TECHNICAL SPECIFICATION

ISO/IEC TS 27100

First edition
2020-12

Information technology — Cybersecurity — Overview and concepts

Reference number
ISO/IEC TS 27100:2020(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Cybersecurity is a broad term used differently through the world.

Cybersecurity concerns managing information security risks when information is in digital form in computers, storage and networks. Many of the information security controls, methods, and techniques can be applied to manage cyber risks.

ISO/IEC 27001 provides requirements for information security management systems. The focus of ISO/IEC 27001 is on security of information, and associated risks, within environments predominantly under the control of a particular organization. Cybersecurity focuses on the risks in cyberspace, an interconnected digital environment that can extend across organizational boundaries, and in which entities share information, interact digitally and have responsibility to respond to cybersecurity incidents.

Information technology — Cybersecurity — Overview and concepts

1 Scope

This document provides an overview of cybersecurity.

This document:

— describes cybersecurity and relevant concepts, including how it is related to and different from information security;

— establishes the context of cybersecurity;

— does not cover all terms and definitions applicable to cybersecurity; and

— does not limit other standards in defining new cybersecurity-related terms for use.

This document is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
cyber attack
attack
malicious attempts to exploit vulnerabilities in information systems or physical systems in *cyberspace* (3.5) and to damage, disrupt or gain unauthorized access to these systems

Note 1 to entry: Expression of an offensive operation in or through the cyberspace leading to unauthorized use of services, creating illicit services, orchestrating denial of service, altering or deleting data or resources.

3.2
cybersecurity
safeguarding of people, society, organizations and nations from cyber *risks* (3.7)

Note 1 to entry: Safeguarding means to keep cyber risks at a tolerable level.

3.3
cybersecurity event
occurrence indicating a possible breach of *cybersecurity* (3.2) or failure of controls

[SOURCE: ISO/IEC 27035-1:2016, 3.3, modified — In the term and the definition, “information security” has been replaced with “cybersecurity”.]

3.4
cybersecurity incident
one or multiple related and identified *cybersecurity events* (3.3) that can harm people, society, organizations or nations

[SOURCE: ISO/IEC 27035-1:2016, 3.4, modified — In the term and the definition, “information security” has been replaced with “cybersecurity”. In the definition, new wording has been added after "harm".]

3.5
cyberspace
interconnected digital environment of networks, services, systems, people, processes, organizations, and that which resides on the digital environment or traverses through it

Note 1 to entry: Interconnected digital environment that traverses public infrastructure e.g. the internet, rather than parts of the organisation’s internal network or air-gapped digital environments that may not traverse public infrastructure.

[SOURCE: ISO/IEC 27102:2019, 3.6, modified — In the definition, the part after "processes" has been added.]

3.6
cyber threat
potential cause of an unwanted *cybersecurity incident* (3.4), which can result in harm to a system, people, society, organization, or other entities in *cyberspace* (3.5)

[SOURCE: ISO/IEC 27000:2018, 3.74, modified — The term “threat” has been replaced with “cyber threat”. In the definition, “incident” has been replaced with “cybersecurity incident”, and new wording has been added after "system".]

3.7
risk
effect of uncertainty on objectives

Note 1 to entry: Cyber risk can be expressed as effect of uncertainty on objectives of entities in *cyberspace* (3.5).

Note 2 to entry: Cyber risk is associated with the potential that threats will exploit vulnerabilities in cyberspace and thereby cause harm to entities in cyberspace.

[SOURCE: ISO/IEC 27000:2018, 3.61, modified — Notes 1 to 6 to entry have been replaced.]

4 Concepts

4.1 Cyberspace

Cyberspace is a complex environment based on digital technologies that provides a global place for digital interaction among people including formal and informal interactions with public or private entities such as businesses, governments, non-profit organizations and other groups. Cyberspace is public but as individual components of cyberspace are owned by a variety of entities, it can be considered both public and private space. People and entities interact in cyberspace for many different purposes. This interaction is manifested as sharing, exchange, processing or receipt of information.

Any interaction taken in cyberspace by an individual or an entity potentially has a near-instantaneous impact anywhere in the world.

While interactive actions in cyberspace create knowledge and power, the following features of cyberspace can bring both advantageous and adverse consequences:

a) cyberspace is borderless;

b) anyone can enter and leave cyberspace freely or at a very low cost;

c) cyber actors can be anonymous or obfuscated; and

d) a threat agent can be anywhere in cyberspace from the opposite side of the globe to a close neighbour of the target.

An action in cyberspace and its impacts can be asymmetric. The originating action can have consequences disproportionate in difficulty and cost of counteraction. In order to take advantage of cyberspace, it is important to prevent adverse consequences, that is, to ensure cybersecurity.

