appropriate measures to place the system, systems or facility in a safe and secure condition.
2.	Neutralize the propagation and new infection vectors (e.g. implement compensatory measures)	X		X	The operator is responsible for neutralizing the propagation and any new infection vectors, drawing on assistance from the TA when appropriate.
3.	Conduct a system rebuild and recovery from backup.	X	X	X	The operator is responsible for the system rebuild in accordance with the CA's security guidelines and in consultation with the TA to ensure the system is not re-infected.
4.	Install new equipment.	X	X		Some computer security incidents may lead to the situation where replacement of equipment is preferred to the recovery of existing equipment. The operator may need to install new equipment in accordance with the CA's guidance on installation of systems and their accreditation.
5.	Monitor the mitigation process.	X	X		During mitigation, it is advised that the operator monitor the process to ensure its effectiveness. Similarly, the CA may require periodic updates of the mitigation process and its effectiveness.
6.	Monitor for re-infection	X		X	The operator is responsible for monitoring the environment for re-infection, drawing on the expertise of the TA when appropriate.

If an environment is infected, the CSIRT and forensic examiner have at least two responsibilities:

— Create a list of observable actions that characterize this strain of malware — including file system changes, registry changes, beacons and log events — this information can then be added to the rule sets that receive these sensor feeds.

— Create a list of malware signatures that can then be updated in the master and client anti-virus programs as well as the boundary sensor.

4.5. POST-INCIDENT ACTIVITY

The last phase of response is to carry out post-incident activities. The goal is to implement measures for the future that will prevent the reoccurrence of this type of computer security incident, enable its rapid detection, or minimize its impact. This phase may include learning lessons for internal use and possibly to be shared with the wider computer security incident response community to help prevent a similar attack from succeeding elsewhere. Key findings may ultimately allow the Implementation of new security measures to prevent re-infection, and threat profiles to be updated within the cyber threat assessments. Other activities include evaluation of the effectiveness of the computer security plan and identification of training to address gaps in performance. This may also include an assessment of the resources required to address the computer security incident.

The following table contains a list of tasks within the post-incident activity phase of the computer security incident response process in support of the implementation of measures to prevent reoccurrence of the computer security incident, including development of lessons learned and implementation of new security measures for preventing reoccurrence. Each task is assigned to one or more of: the operator (O), the competent authority (CA) or the technical authority (TA).

TABLE 4. POST-INCIDENT TASKS

	Task	O	CA	TA	Comments
1.	Develop lessons learned.	X	X	X	The operator, CA and TA, depending on their involvement, are all responsible for developing lessons learned after each computer security incident.
2.	Enhance security measures to prevent re-infection.	X	X	X	The operator is responsible for enhancing security measures; the TA can be consulted as needed and where appropriate and the CA may be needed to approve the new security measures, if required.
3.	Update the threat assessment.	X	X	X	The operator will update the threat assessment based on their post-incident analysis; the TA may be consulted as appropriate.
4.	Evaluate the effectiveness of the computer security plan.	X	X		It is advised that the operator evaluate the effectiveness of the computer security plan, reporting to the CA when appropriate.
5.	Carry out training and exercises to address gaps in performance.	X	X	X	Training and exercises to address performance gaps may be designed to include the operator, the CA and/or the TA depending on the nature of the gap and any dependencies.
6.	Report post-incident analysis as required	X	X	X	The operator, CA and TA may all have specific reporting requirements.
7.	Conduct an assessment of resource allocation.	X		X	The operator may conduct an assessment to determine the resources required to address the computer security incident, drawing on the TA for guidance when appropriate.
8.	Share lessons learned with the wider community.	X	X	X	The operator, CA and TA may desire to share lessons learned with the wider community. This may be a single document, but all parties involved in the computer security incident response may contribute to the lessons learned as appropriate.

4.6. REPORTING

During the computer security incident response process there may be a number of situations or phases that require reporting to various agencies, not only on initiation of the incident response, but throughout the process. The goal of reporting is to ensure that everyone who needs to know about a computer security incident is informed in a timely manner, recognizing that in certain types of incidents those responding are likely to be busy. A challenge organizations often face is determination of the frequency of reporting and the level of detail required.

The following table contains a list of tasks within the reporting phase of the computer security incident response process that ensure the relevant agencies are kept aware of any incidents deemed serious or critical. Each task is assigned to one or more of: the operator (O), the competent authority (CA) or the technical authority (TA).

TABLE 5. REPORTING TASKS

	Task	O	CA	TA	Comments
1.	Specify organization-wide standards for the time limit for system administrators and other personnel to report anomalous computer security incidents to the CSIRT.	X	X		These guidelines specify the criteria for reporting and the desired timeliness of the reports. There may be reporting requirements for communications initiated by both the operator and the CA.
2.	Specify the mechanisms for incident response reports and the type of information that need to be included in the incident notification.	X	X	X	It is important to establish the mechanism and format of reports prior to the occurrence of computer security incidents.
3.	Determine when a computer security incident requires notification of the TA in accordance with legal or regulatory requirements.	X	X	X	The operator needs to be aware of when it is required by the CA to report a computer security incident to the TA.
4.	Assemble and maintain contact information to be used to report computer security incidents.	X	X	X	It is important to have points of contact between the operator, CA and TA related to computer security incidents and the reporting of these.
5.	Provide feedback and awareness information to staff and site personnel with regards to prevention and responding to future incidents.	X			It is important that staff and site personnel receive periodic security awareness training that includes clear reporting criteria and structure.

5. COMPUTER SECURITY INCIDENT ANALYSIS

5.1. OVERVIEW

Computer Security Incident Analysis is an activity ongoing during all the phases of the response involving many different objectives and types of expertise. In addition to the security impact, analysis includes technical evaluation of the incident and the multiple levels of operational and safety impact. Some analyses may depend on others and some may be conducted simultaneously. Types of analysis may include (but are not limited to):

- Impact Analysis: What is the environmental, political, economic, financial and social impact of the incident?
- Safety Analysis: What is the impact on nuclear safety and personnel safety functions? Are immediate actions needed to prevent an accident condition or to place the plant in a safe state? Could escalation of this incident increase its severity?
- Technical Characterization: What is the type and nature of the attack? How effective is the current security profile against this type of attack? Is the facility protected from further escalation? In other words, are current security measures sufficient to ensure the incident does not increase in severity?
- Threat Analysis: Analysis of the incident in terms of changes in the threat environment. Is the incident an indicator of aggressive activities from a new adversary? Do the target, tools and tactics indicate a new capability or initiative by an adversary? Thus, does the organization need to update their security position with regards to the threat?

These analyses will assist the leadership and the response teams in characterizing the incident (i.e. according to the severity categories below) and in formulating appropriate priorities for the response (i.e. escalation management).

5.2. SEVERITY CATEGORIZATION

The concept of severity categories helps with communication and the reporting of suspicious computer security incidents. The assessment of a computer security incident and assignment of a severity category provides a means for expressing the actual or potential impact of an incident. While computer security incidents can be categorized in many different ways — by type, manifestation, etc. — assigning a severity category focuses specifically on the impact.

An established international consensus for assigning computer security incidents to severity categories with respect to nuclear security does not yet exist, however the following table provides one example of a possible categorization scheme. This scheme may be adapted for individual organizations and is designed to help in prioritizing response activities and resources. It is recommended that Member States identify an appropriate categorization scheme that addresses their needs.

The severity category ranges from Category 0 (normal operation) up to Category V for the most severe impact.

