INTERNATIONAL STANDARD

ISO/IEC 27102

First edition
2019-08

Information security management — Guidelines for cyber-insurance

Gestion de la sécurité de l'information — Lignes directrices pour la cyber-assurance

Reference number
ISO/IEC 27102:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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 http://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

Cyber-incidents can occur at any time with various potential impacts to an organization. For example, an organization's information and assets are under constant attack as cyber-threats become more pervasive, persistent and sophisticated.

The adoption of cyber-insurance to reduce the impacts of the consequences arising from a cyber-incident should be considered by an organization in addition to information security controls as part of an effective risk treatment approach.

Cyber-insurance is no substitute for robust security and effective incident response plans, along with rigorous training of all employees.

Cyber-insurance should be considered as an important component of an organization's overall security risk treatment plan to increase resilience.

Information security management — Guidelines for cyber-insurance

1 Scope

This document provides guidelines when considering purchasing cyber-insurance as a risk treatment option to manage the impact of a cyber-incident within the organization's information security risk management framework.

This document gives guidelines for:

a) considering the purchase of cyber-insurance as a risk treatment option to share cyber-risks;

b) leveraging cyber-insurance to assist manage the impact of a cyber-incident;

c) sharing of data and information between the insured and an insurer to support underwriting, monitoring and claims activities associated with a cyber-insurance policy;

d) leveraging an information security management system when sharing relevant data and information with an insurer.

This document is applicable to organizations of all types, sizes and nature to assist in the planning and purchase of cyber-insurance by the organization.

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 and the following 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-incident
cyber-event that involves a loss of information security or impacts business operations

3.2
cyber-insurance
insurance that covers or reduces financial loss to the *insured* (3.7) caused by a *cyber-incident* (3.1)

3.3
cyber-insurance policy
contract for *cyber-insurance* (3.2) coverage

3.4
cyber-risk
risk caused by a *cyber-threat* (3.5)

3.5
cyber-threat
threat that exploits a *cyberspace* (3.6)

3.6
cyberspace
interconnected digital environment of networks, services, systems, and processes

3.7
insured
entity that shares or considers sharing *cyber-risk* (3.4) with an insurer

4 Structure of this document

Guidelines are given in Clauses 5 to 8.

Clause 5 provides information and a general description of cyber-insurance; Clause 6 discusses cyber-risk of an organization that can be covered under a cyber-insurance policy. Both Clause 5 and Clause 6 are of relevance to both the organization and an insurer.

Clause 7 describes the generic risk assessment an insurer typically undertakes as part of its cyber-insurance underwriting and Clause 8 describes the use of an information security management system (ISMS) by an insured to produce data, information and documentation that can be shared with an insurer.

Annex A provides examples of ISMS documents that an insured can provide to an insurer.

5 Overview of cyber-insurance and cyber-insurance policy

5.1 Cyber-insurance

Cyber-insurance is a risk treatment option that can compensate the insured against potentially significant financial losses associated with a cyber-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 cyber-incidents, for example: data breaches, business interruption, and network damage.

Adoption of cyber-insurance can assist the insured to:

a) minimize the impact of a cyber-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 cyber-incidents.

The insured can be required to demonstrate their compliance with any conditions imposed by the cyber-insurance policy relating to the on-going management of the cyber-risk covered.

5.2 Cyber-insurance policy

Contractual terms for cyber-insurance are given in a cyber-insurance policy. A cyber-insurance policy can be either a stand-alone policy or be included as special endorsements as a part of general liability, property or other insurance policy.

Coverage offered by a cyber-insurance policy typically takes a wide perspective and covers a broad range of threats that can cause financial or other forms of impact. Impact can occur through loss of confidentiality, integrity, or availability of information or systems irrespective of the exact cause of a cyber-incident and whether it was accidental or deliberate. Cyber-insurance coverage varies quite a lot between different cyber-insurance products, is not standardized and varies depending on:

a) needs of the insured;

b) limitations posed by laws and regulations;

c) generally accepted market practices;

d) business decisions of an insurer.