4.2 Cybersecurity

The objective of adequate cybersecurity is to maintain an acceptable level of stability, continuity and safety of entities operating in cyberspace. While it is not possible to always achieve these objectives, cybersecurity aims to reduce cyber risks to a tolerable level.

Areas of concern for cybersecurity include:

a) stability and continuity of society, organizations and nations;

b) property (including information) of people and organizations; and

c) human lives and health.

Cybersecurity with these characteristics is implemented by individual organizations. In cyberspace, organizations need to consider not only themselves, but also other parties who share cyberspace. While an organization needs to manage its vulnerabilities to ensure that the organization does not adversely affect other actors, it needs to work with others to reduce cyber risks. In addition, cybersecurity needs to reduce social and human losses in real space caused by cybersecurity incidents in cyberspace. Therefore, immediate detection and appropriate response of information security incidents are important elements of cybersecurity.

5 Relationship between cybersecurity and relevant concepts

5.1 Relationship between information security and cybersecurity

Information security and cybersecurity have different perspectives and concerns while they are closely related and overlapping.

Information security is defined in ISO/IEC 27000 as “preservation of confidentiality, integrity and availability of information”. It primarily deals with information. The definition is general and does not specify its application and subject entity. Once an entity with its context is determined as subject of information security, concerns of information security can be established, e.g.;

a) confidentiality of information that has value to an organization;

b) integrity and availability of information that is critical to business operation;

c) availability of information and communication technology (ICT) infrastructure on which business processes depend; and

d) reliable and trusted delivery of ICT services.

Breach of information security in cyberspace can cause a cybersecurity incident. This means that the information security risks are viewed as cyber risks in the context of cybersecurity. However,

cybersecurity and information security differ in their objectives. Cybersecurity is primarily concerned with protecting entities including people, society, organizations and nations from cyber risks (see 4.2), while information security addresses maintaining confidentiality, integrity and availability of information with consequences.

Cyberspace can contain information systems controlling physical devices and systems. Compromising information security of these connected information systems via the cyberspace can have implications on society or individuals. Cybersecurity reduces the likelihood of such events.

In order to reduce social, human and economic impacts caused by cybersecurity incidents, entities who connect to cyberspace have a responsibility for collectively managing cyber risks including sharing information about cyber risks, implementing protective controls, monitoring and detecting potential incidents, and cooperating in response and recovery from incidents. Activities of information security are performed by an entity that handles the information to reduce its own risks. However, cybersecurity is performed by an entity to address not only its own risks, but also risks of the other entities that are directly or indirectly involved. Those entities can reside anywhere in cyberspace.

5.2 Relationship between ISMS and cybersecurity

5.2.1 Cyberspace as a field of risk sources for an ISMS

An information security management system (ISMS) is applicable within an organization with interfaces and interactions with external entities. Specifically, the scope of the ISMS and the scope of risk identification are within an organization [see ISO/IEC 27001:2013, 4.3 and 6.1.2 c)]. Information security objectives (see ISO/IEC 27001:2013, 6.2) aim at protection of information that has value to the organization or of the information of other entities that are in custody of the organization.

Cybersecurity transcends the boundaries and control of an organization because of the interconnectedness of cyberspace. Organizations frequently interface and interact with external entities by using cyberspace. As such, the use of cyberspace represents risks to the organization that need to be managed as a part of an organization's ISMS. If the organization has an ISMS, cyberspace shapes part of context of the ISMS as referred to in ISO/IEC 27001:2013, 4.1. Threat vectors that originate in cyberspace can expose the organization to information security risks. The organization identifies risks from threats in cyberspace, along with other risks, during the process of risk identification as required in ISO/IEC 27001:2013, 6.1.2 c).

5.2.2 ISMS in support of cybersecurity

An ISMS provides a mechanism for organizations to use a risk-based, prioritized, flexible and communications-enabling approach to manage information security risks based on their business needs. An organization can operate its ISMS as a means of managing cyber risks. This is facilitated by a consistent and iterative approach to identifying, assessing and managing risk and evaluating implementation of the ISMS. An ISMS as described in ISO/IEC 27001 is applicable regardless of an organization's size and should reflect a clear understanding of the organization's particular business drivers and security considerations. An ISMS facilitates communication about the implementation of desired outcomes and associated information security activities across the organization, from the top management level by using the management system requirements, to the implementation and operations levels by using the controls. The application of ISMS does not only provide a clear and understandable set of controls as an outcome but also provide a clear scope, boundaries and dependencies of cybersecurity activities in the organization.