TABLE 6. GENERAL DESCRIPTION OF SEVERITY CATEGORIES

Severity Category	Description
V	Computer security incidents that result in one or more of the following: — a nuclear safety event; — the theft of nuclear or other radioactive materials; — sabotage of nuclear or other radioactive facilities causing significant physical damage/consequences.
IV	Computer security incidents that result in one or more of the following: — the execution/operation of safety systems (e.g. automatic shutdown), safety procedures (e.g. operator-initiated shutdown), and/or emergency procedures; — the loss or compromise of physical protection system functions; — the loss or compromise of nuclear material accountancy and control functions; — the loss or compromise of nuclear sensitive information that could severely impact nuclear safety and security and potentially support a Category V event.
III	Computer Security incidents that include: — indicators of aggressor activity on internal systems; — indicators of possible reconnaissance activities; — non-directed attacks with minimal impact; — the loss or compromise of nuclear sensitive information that could moderately impact nuclear security and nuclear safety.
II	There is an exploit or activity at another location which could impact nuclear security or nuclear safety. No immediate impact is detected.
I	Detection of a computer security vulnerability that could impact nuclear security or nuclear safety.
0	Normal operation.

Severity categories III to V involve indications that an actual cyber-attack on internal systems has occurred.

Note that the severity categories are related to impact and not to the attack or intrusion vector itself, and that the table and the following description are given only as an example to help organizations report and prioritize a computer security incident response.

5.2.1. Severity Categories V and IV

Category V computer security incidents are those that result in serious breaches of nuclear security and/or nuclear safety. Category V attacks generally have physical consequences.

Category IV computer security incidents are those that may pose an immediate and severe threat to nuclear safety and security objectives. These incidents result in the degradation of security, safety, or operational systems but do not result in total inability of these systems to meet their safety or security functions.

The following list of activities [9] may contribute to Category V and Category IV incidents:

- System Compromise/Intrusion. All unintentional or intentional instances of system compromise or intrusion by unauthorized persons, including user level compromise, root (administrator) compromise, and instances in which users exceed privilege levels.
- Malicious Code. All instances of successful infection or persistent attempts at infection by malicious code — such as viruses, Trojan horses, or worms — that pose a threat to systems or their functions.
- Denial of Service. Intentional or unintentional denial of service (either successfully or persistent attempts to do this) that affects or threatens to affect a system or to deny access to large portions of a network.
- Unplanned Activity. Any unplanned activity that adversely affects one or more sensitive digital assets or related functions for nuclear safety, security or emergency services.
- Unauthorized Use. Any activity that adversely affects an sensitive digital asset or associated system's normal, baseline performance and/or is not recognized as being related to an Operating Unit or a senior management mission. Unauthorized use includes, but is not limited to: port scanning that excessively degrades performance; Internet protocol (IP) spoofing; network reconnaissance; monitoring; compromised servers; or illegal activities.
- Information Compromise. Any unauthorized disclosure of nuclear security information that is released from control to entities that do not require that information in order to accomplish an official organizational function.

5.2.2. Severity Category III

Category III computer security incidents pose potential long term threats to computer security interests or degrade the overall effectiveness of the organization's computer security position. Examples include:

- Attempted Intrusion. A significant and/or persistent attempted intrusion different from daily activity or noise level and which could result in unauthorized access (compromise) if the system is not adequately protected.
- Reconnaissance Activity. Persistent surveillance and resource mapping probes and scans that stand out above the daily activity or noise level and represent activity designed to collect information about vulnerabilities in a network and to map network resources and available services. The parameters for collecting and reporting data on surveillance probes and scans must be documented.

5.2.3. Severity Category II

Category II computer security incidents are exploits or activities that have occurred elsewhere that could impact the security of the nuclear facility in a similar way. The following are examples of these incidents:

- Malware infection in another nuclear facility. If a malware infection is identified in another nuclear facility and the malware target system is one that exists in your facility than this would be considered a Category II computer security incident.

— Exfiltration of nuclear facility network architecture information from another nuclear facility. If network architecture plans were stolen from a nuclear facility that shares sensitive design elements with your facility then that would be considered a Category II computer security incident.

5.2.4. Severity Category I

Category I computer security incidents are detections of computer security vulnerability that could impact nuclear security or nuclear safety. These will generally be events that are detected across the spectrum of incident and event types but that have not yet been attributed to an active attack.

5.2.5. Relation of the severity categories to security levels

Nuclear Security Series No. 17: Computer Security for Nuclear Facilities [3] discusses the assignment of computer security levels to equipment zones based on a graded approach to protection. The aim is to protect all the facility's computer systems that might be subject to malicious acts according to their assigned computer security level. Assignment of the computer systems to the different computer security levels is therefore based on their relevance to safety and security. If this approach is applied, the severity categories for computer security incidents may be linked to the computer security levels.

The severity category of an incident depends on the potential impact (either directly or indirectly) that may result. This impact may be inferred from a system's assigned computer security level. As a result, the link between the computer security levels and the severity categories may provide a quick 'intuitive' approach to identifying the potential impact or consequence of an incident. In this way, the assignment of computer security levels can help to express the severity of incidents.

This mapping provides a starting point for the initial response. Computer security incident analysis will need to consider whether an incident may require elevation to a higher severity category.

Table 7 shows an example of this approach.

TABLE 7. COMPUTER SECURITY LEVELS VS. SEVERITY CATEGORIES

Computer Security Level	Security Level Description	Maximum Severity Categorization
1	Systems that are vital to the facility and require the highest level of security. Incidents involving these systems may lead directly to a breach of a nuclear security or safety objective.	V
2	Systems that require a high level of security. Incidents involving these systems may lead indirectly, though not directly; to a breach of a nuclear security or nuclear safety objective (one protective function remains available).	IV

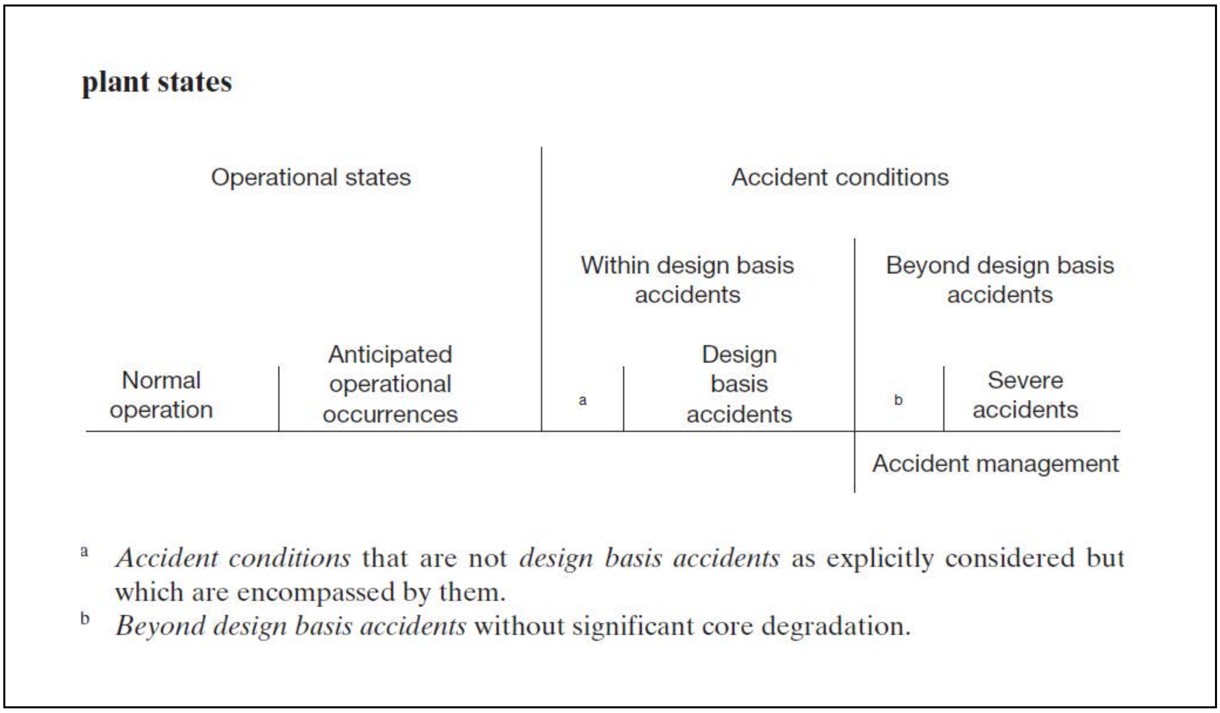
Computer Security Level	Security Level Description	Maximum Severity Categorization
3	Supervision real-time systems not required for operations, which have a medium severity level for various cyber-threats. Incidents involving these systems may be used to prepare for a breach of a nuclear security or safety objective.	III
4	Technical data management systems used for maintenance or operation activity management related to components or systems required by the technical specification for operation, which have a medium severity level for various cyber-threats. Incidents involving these systems may be used to prepare for a breach of a nuclear security or safety objective.	III
5	Systems not directly important to technical control or operational purposes. Incidents involving these systems may be used to support reconnaissance of future activities of adversaries.	III