Cyber-insurance policies cover certain costs associated with cyber-incidents and can provide access to services that support the insured after a cyber-incident. These services include, for example, evaluating the impact of the attack; implementation of response and recovery plans; legal expertise; forensics expertise; public relations and communications support; customer notification; and restoration of business operations after a cyber-incident.

Cyber-insurance coverage offers the ability to recover some or all internal and external costs of the cyber-incident and varies depending on the specific policies and endorsements selected by the insured.

6 Cyber-risk and insurance coverage

6.1 Risk management process and cyber-insurance

A cyber-insurance policy generally allows the insured to reduce losses from cyber-risks through the sharing of these risks with an insurer.

An organization should be protected from cyber-risks by using a process that actively predicts, identifies, assesses, treats and responds to cyber-incidents as part of an effective risk management approach.

The risk assessment process should include appropriate translation of cyber-risks into business terms to highlight the business consequences of cyber-incidents. Such translation can allow risk treatment decisions to determine how risks are to be treated through:

a) avoidance;

b) removing the threat;

c) changing the likelihood or consequences of the risk;

d) retaining the risk; or

e) sharing the risk with other parties, such as insurers.

Risk treatment decisions should consider the incorporation of cyber-insurance, to improve resilience against such risks. The risk management process provides information on risks and business consequences to align a cyber-insurance policy with the security risk management strategy and risk acceptance criteria of the organization.

6.2 Cyber-incidents

6.2.1 General

A cyber-incident occurs where a cyber-risk becomes a reality and leads to a loss of confidentiality, integrity or availability of data or other assets.

A cyber-incident is caused by a threat that exploits a cyberspace vulnerability typically relating to the use of information systems and networks. The use of the cyberspace brings threats such as denial of service attack, intrusion to an organization's network, malware dissemination, improper use of information or information systems, and extortion. In addition, there are also other threats such as errors and omissions and system malfunctions. The organization should identify relevant threats in light of its business and technological contexts.

A cyber-incident can be caused by an actor exploiting a vulnerability, by unintentional error, or by a system malfunction. A cyber-incident can impact the organization’s technology and, as a result, require repair or replacement of the impacted asset.

6.2.2 Cyber-incident types

Cyber-incidents, originating from internal or external threat sources, belong to one or more of the following categories:

a) **system malfunction**: the insured’s system or network is malfunctioning or creating damage to a third-party system or a supplier's system is not functioning, impacting operations;

b) **data confidentiality breach**: data stored in the insured’s system (managed on premise, hosted or managed by a third party) has been stolen or exposed;

c) **data integrity or availability loss**: data stored in the insured’s system (managed on premise, hosted or managed by third party) has been corrupted or deleted;

d) **other malicious activity**: misuse of a technology system to inflict harm (such as cyber-bullying over social platforms or phishing attempts) or to illicitly gain profit (such as cyber-fraud); and

e) **human error**: where something unintentional has been done by a human resulting in harm to a system, network or information.

Root causes for incidents can usually be attributed to failure of people, systems or processes.

Each of these incident types can be covered by cyber-insurance.

6.3 Business impact and insurable losses

6.3.1 Overview

A cyber-incident can result in business impacts to the organization. These impacts can include the loss or compromise of personal data, loss of e-commerce revenue, disruption of supply chains and business interruption. During and after a cyber-incident, the organization can be faced with significant costs to restore operations, conduct investigations and settle regulatory fines and legal cases.

Certain business impacts resulting from a cyber-incident can be quantified, for example: loss of sales, lost profit, cost of crisis management, forensic investigations, lawsuits and indemnification, notifications to business partners and customers, regulatory investigations, fines, attorneys and consultants, public relation professionals, and remedial measures. Some business impacts can be difficult to quantify, for example reputational damage, impact or damages to business executives, management, staff and related personnel or leakage of trade secrets and other infringement of intellectual property rights.

A cyber-incident affecting the organization can also occur at a supplier or another third-party organization supplying goods or performing services for the organization.