An example of using an ISMS in support of cybersecurity is the use of ISO/IEC 27001 with ISO/IEC 27019 to establish, implement, maintain and continually improve an ISMS for the energy utility supplier. The ISMS supports the stability of the energy supply and, hence, contributes to the cybersecurity of a nation.

5.3 Cybersecurity framework

Cyber threats are continually evolving, making protecting users and organizations a constant challenge. To address this challenge, business groups, government agencies and other organizations produce documents and tools called cybersecurity frameworks to help organize and communicate cybersecurity activities of organizations. Other organizations and people then use or reference cybersecurity frameworks in their cybersecurity activities.

Cybersecurity frameworks based on ISO/IEC TS 27110 provide a way to organize and communicate cybersecurity activities through 5 concepts: Identify, Protect, Detect, Respond, and Recover. Structured within these concepts, a cybersecurity framework can further consist of standards, guidelines and practices to promote cyber risk management. Cybersecurity frameworks provide prioritized, flexible, repeatable and cost-effective approaches to help cybersecurity framework users manage cyber risks.

Cybersecurity frameworks can be used in conjunction with ISMSs to organize cybersecurity activities across multiple layers of an organization, communicate those activities outside of the organization, and ensure continuous improvement of those activities over time. While not required by an ISMS, cybersecurity frameworks can provide additional value to internal and external stakeholders when used together with an ISMS.

5.4 Cybersecurity and safety

Events initiated in cyberspace can have consequences in the physical world to include impact to safety, human life and health. This is the case for systems that provide physical infrastructure or health functions, such as building systems, manufacturing systems, medical devices and other similar systems that are collectively known as the internet of things (IoT) and the industrial internet of things (IIoT). These systems connect through cyberspace and are as such subject to cyber risks. Organizations need to understand and manage cyber risks related to safety as well as safety risks related to cybersecurity.

5.5 Cyber insurance

Organizations can choose to share or transfer their cyber risks. Cyber insurance is one way for an organization to *transfer* its risk. Cyber insurance is a risk treatment option that can compensate the insured against potentially significant financial losses associated with a cybersecurity incident. Cyber insurance is provided by an insurer who underwrites risks by signing and accepting liability, thus guaranteeing payment to the insured in case loss or damage occurs.

Cyber insurance is designed to compensate for losses from a variety of cybersecurity incidents, for example, data breaches, business interruption and physical (infrastructure) or logical (misconfiguration/malware) network damage.

Adoption of cyber insurance can assist the insured to:

a) minimize the impact of a cybersecurity incident;

b) provide funding mechanisms for recovery from major losses;

c) assist the return to normal operations; and

d) increase resilience of the insured business to cybersecurity incidents.

The insured can be required to demonstrate their compliance with any conditions imposed by the cyber insurance policy relating to the ongoing management of the cyber risks covered.

6 Risk management approach in the context of cybersecurity

6.1 General

To manage cyber risks, a clear understanding of the organization's business drivers and security considerations specific to its use of technology is required. Because each organization's risks, priorities and systems are unique, the tools and methods used to achieve the expected outcomes vary. ISO/IEC 27005 provides information about managing information security risks and can also be referred to for how to manage cyber risks.

The risk management process should allow for the organization to do the following.

a) Develop an organizational understanding of how to manage cyber risks to systems, people, assets, data and capabilities for safeguarding the organization. This organizational understanding can also contribute to the safeguarding of people, society, organizations and nations. These activities are foundational. Understanding the business context, the resources that support critical functions, and the related cyber risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcomes include: asset management; business environment; governance; risk assessment; and risk management strategy.

b) Develop and implement appropriate safeguards to ensure delivery of critical services. This supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcomes include: identity management and access control; awareness and training; data security; information protection processes and procedures; maintenance; and protective controls.

c) Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. This enables timely discovery of cybersecurity events. Examples of outcomes include: anomalies and events; security continuous monitoring; and detection processes.

d) Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. This supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcomes include: response planning; communications; analysis; mitigation; and improvements.

e) Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. This supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcomes include: recovery planning; improvements; and communications.

6.2 Threat identification

In cyberspace, varied cyber threats can be identified in relation to the concerned business and societal contexts of the subject entity. While these threats also relate to information security, the following are examples of cyber threats that require special attention which can be further refined when applied to a specific situation of the entity.

a) Cyber threats related to persons

   1) Actors who have malicious intent of attacking or abusing information, systems and services through network.

   2) Software and other tools actors utilize in attacking and abusing information systems and services.

   3) Possibility that persons do not have knowledge and skills required to use or provide a system or service securely.