5.3. THE IMPACT OF COMPUTER SECURITY INCIDENTS ON SAFETY

Nuclear security and nuclear safety have in common the aim of protecting persons, property, society and the environment. Security measures and safety measures have to be designed and implemented in an integrated manner to develop synergy between them and ensure that security measures do not compromise safety and safety measures do not compromise security [1]. Computer security has impact for both nuclear safety and nuclear security.

Computer security incidents (i.e. cyber-attacks) can result in nuclear safety events. Cyber-attacks have been shown to have the ability to modify control system functions within a nuclear facility to inflict physical damage; the Stuxnet malware attack is an example.

For a nuclear reactor (either a power reactor or a research reactor), there are multiple possible plant states, as Figure 3 illustrates. A cyber-attack could potentially place the system in an unanalysed condition that deviates from normal operations. Cyber-attacks may modify the logic, configuration, or set points of an operating system or deceive the operator into performing incorrect actions. The result of these attacks may leave the plant in a state that has not been considered in the design basis analysis, including a state that could lead to accident conditions.



plant states

Operational states		Accident conditions			
		Within design basis accidents		Beyond design basis accidents	
Normal operation	Anticipated operational occurrences	[a]	Design basis accidents	[b]	Severe accidents
				Accident management	

[a] *Accident conditions* that are not *design basis accidents* as explicitly considered but which are encompassed by them.

[b] *Beyond design basis accidents* without significant core degradation.

FIG. 4. Plant states (reactor states)[10].

The IAEA Safety Glossary [10] defines *accident conditions* as "deviations from normal operation more severe than anticipated operational occurrences, including design basis accidents and sever accidents.

Emergency operating procedures (EOPs) are normally developed for the failure of I&C system functions, but EOPs may also be needed to address the mal-operation of systems where the root cause may be malware or computer compromise. The primary goal of EOPs is the protection of individuals, society and the environment from harm from radiological hazards. Nuclear event response and reporting needs to be carried out in accordance with approved national and international guidance. Secondary considerations may be given to response to a computer security incident such as information collection and analysis of the incident.

IAEA Safety Standards Publication, Safety Guide NS–G–2.11[11], paragraph 2.21 states that "Operating experience at the plant shall be evaluated in a systematic way. Abnormal events with significant safety implications shall be investigated to establish their direct and root causes." In today's environment, the possibility of a cyber-attack needs to be considered during such investigations.

Computer security incidents may also be reportable safety events. Examples of possible reportable safety events include (but are not limited to):

- A plant shutdown required by the operational limits and conditions;
- An operation or condition prohibited by the operational limits and conditions;
- Any event or abnormal condition that resulted in the condition of the nuclear installation, including its principal safety barriers, being seriously degraded;
- Any event or abnormal condition that resulted in the manual or automatic operation of the reactor protection system or of engineered safety features;
- Any event in which a single cause or condition or sequence of events resulted in a significant loss of operability in a safety system;

- Any problem or defect in the safety analysis, design, fabrication or operation that has resulted in, or that could result in, an operating condition that had not previously been analysed or that could exceed design basis conditions;
- Any safety significant event during shutdown or refuelling (e.g. the dropping of a fuel assembly);
- Any nuclear event that results in the death of or serious injury to personnel on the site.

A System for the Feedback of Experience for Events in Nuclear Installations NS–G–2.11 [10] similarly provides a description of these events with their reporting and investigation requirements.

While this discussion has focused on nuclear facilities, similar considerations may be given to safety at other nuclear and other radioactive material facilities.

5.4. LOSS OR COMPROMISE OF SENSITIVE INFORMATION

Computer security incidents may result in the compromise or loss of sensitive information. Sensitive information in the context of nuclear security is defined as information whose unauthorized disclosure (or modification, alteration, destruction or denial of use) could compromise nuclear security. Guidance on the identification, protection, and management of nuclear information is further discussed in NSS 23-G [6]. This publication [6] also provides implementing guidance on the investigation of information security incidents.

A computer security incident of this nature may involve:

- The loss or theft of computer equipment or portable media (such as a USB flash drive, DVD, etc.);
- The loss or theft of a mobile phone;
- Unauthorized computer or network access;
- Compromise of password or access control;
- Information collecting malware or hardware such as key loggers, network packet capture, screen capture, or image capture appliances.

While part of the technical analysis will focus on the mechanics of the incident, the analysis must also evaluate its impact. This may consider:

- Who potentially has the information?
- Was the information theft targeted or a random criminal act?
- Is the information available via open source?
- Is the information sensitive in part or as a whole sensitive?
- When was the information lost or compromised?
- What is the time sensitivity of the lost information?
- How could the information be used with malicious intent? What is the potential impact?
- What measures can mitigate the use or impact of such information?
- Who else holds the information and may need to be notified of its compromise?

The sensitivity of the information compromised or lost may dictate the requirements and timeframe for reporting the loss or compromise to competent authorities. Even if the information is not directly related to nuclear security, its nature may mean the incident is governed by national law reporting requirements; examples would be the loss of medical records or other personally identifiable information about individuals.

5.5. THREAT ANALYSIS

Threat analysis is an ongoing process by which intelligence, law enforcement, and open source information is combined with knowledge of an organization's priorities and vulnerabilities to create an evaluation of the threat to the organization. The threat analysis may also describe the motivations, intentions, and capabilities associated with these threats. A computer security incident may be an indication of action or a change of tactics by an adversary or of malicious acts pending or already in progress, and needs to be evaluated with these possibilities in mind. The objective is to determine if the incident identifies a new or changing threat actor regarding tactics, capability and intent.

Questions to consider in the analysis include:

- Does the computer security incident indicate the specific objectives or intent, either short or long term, of the attacker?
- Within the attack cycle, what stage of the attack does the incident indicate (i.e. reconnaissance, exploitation, removal of evidence, etc.)?
- Can the attack be attributed to a known threat actor? If so, does it show a change in tactics or capability for that threat actor?
- Can the incident or attack be linked to similar attacks seen before?
- Is the attack targeted or random?
- How long has the attack been in progress?
- From the nature of the attack and the potential information gained, what is the likely follow-on target?
- What measures are needed to identify the attacker and reach the source of the attack?

5.6. TECHNICAL CHARACTERIZATION

The technical characterization of an attack provides a concise definition of the attack's indicator operational characteristics, potential goal, and impacts. Recording this information in structured format supports analysis, trending, and information exchange. A suggested technical characterization for a computer security incident would include a set composed of the following descriptors. This listing is not intended to be all inclusive; its purpose is to illustrate key characteristics of an attack that may be identified and recorded.

- Impact: {confidentiality, integrity and availability}
- Scope of Impact: {single or multiple organization, national or international impact}
- Classes: {network, policy, configuration, platform, ICS, device}
- Actor: {insider, external}
- Severity Category: {malfunction, degradation of services, loss of confidence, misuse}

— Motivation: {intentional vs. unintentional}

— Compromise Method: {phishing attack, infected web page, USB device, insider, third party, etc…}

Annex VII provides examples of incidents with their technical characterizations.

