INTERNATIONAL STANDARD

ISO/IEC 27032

First edition
2012-07-15

Information technology — Security techniques — Guidelines for cybersecurity

Technologies de l'information — Techniques de sécurité — Lignes directrices pour la cybersécurité

Reference number
ISO/IEC 27032:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27032 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

The Cyberspace is a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical information and communications technology (ICT) devices and connected networks. However there are security issues that are not covered by current information security, Internet security, network security and ICT security best practices as there are gaps between these domains, as well as a lack of communication between organizations and providers in the Cyberspace. This is because the devices and connected networks that have supported the Cyberspace have multiple owners, each with their own business, operational and regulatory concerns. The different focus placed by each organization and provider in the Cyberspace on relevant security domains where little or no input is taken from another organization or provider has resulted in a fragmented state of security for the Cyberspace.

As such, the first area of focus of this International Standard is to address Cyberspace security or Cybersecurity issues which concentrate on bridging the gaps between the different security domains in the Cyberspace. In particular this International Standard provides technical guidance for addressing common Cybersecurity risks, including:

— social engineering attacks;

— hacking;

— the proliferation of malicious software (“malware”);

— spyware; and

— other potentially unwanted software.

The technical guidance provides controls for addressing these risks, including controls for:

— preparing for attacks by, for example, malware, individual miscreants, or criminal organizations on the Internet;

— detecting and monitoring attacks; and

— responding to attacks.

The second area of focus of this International Standard is collaboration, as there is a need for efficient and effective information sharing, coordination and incident handling amongst stakeholders in the Cyberspace. This collaboration must be in a secure and reliable manner that also protects the privacy of the individuals concerned. Many of these stakeholders can reside in different geographical locations and time zones, and are likely to be governed by different regulatory requirements. Stakeholders include:

— consumers, which can be various types of organizations or individuals; and

— providers, which include service providers.

Thus, this International Standard also provides a framework for

— information sharing,

— coordination, and

— incident handling.

The framework includes

— key elements of considerations for establishing trust,

— necessary processes for collaboration and information exchange and sharing, as well as

— technical requirements for systems integration and interoperability between different stakeholders.

Given the scope of this International Standard, the controls provided are necessarily at a high level. Detailed technical specification standards and guidelines applicable to each area are referenced within this International Standard for further guidance.

Information technology — Security techniques — Guidelines for cybersecurity

1 Scope

This International Standard provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular:

— information security,

— network security,

— internet security, and

— critical information infrastructure protection (CIIP).

It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides:

— an overview of Cybersecurity,

— an explanation of the relationship between Cybersecurity and other types of security,

— a definition of stakeholders and a description of their roles in Cybersecurity,

— guidance for addressing common Cybersecurity issues, and

— a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

2 Applicability

2.1 Audience

This International Standard is applicable to providers of services in the Cyberspace. The audience, however, includes the consumers that use these services. Where organizations provide services in the Cyberspace to people for use at home or other organizations, they may need to prepare guidance based on this International Standard that contains additional explanations or examples sufficient to allow the reader to understand and act on it.

2.2 Limitations

This International Standard does not address:

— Cybersafety,

— Cybercrime,

— CIIP,

— Internet safety, and

— Internet related crime.

It is recognized that relationships exist between the domains mentioned and Cybersecurity. It is, however, beyond the scope of this International Standard to address these relationships, and the sharing of controls between these domains.

It is important to note that the concept of Cybercrime, although mentioned, is not addressed. This International Standard does not provide guidance on law-related aspects of the Cyberspace, or the regulation of Cybersecurity.

The guidance in this International Standard is limited to the realization of the Cyberspace on the Internet, including the endpoints. However, the extension of the Cyberspace to other spatial representations through communication media and platforms are not addressed, nor the physical security aspects of them.

EXAMPLE 1 Protection of the infrastructure elements, such as communications bearers, which underpin the Cyberspace are not addressed.

EXAMPLE 2 The physical security of mobile telephones that connect to the Cyberspace for content download and/or manipulation is not addressed.

EXAMPLE 3 Text messaging and voice chat functions provided for mobile telephones are not addressed.

3 Normative references

The following referenced documents are indispensable for the application 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*

4 Terms and definitions

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

4.1
adware
application which pushes advertising to users and/or gathers user online behaviour

NOTE The application may or may not be installed with the user's knowledge or consent or forced onto the user via licensing terms for other software.