4) Human errors in the use or provision of the system or service.

b) Cyber threats related to system configurations and environments

1) The system or service is publicly accessible via the internet.

2) Devices, e.g. cameras and other IoT devices, are located at physically unprotected places.

c) Cyber threats related to infrastructures

1) Operation of the system or service depends on electric power supply.

2) Operation of the system or service depends on network services.

d) Cyber threats related to suppliers and ICT supply chain

1) Possibility that developers of the system or service lack knowledge and skills required of secure development.

2) Vulnerable system or service originating from ICT supply chains.

6.3 Risk identification

Identification of cyber threats is followed by identification of cyber risks. Likelihood and consequences of conceivable cybersecurity incidents are evaluated. In these processes, the entity should consider the developing matters in cyberspace, e.g.:

a) changing interests of actors and the advent of capable state actors;

b) emerging application areas of the internet;

c) lack of visibility into the distributed data locations;

d) the omnipresence of social media; and

e) hostile practices associated with the above.

ISO/IEC 27005 provides guidance on information security risk assessment commonly applicable to cyber risk assessment.

7 Cyber threats

7.1 General

The definition of cybersecurity is inclusive of varied understandings of the term conceived by entities including different persons, organizations and nations and of different roles in society, industry and economy. Entities from sectors, e.g. general business organizations, persons, government agencies, public utilities, financial service providers, transport service providers, manufacturers and ICT service providers, can have respective views about cybersecurity characterized by their own threat scenarios. There can be sector-specific understandings of cybersecurity. Subclauses 7.2 to 7.6 provide descriptions of cyber threats.

7.2 General business organization

Performance of a business organization is supported by the ICT infrastructure of its own and its connectedness to the global network. Cyber threats for the organization communicating and interacting with other entities in the network can include:

a) attacks through networks, e.g. intrusion to the intranet, malware infection, advanced persistent threat (APT) attack and a denial of service (DoS) attack;

b) information theft by personnel to include external parties, external threat actors and remote workers;

c) quality issues of ICT devices and systems resulting in failure of their operation; and

d) system management and operational issues that result in a failure to effectively implement cybersecurity controls.

These cyber threats cause consequences impacting the organization. Additionally, an organization's behaviour can cause risks and consequences to other entities. Vulnerable devices of the organization at the network boundary can be maliciously used as a tool for attacks on other entities. Incorrect configuration of assets can generate abnormal data traffic on the network or provide entry points for threats.

7.3 Industrial organization and industrial automation and control systems

Industrial organizations have information systems that control operations of product lines, machines and equipment in the factory, collectively called industrial automation and control systems (IACSs). While each IACS has processes specific to its application, there is a series of processes generally observed in IACS:

a) sensing states or movement of equipment or materials;

b) transmitting the sensed data over the network to an information system;

c) processing of the data;

d) generating controlling data;

e) transmitting the controlling data over the network; and

f) actuating the controlling data into the states or movement of equipment or materials.

Cyber threats in these processes are:

a) attacks on the systems and networks;

b) quality issue of the IACS;

c) loss of integrity or availability of the sensed data or control data;

d) failure in operation of hardware and software; and

e) incorrect or halt of physical operations.

Within these cyber threats, there are cascading relationships of causes and consequences.

An IACS can be a system of devices, machines and other equipment as "things" connected to the network through sensors and actuators.

7.4 Products, services, and supplier relationships

Organizations often choose to form and/or retain supplier relationships for a variety of business reasons to take advantage of the benefits they can provide. Suppliers can provide a multitude of products or services, including IT outsourcing, professional services, basic utilities (equipment maintenance service, security guards service, cleaning and delivering services, etc.), cloud computing services, ICT, knowledge management, research and development, manufacturing, logistics, healthcare services, internet services, and many others.

Most organizations have suppliers and act as suppliers themselves. Organizations connect to their suppliers and customers through cyberspace forming lengthy and complex supply chains where upstream and downstream suppliers are not necessarily known to the organization. Connecting to

suppliers through cyberspace represents a risk to the organization. Extended supply chains present additional risks due to lack of transparency or inconsistency of security controls implemented by suppliers and sub-suppliers.

ICT supply chains present unique cyber risks because ICT forms systems and networks that comprise cyberspace within and outside of the organization's boundaries. When organizations acquire ICT products and services, they inherit vulnerabilities and other quality defects in those products and services. Limited visibility into quality practices of ICT suppliers represents a cyber risk to the organization.

ICT service providers include telecommunication service providers, internet service providers (ISPs), cloud service providers and related product and service providers. They provide products and services to the wide sectors of general business organizations, industrial organizations, critical infrastructures and other organizations and persons.