5.7. ESCALATION LEVELS

The response will not be the same for all computer security incidents and needs to be commensurate with the incident's actual or potential impact to an organization. This section introduces the concept of escalation levels. In many ways this is similar to the severity categories, but the escalation level refers to the level of involvement or response to a particular incident. A computer security incident may escalate in terms of the amount and type of resources required to provide an adequate response. The table below sets out notional escalation levels and possible response profiles.

TABLE 8. POSSIBLE RESPONSE PROFILES FOR DIFFERENT ESCALATION LEVELS

Escalation Level	Description	Role(s) involved
0	Normal Operations. Engineering groups monitoring for security alerts and incident indicators from various sources.	• Technical Assessment
1	Incident Discovery A computer security incident or threat has been discovered. Determine the defensive action to take. If necessary, inform employees of required actions.	• Technical Assessment • Incident Response Coordinator • Communication Role • Impact Analysis Role • Technical Support Role
2	Incident Manifestation A computer security incident or threat has manifested. Determine the course of action for containment and eradication. If necessary, inform employees of required actions.	• Incident Response Management • Incident Response Coordinator • Technical Assessment Role • Technical Support Role • Communications Role • Impact Analysis Role
3	Significant Event The computer security incident or threat is widespread or the impact is significant. Determine the course of action for containment and eradication. Inform employees. Prepare to take legal action.	• Incident Response Management • Incident Response Coordinator • Technical Assessment Role • Technical Support Role • Communications Role • Incident Response Support Role • Impact Analysis Role

The roles in the different escalation levels are discussed in greater detail in the following sections.

5.8. PROCESS FLOW AND ESCALATION

5.8.1. Escalation Level 0

Level 0 represents normal facility or organizational operations. This is the proactive phase of incident response requiring diligence and the investigation of potential threats, possible vulnerabilities, and new attack vectors. The objective is to take proactive measures to ensure that any attack would readily be detected and to facilitate the appropriate attack severity characterization and response. Level 0 activities include:

- Continuous computer system monitoring;
- Monitoring for external alerts and notices about new vulnerabilities and threats.

5.8.2. Escalation Level 1

Level 1 represents the stage at which an indication of some level of computer compromise or malicious activity is first detected. Initial indication may simply be anomalous behaviour of a specific component or system. There may not yet be any adverse impact at this stage. Initial efforts will focus on investigation to determine the nature of the indication and its potential impact, and whether or not there has been an actual attack or if the indication resulted from other factors such as misconfigurations or failure within the control environment. In either case, the root cause of the observed event is identified and steps are taken to prevent the possibility of a similar event in the future. Level 1 activities include:

- Examination and collection of information about the incident;
- Anomaly logging and tracking;
- Triage;
- Determination of whether or not this may be classified as a computer security incident.

If the incident is classified as a computer security incident, the Incident Response Coordinator needs to be notified. The Coordinator will determine the membership of the Technical Analysis and Technical Support teams and, with support from Communication Team personnel, will begin notifying all employees about the incident. This notification is designed to provide employees with information and guidance to reduce their exposure to the threat in the short term. As the Technical Support personnel respond to the incident, the Incident Response Coordinator will work with the Impact Analysis personnel to determine the overall impact of the incident and whether the incident needs to be escalated to Escalation Level 2.

Technical assessment functions:

- Determine the initial defensive action required;
- Notify the Incident Response Coordinator;
- If employee action is required, such as updating anti-virus files, notify the responsible party or organization.

Incident Response Coordinator functions:

- Receive and track all reported potential threats;
- Determine the required membership of the Technical Assessment Team;
- Alert internal organizations and relevant support organizations of the potential threat and any defensive action required;
- Alert the Incident Response Management to the potential threat;
- Alert the Communication Team if internal or external notification is required;
- Escalate the incident response to Level 2 if a report is received indicating that the threat has manifested itself;

- Start a chronological log of events.

Communications functions:

- If employee action is required, notify employees about this.

5.8.3. Escalation Level 2

Once the Incident Response Coordinator and Impact Analysis personnel have decided to escalate the incident to Level 2, the Incident Response Manager is engaged and assumes overall responsibility for the incident.

Level 2 starts as a Level 1 incident, which then becomes Level 2 as a result of the emergence of adverse impact(s). In addition to involvement of the CIRT member in the initial response, the impact conditions may require consultation with a system vendor or security personnel. In many cases a Communications Team will be required to ensure that all appropriate notifications take place. Level 2 activities include:

- Analysis (forensics, evidence collection, recommendations for mitigation);
- Initiation of safety emergency operation procedures where there is a loss of safety function (either actual or perceived);
- Provision of information to the plant operator;
- Mitigation and recovery (by Standard Operating Procedure or ad hoc procedure);
- Damage assessment;
- Documentation and chain of custody;
- Evaluation of the actions taken.

Team activities are similar to Level 1, but will also include greater integration between the various Competent Authorities and Technical Authorities, and may also include parallel activities for a safety and emergency response.

Incident Response Manager functions:

- Direct the incident response activities;
- Provide incident status and advice to the organization’s leadership;
- Escalate the incident to Level 3 if appropriate;
- Determine when the risk has been mitigated to an acceptable level.

Technical assessment functions:

- Determine best course of action for containment of the incident;
- Notify the Technical Support Team of any action required;
- Report actions taken and status to the Incident Response Coordinator.

Incident Response Coordinator functions:

- Notify the Incident Response Management of the manifestation of the threat;
- Alert the Incident Response Support Team about the incident;
- Alert the Extended Team;

— Receive the status from the Technical Assessment Team and report to the Incident Response Management.

Communications functions:

— Inform the organization on behalf of the Incident Response Management;

— Inform the organization’s employees of any action they need to take as determined by the Technical Assessment Team and directed by the Incident Response Management.

Technical support functions:

— Take whatever action as determined by the Technical Assessment Team;

— Report the actions taken, the number of personnel involved, etc. to the Incident Response Coordinator for inclusion in the chronological log.

5.8.4. Escalation Level 3

Level 3 may not have an immediately identifiable impact outside of the local facility, but it differs from Level 2 due to the necessity of contacting the technical authority (such as CERT) for additional expertise. This would often be the case if the attack mechanism is outside of the known body of published computer security bulletins, such as in the case of a ‘Zero Day’ or initial manifestation of malware outside of controlled environments. The technical authority would not only assist in technical characterization and incident resolution, but would also be responsible for ensuring that the required international, government-to-government, communication takes place to deter widespread propagation.

A Level 3 incident has immediate and widespread impact that spreads beyond the sphere of control of the facility or plant’s organization. Not only are the Technical Authorities involved in impact resolution, but governmental officials and law enforcement agents will attempt to determine attribution of the attack for eventual prosecution. It may also be necessary to engage emergency management organizations if there is an inadvertent release of radiation, a threat to special nuclear materials or any other significant event with safety or security ramifications. Level 3 activities include:

— Technical authority level management and decision making;

— Possibly national level management and decision making;

— Criminal investigation;

— International communication.

Team activities are similar to Level 2, but will also include greater integration between the various Competent Authorities and Technical Authorities, and may also include parallel activities for a safety and emergency response.

Incident Response Manager functions:

— Direct incident response activities;

— Provide incident status and advice to the organization’s leadership;

— Determine when the risk has been mitigated to an acceptable level.

Technical assessment functions:

— Continue to monitor all known sources for alerts, looking for further information or actions to take to eliminate the threat;

- Continue reporting the status to the Incident Response Coordinator for inclusion in the chronological log of events;
- Monitor the effectiveness of actions taken and modify them as necessary;
- Update the Incident Response Manager on the effectiveness of actions taken and progress in eliminating the threat.

Incident Response Coordinator functions:

- Assist the Incident Response Manager with executing the incident response;
- Maintain the chronological log of events;
- Record with sequence numbers the status messages that are posted to the incident management repository so these are readily accessible to all personnel requiring current status information.

Communications functions:

- Inform organization employees as directed by the Incident Response Manager.