4.2
application
IT solution, including application software, application data and procedures, designed to help an organization's users perform particular tasks or handle particular types of IT problems by automating a business process or function

[ISO/IEC 27034-1:2011]

4.3
application service provider
operator who provides a hosted software solution that provides application services which includes web based or client-server delivery models

EXAMPLE Online game operators, office application providers and online storage providers.

4.4
application services
software with functionality delivered on-demand to subscribers through an online model which includes web based or client-server applications

4.5
application software
software designed to help users perform particular tasks or handle particular types of problems, as distinct from software that controls the computer itself

[ISO/IEC 18019]

4.6
asset
anything that has value to an individual, an organization or a government

NOTE Adapted from ISO/IEC 27000 to make provision for individuals and the separation of governments from organizations (4.37).

4.7
avatar
representation of a person participating in the Cyberspace

NOTE 1 An avatar can also be referred to as the person's alter ego.

NOTE 2 An avatar can also be seen as an "object" representing the embodiment of the user.

4.8
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

[ISO/IEC 27000:2009]

4.9
attack potential
perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation

[ISO/IEC 15408-1:2005]

4.10
attack vector
path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome

4.11
blended attack
attack that seeks to maximize the severity of damage and speed of contagion by combining multiple attacking methods

4.12
bot
robot
automated software program used to carry out specific tasks

NOTE 1 The word is often used to describe programs, usually run on a server, that automate tasks such as forwarding or sorting e-mail.

NOTE 2 A bot is also described as a program that operates as an agent for a user or another program or simulates a human activity. On the Internet, the most ubiquitous bots are the programs, also called spiders or crawlers, which access websites and gather their content for search engine indexes.

4.13
botnet
remote control software, specifically a collection of malicious bots, that run autonomously or automatically on compromised computers

4.14
cookie
<access control> capability or ticket in an access control system

4.15
cookie
<IPSec> data exchanged by ISAKMP to prevent certain Denial-of-Service attacks during the establishment of a security association

4.16
cookie
<HTTP> data exchanged between an HTTP server and a browser to store state information on the client side and retrieve it later for server use

NOTE A web browser can be a client or a server.

4.17
control
countermeasure
means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature

[ISO/IEC 27000:2009]

NOTE ISO Guide 73:2009 defines control as simply a measure that is modifying risk.

4.18
Cybercrime
criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime

4.19
Cybersafety
condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable

NOTE 1 This can take the form of being protected from the event or from exposure to something that causes health or economic losses. It can include protection of people or of assets.

NOTE 2 Safety in general is also defined as the state of being certain that adverse effects will not be caused by some agent under defined conditions.

4.20
Cybersecurity
Cyberspace security
preservation of confidentiality, integrity and availability of information in the Cyberspace

NOTE 1 In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

NOTE 2 Adapted from the definition for information security in ISO/IEC 27000:2009.

4.21
the Cyberspace
complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form

4.22
Cyberspace application services
application services (4.4) provided over the Cyberspace

4.23
cyber-squatter
individuals or organizations that register and hold on to URLs that resemble references or names of other organizations in the real world or in the Cyberspace

4.24
deceptive software
software which performs activities on a user's computer without first notifying the user as to exactly what the software will do on the computer, or asking the user for consent to these actions

EXAMPLE 1 A program that hijacks user configurations.

EXAMPLE 2 A program that causes endless popup advertisements which cannot be easily stopped by the user.

EXAMPLE 3 Adware and spyware.

4.25
hacking
intentionally accessing a computer system without the authorization of the user or the owner

4.26
hactivism
hacking for a politically or socially motivated purpose

4.27
information asset
knowledge or data that has value to the individual or organization

NOTE Adapted from ISO/IEC 27000:2009.

4.28
internet
internetwork
collection of interconnected networks

NOTE 1 Adapted from ISO/IEC 27033-1:2009

NOTE 2 In this context, reference would be made to "an internet". There is a difference between the definition of "an internet" and "the Internet".

4.29
the Internet
global system of inter-connected networks in the public domain

[ISO/IEC 27033-1:2009]

NOTE There is a difference between the definition of "an internet" and "the Internet".

4.30
Internet crime
criminal activity where services or applications in the Internet are used for or are the target of a crime, or where the Internet is the source, tool, target, or place of a crime

4.31
Internet safety
condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Internet which could be considered non-desirable

4.32
Internet security
preservation of confidentiality, integrity and availability of information in the Internet

4.33
Internet services
services delivered to a user to enable access to the Internet via an assigned IP address, which typically include authentication, authorization and domain name services

4.34
Internet service provider
organization that provides Internet services to a user and enables its customers access to the Internet

NOTE Also sometimes referred to as an Internet access provider.