Organizations can manage cyber risks to ICT supply chains by establishing supplier agreements that define rules for:

a) governing supplier relationships;

b) stating how suppliers connect to the organization's systems and networks through cyberspace;

c) flowing security requirements to suppliers' suppliers;

d) establishing quality assurance requirements for ICT products and services.

For cases where supplier agreement cannot be established (for example, the organization relies on an information source that is publicly available for its critical functions), the organization should identify and appropriately manage resulting cyber risks.

ISO/IEC 27036 (all parts) provides principles and guidelines for information security in supplier relationships.

7.5 Telecommunications services/internet service providers

The providers of telecommunication and internet services provide the entry points to the cyberspace to all users. They have a key role in protecting, responding and recovering to cybersecurity incidents. This includes, for example:

a) activating and operating computer emergency readiness teams (CERT)/computer security incident response teams (CSIRT) that interact with the national CERTs or CSIRTs;

b) identifying and reporting threats to help the users and public authorities to prepare themselves; and

c) providing defensive solutions to block the threats at the point of entry to cyberspace.

7.6 Public authorities

The public authorities have an important role in the national cyberspace. Some examples of what public authorities can do include:

a) publishing and enforcing laws and regulations for sound cybersecurity;

b) establishing and operating national CERT or CSIRT:

c) coordinating actions and reactions to wide scale cybersecurity incidents;

d) organizing certifications for security product and service providers, as well as for critical infrastructure organizations;

e) organizing public-private partnership to provide a better coordinated response to cybersecurity incidents and cyber threats; and

f) encouraging the academia to prepare education programs on cybersecurity.

7.7 Critical infrastructure

The critical infrastructure of a nation provides the means and services to enable safe and secure conduct of the economic, business, and other functions necessary for society's wellbeing, such as financial services and public utilities, e.g. electric power supply. These services support lives and safety of people and operations of organizations, society and nation. Cyber threats to critical infrastructure include attacks via network, degradation and other quality issues of the supporting ICT, human errors in the operation, or a combination thereof. Dependencies among the functions of critical infrastructure make the cyber threats complex and consequences more severe. An organized approach is required to manage the risks across the organization.

7.8 Individual person

IoT devices, e.g. home electric appliances, home security devices, web cameras, game machines, smart phones and varied wearable devices, are abundant in personal life. Using these devices can facilitate cyber threats and cause risks to the person. Attacks on the devices can result in information disclosure or leakage, privacy issues, physical damage to the person or device, compromise of personal identity, or monetary losses.

The use of IoT devices can also cause cyber threats to the entities other than the owner of the device. Vulnerable devices can be abused for attacks on other entities while the owner is unaware of the abuse.

Considerations required of IoT device/service developers and providers are that individual persons:

a) cannot be expected to have expertise in cybersecurity; and

b) have no support by organizational management for cybersecurity measures.

8 Incident management in cybersecurity

8.1 General

While cybersecurity activities aim at preventing occurrence of cybersecurity incidents, there is a possibility of experiencing a cybersecurity incident. Cybersecurity incidents can have consequences on the society, people, environment, organizations and nations. Cybersecurity incidents can be caused by:

a) governance, policy, procedure, process or other relevant failure;

b) unintentional actions or mistakes by organizational personnel or by third parties; and

c) intentional acts or attacks on digital devices, systems, machines, facilities or services or the internet.

Once a cybersecurity incident has occurred, it should be responded to appropriately. To prevent and respond to cybersecurity incidents, private and public sector organizations and people should have awareness and knowledge of cybersecurity commensurate with their roles, and be prepared for protecting, detecting, responding to and recovering from the cybersecurity incidents. Prior to taking these actions, organizations and people need to identify their digital environment, stakeholders, practices and associated cyber risks. Thus, organizations and people address cybersecurity incidents through the phases of identifying, protecting, detecting, responding and recovering.

Incident management in cybersecurity has three areas:

a) incident management within an organization (8.2);

b) cross-organizational coordination (8.3); and

c) technical support by product and service supplier (8.4).

ISO/IEC 27035 (all parts) provides principles and guidelines for information security incident management.

8.2 Incident management within an organization

As an entity in the cyberspace, an organization should be prepared for and react to incidents.

The organization develops and implements a plan for cybersecurity incident management. The plan can include incident handling processes, incident classification, personnel roles and responsibilities, a communication scheme both within the organization and with external entities, use of technical support by external entities, education and training program, performance evaluation scheme, and reporting requirements.