Technical support functions:

- Continue actions to eradicate the threat as directed by the Incident Response Manager and the Technical Assessment Team;
- Continue to report the actions taken, the number of personnel, etc. to the Incident Response Coordinator for inclusion in the chronological log.

Support functions:

- Contact local authorities if deemed appropriate;
- If local authorities are called in, make arrangements for them to be allowed into the command centre;
- Ensure that all necessary information is being collected to support legal action or financial restitution.

5.8.5. Post-incident activities

After the computer security incident response activities have ceased, it is important to capture knowledge of the incident for process and security improvements. Recommended activities to be performed following the incident include:

Incident Response Manager functions:

- Prepare a report for Executive Management to include:
  - An estimate of the damage/impact;
  - The action taken during the incident (without technical detail);
  - Follow-on actions needed to eliminate or mitigate vulnerability;
  - Policies or procedures that require updating;
  - Actions taken to minimize liabilities or negative exposure;
  - The chronological log and any system audit logs.

- Document the lessons learned and any recommendations for avoiding repetition of the incident, modifying the Computer Security Incident Response Plan accordingly.

Support functions:

- Legal and finance: Work with the local authorities as appropriate if the incident was caused by an external source;
- HR and security: Work with management to determine any necessary disciplinary actions are needed, if the incident was due to an internal source.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Fundamentals: Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011)

[4] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Guide to Industrial Control Systems (ICS) Security, Special Publication 800–82, USA (2011).

[5] COUNCIL OF EUROPE CONVENTION ON CYBERCRIME, Budapest (2001). Available online at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

[8] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Computer Security Incident Handling Guide, Special Publication 800–61 Revision 2, USA (2012).

[9] UNITED STATES DEPARTMENT OF ENERGY, Environmental Management Consolidated Business Center (EMCBC), Subject: Cyber Security Incident Response, IP-240-04, Rev. 2, USA (2010)

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary 2007 Edition, Vienna (2007).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, A System for the Feedback of Experience for Events in Nuclear Installations, IAEA Safety Standards Safety Guide No. NS–G–2.11, Vienna (2006).

GLOSSARY

Terms used in this publication are defined below. When available, definitions are taken from existing IAEA publications or international standards. Where this is the case, the definition includes a reference to the originating publication (listed in the Reference section at the end of the main document).

Competent authority. A governmental organization or institution that has been designated by a State to carry out one or more nuclear security functions. [1]

Competent authorities may include regulatory bodies, law enforcement agencies, customs and border control, intelligence and security agencies, health agencies, etc.

Compromise. The accidental or deliberate violation of confidentiality, loss of integrity, or loss of availability of an information asset.

Malicious act. An act of or attempt at unauthorized removal or sabotage. [2]

Nuclear facility. A facility (including associated buildings and equipment) in which nuclear material is produced, processed, used, handled, stored or disposed of and for which an authorization or license is required.

Nuclear material. Any material that is either special fissionable material or source material as defined in the IAEA Statute, Article XX. [1]

Nuclear security event. An event that has potential or actual implications for nuclear security that must be addressed.

Nuclear security threat. A person or group of persons with motivation, intention and capability to commit criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities or other acts determined by the State to have an adverse impact on nuclear security.

Operator. Any person, organization, or government entity licensed or authorized to undertake the operation of an associated facility or to perform an associated activity.

Other radioactive material. Any radioactive material that is not nuclear material. [1,3]

Radioactive material. Any material designated in national law, regulation, or by a regulatory body as being subject to regulatory control because of its radioactivity. [3]

Risk. The potential that a given threat will exploit the vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the likelihood of an event and the severity of its consequences. [5]

Risk management. The process designed to reduce risk to an acceptable level, and to limit damage resulting from the compromise of information.

Sensitive digital assets. Computer-based systems performing functions that are important to nuclear safety, nuclear security, or nuclear material accountancy and control (NMAC).

Sensitive information. Information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security. [1]

Target. Nuclear material, other radioactive material, associated facilities, associated activities, or other locations or objects of potential exploitation by a nuclear security threat, including major public events, strategic locations, sensitive information, and sensitive information assets.

ANNEX I

INCIDENT INDICATORS

The computer security incident response process is driven by the detection and investigation of events and incidents that indicate a potential threat or compromise. Indicators of such incidents are not limited to the technical domain and may include analysis of process workflow and interaction with personnel across the facility.

The following two lists are of incident indicators. The first list was developed by the multinational IAEA consultancy on computer security incident response. The second is taken from NIST 800–82, Guide to Industrial Control System (ICS) Security [I-1].

Indicators of computer security incidents:

- Abnormal network traffic — data exfiltration;
- Unscheduled modification to the environment;
- Erratic behaviour — increased network latency, additional CPU cycles on the engineer's workstation/operator's console, etc.;
- Undocumented wireless network connectivity;
- Bridged traffic onto the enterprise LAN;
- Escalated access via physical security systems;
- Physical tampering with components;
- Failed login attempts;
- Console versus actual status discrepancies;
- System hashes for valid software builds do not match recorded values;
- Irregularities in consolidated logs;
- Illicit attempts to access sensitive controlled information;
- Theft of engineering design documents or plant personnel records, increased external probes regarding nuclear operations, vendors and plant construction, subcontractors etc. (i.e. anything that can assist an aggressor in achieving an advantage).

NIST 800–82 indicators of computer security incidents:

- Unusually heavy network traffic;
- Out of disk space or significantly reduced free disk space;
- Unusually high CPU usage;
- Creation of new user accounts;
- Attempted or actual use of administrator level accounts;
- Locked-out accounts;
- Cleared log files;
- Full log files with an unusually large number of events;
- Antivirus or IDS alerts;
- Disabled antivirus software and other security controls;

- Unexpected patch changes;
- Machines or intelligent field devices connecting to;
- Requests for information about the system (social engineering attempts);
- Unexpected changes in configuration settings;
- Unexpected system shutdown;
- Stoppage or displayed error messages on a web, database, or application server;
- Unusually slow access to hosts on the network;
- Filenames containing unusual characters or new or unexpected files and directories;
- Auditing configuration changes;
- A large number of bounced emails with suspicious content;
- Unusual deviation from typical network traffic flows;
- Erratic ICS equipment behaviour, especially when more than one device exhibits the same behaviour;
- Any apparent override of safety, backup, or failover systems;
- Equipment, servers, or network traffic that has bursts of temporary high usage when the operational process itself is steady and predictable;
- Unknown or unusual traffic from corporate or other network external to control systems network;
- Unknown or unexpected firmware pulls or pushes.

REFERENCE

[I-1] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, “Guide to Industrial Control System (ICS) Security (Final Public Draft)”, Special Publication 800–82, USA (2008), pp 6–19.

ANNEX II

INCIDENT ANALYSIS GUIDE

This Annex describes categories of incident information that may be used to assess and measure the attributes of a threat. A computer security incident may be the manifestation of a malicious act. The motivation behind this act and its perpetrators are not often readily evident. Analysis of the incident in terms of threat actors is important not only in helping to identify the motive, but also to identify changing threat characteristics, tactics, and potential follow-on activities.

This material has been developed from guidance provided in Cyber Threat Metrics [II-1].

Incident characteristics

— What type of incident occurred (e.g. website defacement, denial of service, unauthorized access, reconnaissance/probing)?

— If malicious software (e.g. a virus or Trojan) was involved in the incident, was its purpose:

- Command and control (C&C)?
- Remote access?
- Data exfiltration?
- Data manipulation?
- Activity monitoring?

Target system characteristics

— Was the level of security protection on the target system:

- High — fully protected using access control, file monitoring, up-to-date patches, etc.?
- Moderate — some protections implemented?
- Low — very limited protections implemented?

Timeline

— What is the date of initial activity related to incident?

— What is the most recent date of activity related to incident?

— On what date was the incident detected?