To ensure the organization has the capability for cybersecurity incident management, it establishes an incident response team (IRT) with defined roles in cybersecurity incident management. When defining the roles of an IRT, the organization determines:

a) the services provided, e.g.:

   1) if it provides hands-on cybersecurity incident response or support for other parts of the organization;

   2) if it undertakes cybersecurity monitoring operations; or

   3) if it provides a preventive in addition to a responsive role;

b) the relationships and communications with other parts of the organization; and

c) the relationships and communications with IRTs of other organizations.

A computer security incident response team (CSIRT) is an alternative term for IRT. The term CSIRT is also used for a national centre or other function that coordinates communications between, and provides support for, organizations in cybersecurity incident management.

If a cybersecurity incident is detected, the organization follows the incident handling processes as stipulated in the cybersecurity incident management plan.

The incident handling processes can include detection, notification, triage, analysis, response and reporting activities.

8.3 Cross-organizational coordination

Organizations of an industry including those providing critical infrastructure of society and nation share cyber risk posture of the industry. The organizations recognize common risk sources, risks and incident scenarios with consequences characteristic to the industry. To cope with the risks, organizations should have a strategy for coordinated risk mitigation and incident management activities. Establishing an organization called information sharing and analysis centre (ISAC) is a way of supporting coordinated activities and communications in the industry.

There are cases where the risk scenario of causes and consequences extends across industries. For example, failure to provide electric power or other utility supply, telecommunications or financial services has impacts on the activities of other industries. Cybersecurity incident management activities in industries should have mutual links in order to ensure those activities to be effective. National government can support the industries in organizing cross-industrial cybersecurity information sharing and incident response activities.

8.4 Technical support by product and service supplier

Networks, devices, systems and services in the cyberspace are provided by product and service suppliers. These elements can be relevant to cybersecurity incidents whether they have vulnerabilities

or not. It is possible that a vulnerability of device or system is exploited by a person with malicious intent. It is also possible that non-vulnerable elements are abused to trigger a behaviour that results in a cybersecurity incident, e.g. operation of networks, systems and services supporting the activities of society, people, organizations and nations can be interfered by overloaded traffic.

In this context of cyberspace, product and service suppliers have roles in cybersecurity incident management. They are expected to take part through the phases of identify, protect, detect, respond and recover. Their activities can include:

a) operating a support desk of the product and service;

b) identifying and reporting about vulnerabilities of the product and service;

c) detecting and analysing cybersecurity incidents;

d) providing software updates, workarounds and other support;

e) reporting of the cybersecurity incidents; and

f) providing customers with patch management support.

To meet the needs of these activities consistently and effectively, a product and service supplier can have the function called product security incident response team (PSIRT). For a CSIRT of an organization in need of supplier's support, the PSIRT can be the contact point of the supplier. Additionally, a vendor management performance evaluation scorecard can be established to measure the performance and effectiveness of vendors and suppliers that provide products, services or support during an incident.

Annex A
(informative)

A layered model representing cyberspace

A.1 General

This annex provides an example of how to represent cyberspace. This makes possible, at context establishment, first process step of the risk management, the correct positioning of the primary and supporting assets, their risk sources and the organization's stakeholders.

This improves the approach for the contextualization of known attack scenarios, the assessment of their consequence and likelihood, and optimizes the selection of the defence tactics to prepare the risk treatment decisions.

A.2 Layered model representing cyberspace

In this annex, a way of modelling the cyberspace is suggested. A system can be considered in the cyberspace by introducing a model made with three fundamental layers:

— the ANTHROPOGENIC layer which represents individuals and groups of individuals organized in social networks;

— the DIGITAL layer which represents the logical processes, software, and computer data and configurations. In this layer, a sublayer includes the cyber persona layer, i.e. digital avatars of individuals;

— the PHYSICAL layer which represents physical components and their geographic location.

Figure A.1 shows the structure of the cyberspace consisting of these three layers.

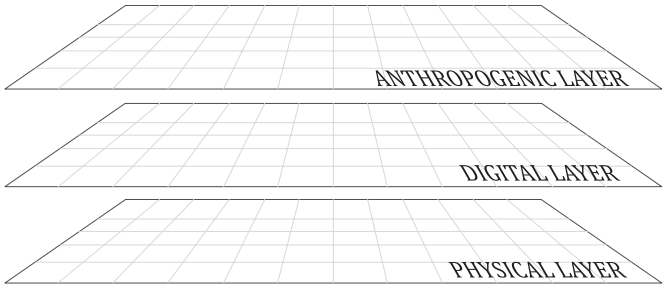


Figure A.1 — Layered cyberspace model

The layered representation model allows a system and its ecosystem to be modelled with a flexible level of detail. It is up to the analyst to select it, depending on the required depth of the analysis. The links between layers are not presented to keep the simplicity of the drawing. The benefit of the layered model is that it keeps the same regardless the size of the objects (nodes and links) being positioned on it.