Covert activity

— Was activity related to the incident identified by:

- Network monitoring?
- A monitoring application (e.g. an intrusion detection system or anti-virus software)?
- A system administrator?
- A system user?

— Were identified activities immediately associated with the incident? Or were identified activities originally dismissed as false alarms?

— Were event logs or timestamps modified or deleted to obfuscate activity associated with the incident?

— Were file/disk deletion tools involved in the incident?

— Were incident activities related to the reconnaissance, probing, execution, or exploitation stages of attack?

Attack vector

— Was the incident facilitated by:

- Phishing?
- Social engineering (other than phishing)?
- Remote access (e.g. VPN or modem)?
- Inside access?

— If the attack was facilitated by any type of social engineering, including phishing, was it a targeted, individual approach or a broad blanketing approach?

Attack sophistication

— Was more than one computer system affected by this incident?

— Was the internal network accessed on multiple occasions during this incident?

— Were activities associated with the incident novel in any way (i.e. a zero-day attack) or common (i.e. easily acquired toolsets)?

Anti-virus signature

— Does an anti-virus signature (from any vendor) exist for any malicious software involved in the incident?

— If so, did the signature exist and was it widely available on the date of initial activity?

— Physical interaction:

- Was the system physically accessed as part of the incident?
- Was the incident facilitated via the introduction of a physical medium (e.g. USB drive, CD, hardware)?
- Did the incident result in any physical, real-world effects?

Obfuscation

— Was any of the malicious software involved encrypted or packed?

— Was any activity, function or script injected into another for malicious purposes?

Data compromise

— Was data compromised (e.g. manipulated, exposed or deleted) in relation to the incident? If so,

- What type of data (e.g. OUO, PII, SUI or UCNI) was compromised?

  - Did compromised data affect system operation or mission?

- — Was data exfiltrated as part of the incident? If so,
  - What type of data (e.g. password hashes, PII, OUO, UCI, proprietary, military, security) was exfiltrated?
  - Was data exfiltrated on multiple occasions?
  - Was data encrypted as part of the exfiltration process?

Attribution

- — Is it possible to definitively attribute the activities associated with the incident to a specific actor?
- — Has any group or individual claimed responsibility for the incident?
- — If so, was the statement public or private? Was the statement a general, specific, or limited declaration?
- — Has any group or individual made a targeted threat statement against the victim organization?
- — Were hop-points used? If so, how many?
- — Frome where did the attack originate?

REFERENCE

[II-1] Mateski, M., et al., Cyber Threat Metrics, Sandia Report SAND2012–2427, March 2012.

ANNEX III

SPECIAL CONSIDERATIONS FOR INDUSTRIAL CONTROL SYSTEMS

Industrial control systems represent unique operating environments that may require special considerations in responding to a computer security incident. The following list identifies possible considerations for planning and response.

- A computer attack may lead to physical consequences in the operating environment;
- The response must first focus on maintaining safety and the prevention of unacceptable radiological consequences;
- The computer security incident response may only be part of wider response activities for attacks that concern safety or the unauthorized access to nuclear materials;
- Facility control system designs and modifications need to include considerations specific to computer security;
- Multiple modes of operation are available to facilitate bringing a nuclear power plant to a safe condition following a cyber-attack;
- Industrial control systems often include dependencies on critical secondary infrastructure, which must also be considered in light of a cyber-attack. Attacks on these secondary systems and infrastructure can often directly impact primary functions;
- The computer security incident response may require facility or operations environment specific training;
- The Computer Security Incident Response Team will need to include systems engineers, pre-approved tools (tested for operational impact) and acceptable processes;
- Computer security must be considered with regards to the overall site security plan;
- Computer security scenarios need to be included as part of facility security and safety exercises;
- Computer security needs to be integrated into the plant operational and safety culture; to be successful this requires a fusion of physical security, network, enterprise server, computer, plant operations etc.;
- An evaluation of business continuity impact needs to be performed on potential computer response actions involving sensitive digital assets;
- It is vital to validate all responders against pre-approved credentials and background checks;
- The response team will need to include system engineers, I&C Engineers, and computer specialists.

ANNEX IV

INCIDENT SCENARIOS

Improving computer security incident response capabilities not only requires a thorough understanding of the core technology and how it is used to detect incidents, but benefits from an understanding of the context of the incident within an attack scenario. It is often difficult to understand incidents outside of the attack context. Why did that control system component working but yet produce no failure event? What are these seemingly innocuous packets trying to escape from my network every day at 13.00? For this reason we present here several computer security incident scenarios that will help to put computer security incidents in context.

IV-1. POSSIBLE INCIDENT SCENARIOS

There are many possible incident scenarios that could impact a facility. Methods by which system operation could be compromised in various ways include:

- Disruption by delaying or blocking the flow of information through corporate or control networks;
- Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, changes to alarm thresholds, or unauthorized commands issued to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), causing an environmental incident, or even disabling control equipment;
- False information sent to authorized nuclear operators either to disguise unauthorized changes or to initiate inappropriate actions by authorized nuclear operators;
- Modification of sensitive digital asset software or configuration settings, producing unpredictable results;
- Interference with safety systems operation;
- Malicious software (e.g. virus, worm, Trojan horse) introduced into the system containing sensitive digital assets;
- Electronic or paper-based procedures or work instructions modified to bring about damage to products or equipment, or harm to personnel;
- Physical breaching of control systems at unstaffed remote sites and may not be physically monitored. If such remote systems are physically breached, the adversaries could establish a trusted connection back to a control network containing sensitive digital assets.

IV-2. POTENTIAL ATTACK VECTORS

Potential attack vectors include:

- An infected laptop used for the maintenance and configuration of control systems components connected to the system;

- Removable media and mobile devices that interface with sensitive digital assets;
- A subcontractor performing maintenance activities who remotely infects systems through his remote system;
- Rogue wireless connections to systems or sensitive digital assets;
- Loss of access control for onsite third party maintenance personnel who have unescorted access to I&C components. These datasets may exist on the enterprise systems and not the engineering systems themselves and so are more readily available to an inside activist;
- Compromise of remote data links used for persistent site monitoring;
- Loss of access control and accountability for electronic parts and repair components;
- Lack of a security culture regarding the introduction of malware and the recognition and response to computer compromise;
- Unauthorized use of known vendor backdoor accounts or hard-coded passwords.

ANNEX V

INCIDENT REPORTING

When reporting a computer security incident, it is important to capture the relevant characteristics of the compromise as well as the circumstances that surround the discovery of the incident. This section lists incident reporting details that are commonly collected during the computer security incident response process. This information applies to both internal and external investigations. It is important that specific protocols for information release be followed which identify the exact information to be released, whom is authorized to release the information, to whom can the information be released, and under what circumstances the information can be released. Not all information will apply to every incident.

Category	Example
Incident report classification.	Sensitive, Classified, etc.
Name of organization.	
Contact information for the incident (name, telephone, email address).	
Physical location of the affected computer/network.	
Classification level of the compromised system.	Classified, Unclassified, Secret, Sensitive.
Date of the incident.	
Time of the incident (including time zone).	
Description of the affected critical infrastructure.	
Type and impact category.	Intrusion: Moderate impact. Denial of service: High impact.
Internet Protocol (IP) addresses and domain names affected.	
IP addresses and domain names of the attack's origin.	
Operating system of affected host(s).	
Functions of affected host(s).	
Number of affected hosts.	
Suspected method of intrusion / attack.	
Suspected perpetrators and/or possible motivation.	
Evidence of spoofing.	

Category	Example
Application software affected.	
Description of the security infrastructure in place at the time of the incident.	
Did the intrusion or incident result in the loss or modification of information?	
If private personnel information was involved, have affected organizations and individuals been notified?	
Evidence of damage to the affected system(s) including the level / extent of unauthorized access.	
Description of any adversary tactics, techniques and procedures (TTPs).	
Which vulnerabilities were exploited, if applicable?	
Description of investigation actions and mitigation efforts.	
Last time the affected system(s) were modified or powered up.	
Assessment of incident impact.	
Status of anti-virus: version and last update.	
Methodology for identifying incidents.	IDS, audit log analysis, system administrators.

ANNEX VI

EVIDENCE COLLECTION

An incident response needs to consider collection of evidence for post-response analysis and law enforcement investigation. “Forensic computing is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable.” [VI-1]

VI-1. RULES OF FORENSIC INVESTIGATION

When conducting computer forensic examinations there are certain rules that must be applied to your investigation. [VI-2]

Minimal handling of the original

This can be regarded as the most important rule in computer forensics. Where possible, make duplicate copies of the evidence and use the duplicates for examination. In doing this, the copy must be an exact reproduction of the original, and you must also authenticate the copy, otherwise questions may be raised over the integrity of the evidence.

Account for any change

In some circumstances changes to the evidence may be unavoidable. For instance, booting up or shutting down a machine can result in changes to the memory, and/or temporary files. Where changes do occur, the nature, extent and reason for the changes must be documented.

Comply with the rules of evidence

The rules of evidence are the rules investigators must follow when handling and examining evidence, to ensure the evidence they collect will be accepted by a court of law.

Do not exceed your knowledge

Do not proceed with an investigation if it is beyond your level of knowledge and skill. If you find yourself in this situation, then seek assistance from someone with more experience, such as a specialist investigator, or if time permits, obtain additional training to improve your knowledge and skills. It is advisable not to continue with the examination as you may damage the outcome of the case.

VI-2. EVIDENCE COLLECTION

Matthew Braid, in his AusCERT paper *Collecting Electronic Evidence After a System Compromise* [VI-3], has compiled a list of five rules of evidence that need to be followed in order for evidence to be useful, explaining them in an easy to understand way. He explains the rules of evidence as follows:

Admissible

This is the most basic rule — the evidence must be able to be used in court or elsewhere. Failure to comply with this rule is equivalent to not collecting the evidence in the first place, except the cost is higher.

Authentic

If you can't tie the evidence positively to the incident, you can't use it to prove anything. You must be able to show that the evidence relates to the incident in a relevant way.

Complete

It is often not enough to collect evidence that just shows one perspective of the incident. Not only do you need to collect evidence that can help prove the attacker's actions but for completeness it is also necessary to consider and evaluate all evidence available to the investigators and retain that which may contradict or otherwise diminish the reliability of other potentially incriminating evidence held about the suspect. Similarly, it is vital to collect evidence that eliminates alternative suspects. For instance, if you can show the attacker was logged in at the time of the incident, you also need to show who else was logged in and demonstrate why you think they didn't do it. This is called Exculpatory Evidence and is an important part of proving a case.

Reliable

Your evidence collection and analysis procedures must not cast doubt on the evidence's authenticity and veracity.

Believable

The evidence you present needs to be clear, easy to understand and believable by a jury. There's no point presenting a binary dump of process memory if the jury has no idea what it all means. Similarly, if you present them with a formatted version that can be readily understood by a jury, you must be able to show the relationship to the original binary, otherwise there's no way for the jury to know whether you've faked it.

In addition to the guidance provided above, the following may be considered in regards to evidence collection:

- Develop a continuous activity log to track all activities during the incident;
- Ensure that important investigative elements are properly time stamped and the time source is known to be good and in sync with the rest of the network resources;
- Track everyone who has had access to the information;
- Preserve network dumps and memory dumps (if possible) during the incident;
- Determine whether to isolate and keep the compromised system running until forensics can be performed. This will depend on the nature of the system in question;
- Pre-determine before the incident occurs the nature of evidence to be collected. It is advised that this aspect is coordinated with the respective law enforcement agency;
- Collect the logs and performance information prior to and after the security incident for further analysis.

The U.S. Department of Homeland Security, Industrial Control System CERT prepared a two-page guide on Preparing for Computer Incident Analysis. [VI-4] The guide includes details on establishing systems analysis capabilities, operational preparation, and the importance of logging and preserving forensic data. The recommendations from this paper include:

— Keep detailed notes of what is observed, including dates/times, mitigation steps taken/not taken, whether device logging was enabled/disabled, and machine names for suspected compromised equipment. More information is generally better than less information;

— When possible, capture live system data (i.e. current network connections and open processes) prior to disconnecting a compromised machine from the network;

— Capture forensic images of the system memory and hard drive prior to powering down the system;

— Avoid running any antivirus software 'after the fact' as the AV scan changes critical file dates and impedes discovery and analysis of suspected malicious files and timelines;

— Avoid making any changes to the operating system or hardware, including updates and patches, as they will overwrite important information about the suspected malware.

REFERENCES

[1] McKemmish, Rodney. "What is Forensic Computing", Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice, June 1999. Available online at: <http://aic.gov.au/documents/9/C/A/%7B9CA41AE8-EADB-4BBF-9894-64E0DF87BDF7%7Dti118.pdf>

[2] Ryder, Karen. "Computer Forensics — We've Had an Incident, Who Do We Get to Investigate?". SANS Institute InfoSec Reading Room, 2002. Available online at: <http://www.sans.org/reading-room/whitepapers/incident/computer-forensics-weve-incident-investigate-652>

[3] Braid, Matthew. "Collecting Electronic Evidence After a System Compromise", 2001, Available online at: < https://www.auscert.org.au/download.html?f=22>

[4] United States Department of Homeland Security, "Preparing for Cyber Incident Analysis", 2008. Available online at: <https://ics-cert.us-ce rt.gov/sites/default/files/DHS_CyberSecurity_CSSP-Incident_Handling-v10.pdf>

ANNEX VII

EXAMPLES OF TECHNICAL CHARACTERIZATIONS

This Annex contains examples of technical characterizations to refer to when performing the environment analysis in support of drafting a computer security incident response plan. Each example includes a description and an assignment of characteristics to a proposed set of categories including: impact, scope of impact, classes, actor, severity level, motivation and method of compromise.

VII-1. EXAMPLE 1

An indicator warning arrives from the CERT with details that a new malware sample has been seen in the wild and among its many signatures, infected systems beacon to a specific Internet address. The threat operations cell notifies the networking team to update their auditing filters and network sensors to look for connections to this external address. Later that day multiple alerts are triggered and it is determined that three systems have been infected. The infected systems are all part of the finance group on a network segmented from any plant operations. After further analysis the captured network data is scanned and a file attached to 10 emails matches the hash of the malware payload. The security operations centre creates the following technical characterization of the threat:

Impact:	Confidentiality and Integrity
Scope of Impact:	Single Organization
Classes:	Network, Policy, Configuration and Platform
Actor:	External
Severity Level:	Type 2 — Loss of Confidence (of the financial systems, not the operational part of the plant yet).
Motivation:	Intentional (given the CERT alert trigger)
Compromise Method:	Spear-phishing.

VII-2. EXAMPLE 2

A control board on a computer system experiences a sudden critical failure. Plant operators immediately notice that a critical piece of equipment goes offline and initiates the process for bringing the backup services online. The operator in charge of that piece of equipment connects the maintenance laptop to the control system and downloads the log files and system dump that is available. While she analyses the audit records she passes the system dump to the TA since they have the capability to analyse the file. While the file is being analysed, the system operator notices in the log file a series of messages indicating the core temperature of the device is increasing at a steady rate until the control board fails. A few minutes later the TA calls and states that they found a process resident in memory when the system crashed that may be associated with a known SCADA attack. The security operations centre created the following technical characterization of the threat:

Impact:	Integrity and Availability
Scope of Impact:	Single Organization (with the potential for a national impact if the critical service is not restored to capacity).
Classes:	ICS, Device
Actor:	Unknown at this time

Severity Level:	Type 1 — Degradation of Services and Loss of Confidence*
Motivation:	Intentional
Compromise Method:	Unknown at this time.

* Assuming the malfunction is a non-malicious event. If malfunctions are thought to be malicious, then update appropriately.