A.3 Use of the layered model

Each layer is populated with nodes and links covered by various different flows, depending on the layer considered. They make up the projection of the system and its essential assets on this layer.

Projections are made easier by using knowledge bases. Their level of detail is at the discretion of the analyst, depending on the purpose of their study and the complexity of the observed system. This option is possible thanks to the fractal nature of this layered model. Table A.1 provides classification components for each layer of the model.

Table A.1 — Classification of components per layer

Layer	Characteristics	Components
Anthropogenic layer	Fractal model: the unit is an individual. Individuals can form a group of individuals. Individuals and groups of individuals have social links among them.	Nodes: individuals and groups of individuals Links: various forms of social links (authority, partnership, rivalry, etc.) Flows: interactions associated with social links (subordination, collaboration, confrontation, etc.)
Digital layer	Fractal model: a system can be made up of systems comprising of processes, software and computer data.	Node: system, digital persona Link: communication link Flow: information flow
Physical layer	Fractal model: variable level of detail (floor occupancy plan, building structure, topographical map, routers, switches, servers, computers, etc.). The layer is subject to the laws of physics.	Node: moveable property Link: pipeline [material], electrical cable [energy], Ethernet cable [information], routers, switches, servers, computers [infrastructure] Flow: material flow, energy flow, information flow

The layers communicate with each other. Exchanges between different layers are reflected by inter-layer links. Each of these links has its own nature, which is different from the intra-layer links. Table A.2 shows further explanations about classification of inter-layer links. Figure A.2 shows an example of location links.

Table A.2 — Classification of inter-layer links

Layers links	Nature of inter-layer links
anthropogenic ↔ digital	Identity link: an individual's digital identities (email address, user account, cyber persona on social media, etc.) Knowledge link: knowledge of a digital identity (e.g. a cyber persona on social media) by an individual Access link: access to a physical component or geographic zone by an individual
anthropogenic ↔ physical	Location link: an individual's geographic location (in a zone, building, etc.) Knowledge link: knowledge of physical or geographic location information by an individual Access link: access to a physical component or geographic zone by an individual
digital ↔ physical	Location link: location of physical components which host data (possibly highly distributed) Implementation link: location of physical components which run a program (possibly highly distributed) Control/command link: ability of a program to interact with a physical component (e.g. sensor/switch)

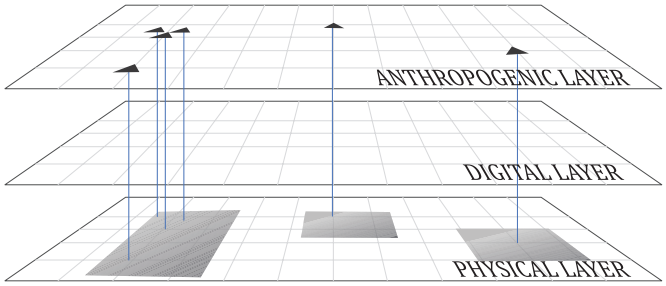


Figure A.2 — Location links (human layer ↔ physical layer)

While this type of modelling can initially appear complex, its approach is largely facilitated by the contribution of several tools and techniques:

— the use of system patterns, which represent structures frequently found and modelled once for all (e.g. hosting in the cloud services, social network, MPLS WAN network, etc.);

— use of existing knowledge bases from various sectors (e.g. physical security, psycho-social risks);

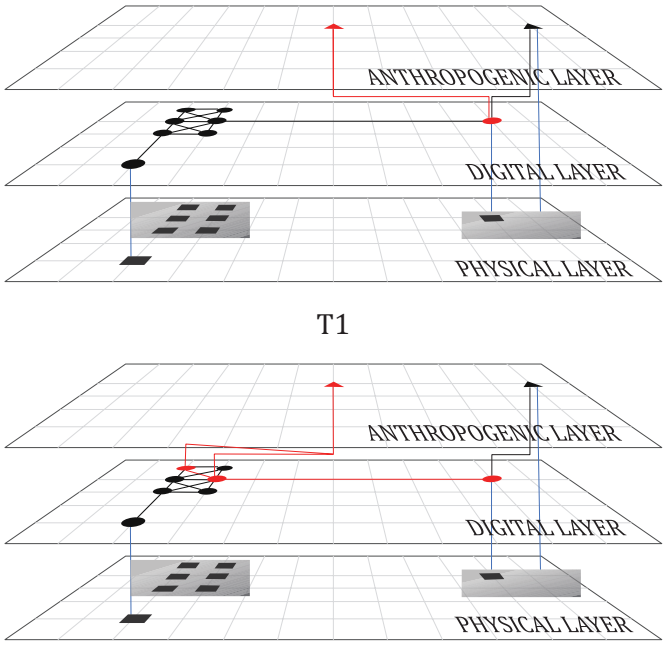
— application of an iterative methodology, by modelling high-level systems and applying successive refinement;

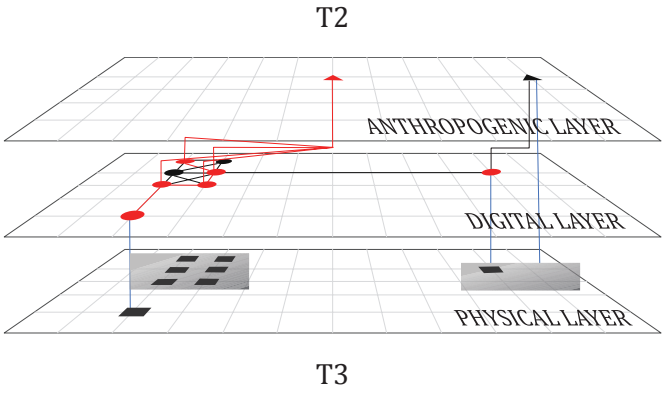
— application of modelling techniques to limit complexity (e.g. symmetry study to only study part of the symmetric pattern of the problem, etc.).

A.4 Dynamic characteristics

The defined structural model should be understood as a dynamic model; in other words, each action performed on a target system modifies its model in cyberspace, by adding or removing nodes or links, or by modifying a flow.

Other manifestations of the time-based dimension are broader, specifically when involving the digital layer. An example is a time-based manifestation of an APT attack in the framework, shown in Figure A.3: the logical intrusion phase, where the attacker has a direct connection to the target-system, then the lateral movement phase within the target-system.





Key

T1 intrusion phishing attack of an exposed user

T2 action taking control of the IT components

T3 exploitation target corruption

Figure A.3 — Representation of different phases of an APT type attack

The cyberspace representation model is versatile enough to allow differing levels of analysis depending on the analyst's requirements.

Furthermore, the base model with 3 fundamental layers can be extended to 6 layers:

— the ANTHROPOGENIC-1 subdivision, called the COGNITIVE layer, is used to model the social representation of human beings;

— the ANTHROPOGENIC-2 subdivision, called the HUMAN layer, is used to model individuals and their organisation into social networks;

— the DIGITAL-1 subdivision, called the CYBER PERSONA layer, is used to model the digital persona of individuals or digital components;

— the DIGITAL-2 subdivision, called the LOGICAL layer, is used to model technical computer data and software running processes;

— the PHYSICAL-1 subdivision, called the COMPONENT layer, is used to model components which make up IT system infrastructure;

— the PHYSICAL-2 subdivision, called the GEOGRAPHIC layer, is used to model the geographic location of people and assets.

Figure A.4 shows the 6-layer cyberspace model.

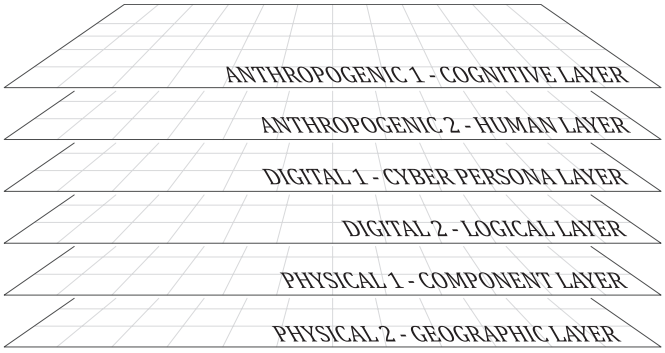


Figure A.4 — Extended layered cyberspace model

Bibliography

[1] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[2] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[3] ISO/IEC 27019, *Information technology — Security techniques — Information security controls for the energy utility industry*

[4] ISO/IEC 27035 (all parts), *Information technology – Security techniques – Information security incident management*

[5] ISO/IEC 27036 (all parts), *Information technology — Security techniques — Information security for supplier relationships*

[6] ISO/IEC TS 27102, *Information technology – Security techniques – Information security management guidelines for cyber insurance*

[7] ISO/IEC TS 27110, *Information technology – Information security, cybersecurity and privacy protection – Cybersecurity framework development guidelines*

[8] ISO 31000, *Risk management — Guidelines*

[9] AFNOR CN SSI N0477, *"Voluntary standards and innovative approaches to cybersecurity", December 2019*

ICS 35.030

Price based on 17 pages