VII-3. EXAMPLE 3

The computer security operations centre starts to receive calls about once an hour from users who state that a person called them claiming to be the security administrator requesting that they provide their password to him for system maintenance and account verification. The security team immediately sends an email to all users reminding them never share their password to anyone. No users report having shared their password.

Impact:	Integrity
Scope of Impact:	Single Organization (with the potential for multiple organizations if a user at more than one facility reuses their password).
Classes:	Policy
Actor:	Likely External but still not sure
Severity Level:	Type 3 — Aggressor Activity Detected
Motivation:	Intentional
Compromise Method:	No compromise identified yet.

ANNEX VIII

EXAMPLE OF A COMPUTER SECURITY INCIDENT RESPONSE POLICY

{This Annex provides organizations with a template for developing their computer security incident response policy. If used, organizations need to customize the policy to fit their specific organizational needs. Text in square brackets [ ] needs to be adapted for the specific organization, while text in curly brackets { } constitutes explanatory information which is to be removed.}

I. Policy objectives and purpose

Maintaining nuclear safety and security against possible threats is a top operational priority at ***[Organization Name]***. In today's environment, it is essential to consider the threat of computer-based attacks.

We recognize that safety and security at ***[Organization Name]*** relies in part on a comprehensive defence-in-depth computer security programme. All our employees are a vital part of this programme.

[Organization Name] must be able to respond to a computer security incident in a manner that maintains nuclear safety and security. This includes the protection of sensitive information and information assets.

This Computer Security Incident Response Policy is designed to provide a well-defined, systematic approach for taking appropriate action when computer-based attacks are detected or there is a violation of the computer security policy.

This Policy with its associated procedures constitute the Computer Security Incident Response Plan, which sets out the organizational priorities, specific technical processes, techniques, checklists, and forms used for incident response. One of the primary functions of the computer security incident response plan is to ensure the integrity and rapid restoration and recovery of essential system functions associated with safety, security, material accountancy and control, and emergency preparedness.

II. Scope of the policy

This Policy applies to all employees, who are responsible for protecting information and computer systems at ***[Organization Name]*** and reporting suspicious behaviour and incidents. If an employee identifies an incident or potential suspicious behaviour, they must first take action to establish a safe and secure situation, and second to notify the Computer Security Officer or other designated management. Operating procedures may define requirements and processes for a computer incident response associated with specific systems, e.g. for engineering or security systems.

III. Computer security incidents

A Computer Security Incident is any event that potentially or actually impacts computer systems or computer networks. A computer security incident also includes the act of violating an explicit or implied computer security policy.

Examples of incidents include:

- attempts (successful or failed) to gain unauthorized access to a system or its data
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

IV. Computer Security Incident Response Team (CSIRT)

[Organization Name] has established a Computer Security Incident Response Team (CSIRT). The CSIRT is an organized response component to provide computer security incident response services. This team consists of a predefined set of individuals covering a range of capabilities, with defined response activities and authorities for the duration of the incident. While it is every employee’s responsibility to establish a safe and secure state during a computer security incident, the CSIRT will identify and lead the processes deemed necessary to contain, mitigate or resolve the issues of concern.

The CSIRT is led by the Computer Security Officer (CSO). The CSIRT consists of a core group of specialists across a range of disciplines. Additional specialists may be added based upon the nature of the incident and potential impact.

The core members of the CSIRT include:

- The Computer Security Officer
- [network engineer]
- [engineering department representative]
- [physical security system administrator]
- [communications representative]
- [safety engineer]

{Note that some of these individuals may be subcontracted subject matter experts to support specific technical skills lacking in the workforce.}

The responsibilities of the CSIRT include but are not limited to:

- Establishing an incident log and capturing all relevant information as the response activity progresses;
- Determining the nature and scope of the incident;
- Determining the potential impact of the incident;
- Ensuring internal and external reporting as required;
- Escalating to executive management as appropriate;
- Recommending a response and taking action as directed by executive management;
- Contacting and involving additional departments as appropriate;
- Monitoring the progress of the response;
- Evidence gathering for law enforcement as appropriate;
- Documentation of a summary of the incident and the restorative action taken;
- Exploration/implementation of mitigation to defend from future attacks;

- Providing training on incident response;
- Conducting periodic exercises on incident response.

V. Communication

During a computer security incident, communication is a key element of a coordinated response. This includes internal and possibly external reporting requirements. As part of the computer security incident response procedures the CSO needs to develop a communications plan covering the required reports and reporting criteria.

The CSIRT is also responsible for incident communication, ensuring that the appropriate information is passed to senior management, law enforcement agents, the regulatory body, etc. The communication plan identifies the appropriate points of contact and contact details for the relevant competent authorities and technical authorities.

VI. Training and exercise requirements

One of the most vital elements both in preventing and in responding to a computer security incident are the people who work in ***[Organization Name]***.

A key component of this Computer Security Incident Response Policy is the establishment of a computer security awareness training programme. On initial access to computer systems and periodically thereafter, all employees will be trained on computer security incident prevention, recognition and response. This training may be tailored to meet the specific requirements for each department.

Technical staff will receive additional training as required to support prevention, response, analysis, and mitigation of computer security incidents.

[Organization Name] will conduct periodic training exercises to test the incident response process. These exercises will focus not only on technical procedures, but on the whole response process including communication requirements with the competent authority and technical authorities.

ORDERING LOCALLY

In the following countries, IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

BELGIUM
Jean de Lannoy
Avenue du Roi 202, 1190 Brussels, BELGIUM
Telephone: +32 2 5384 308 • Fax: +32 2 5380 841
Email: jean.de.lannoy@euronet.be • Web site: http://www.jean-de-lannoy.be

CANADA
Renouf Publishing Co. Ltd.
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: http://www.renoufbooks.com

Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

CZECH REPUBLIC
Suweco CZ, s.r.o.
SESTUPNÁ 153/11, 162 00 Prague 6, CZECH REPUBLIC
Telephone: +420 242 459 205 • Fax: +420 284 821 646
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FRANCE
Form-Edit
5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: fabien.boucard@formedit.fr • Web site: http://www.formedit.fr

Lavoisier SAS
14 rue de Provigny, 94236 Cachan CEDEX, FRANCE
Telephone: +33 1 47 40 67 00 • Fax: +33 1 47 40 67 02
Email: livres@lavoisier.fr • Web site: http://www.lavoisier.fr

L'Appel du livre
99 rue de Charonne, 75011 Paris, FRANCE
Telephone: +33 1 43 07 43 43 • Fax: +33 1 43 07 50 80
Email: livres@appeldulivre.fr • Web site: http://www.appeldulivre.fr

GERMANY
Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28
Email: kundenbetreuung.goethe@schweitzer-online.de • Web site: http://www.goethebuch.de

HUNGARY
Librotrade Ltd., Book Import
Pesti ut 237. 1173 Budapest, HUNGARY
Telephone: +36 1 254-0-269 • Fax: +36 1 254-0-274
Email: books@librotrade.hu • Web site: http://www.librotrade.hu

INDIA
Allied Publishers
1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell
3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: http://www.bookwellindia.com

ITALY
Libreria Scientifica “AEIOU”
Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Web site: http://www.libreriaaeiou.eu

JAPAN
Maruzen-Yushodo Co., Ltd.
10-10, Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Telephone: +81 3 4335 9312 • Fax: +81 3 4335 9364
Email: bookimport@maruzen.co.jp • Web site: http://maruzen.co.jp

RUSSIAN FEDERATION
Scientific and Engineering Centre for Nuclear and Radiation Safety
107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION
Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59
Email: secnrs@secnrs.ru • Web site: http://www.secnrs.ru

UNITED STATES OF AMERICA
Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Co. Ltd.
812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: http://www.renoufbooks.com

Orders for both priced and unpriced publications may be addressed directly to:

IAEA Publishing Section, Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

16-18041

International Atomic Energy Agency
Vienna
ISBN 978–92–0–104416–7