International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1061

(08/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Security management

Cyber insurance acquisition guidelines

Recommendation ITU-T X.1061

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	**X.1050–X.1069**
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
IMT-T SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1061

Cyber insurance acquisition guidelines

Summary

The cyber insurance acquisition guidelines established by Recommendation ITU-T X.1061 provide an understanding of cyber insurance coverage and requirements for cybersecurity risk assessment, selection of insurer, assessment by the insurer and evaluation of insurer for organizations that adopt cyber insurance as a risk treatment option to manage the impact of a cybersecurity incident.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1061	2021-08-22	17	11.1002/1000/14733

Keywords

Information security, information security management, ICT, management guidelines, network security, risk management, security requirements.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1061

Cyber insurance acquisition guidelines

1 Scope

This Recommendation establishes guidelines for acquiring cyber insurance from an insurer to manage the impact of a cybersecurity incident within the information security risk management framework of an organization.

These guidelines apply in managing cybersecurity risks, sharing relevant data and information with insurers, leveraging security risk assessment results and managing the impact of cybersecurity incidents. This Recommendation also provides guidelines to select an insurer and manage contracts based on the organization's information security risk management.

These guidelines apply to organizations that either wish to purchase or use cyber insurance as a result of a risk assessment. This Recommendation also applies to insurers that provide cyber insurance.

Cyber insurance is no substitute for robust cybersecurity and effective incident response plans, along with rigorous training of all employees, but it is considered as an important component of an organization's overall cybersecurity risk treatment plan.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cyber incident [b-ISO/IEC 27102]: Cyber event that involves a loss of information security or impacts business operations.

3.1.2 insured [b-ISO/IEC 27102]: Entity that shares or considers sharing cyber-risk with an insurer.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cyber insurance; cyber risk insurance; cyber liability insurance coverage: An insurance policy that covers or reduces financial loss to the insured caused by a cyber -incident. It mitigates risk exposure to an organization by offsetting costs involved with recovery after a cyber-related security breach or similar event. It is also an insurance that helps organizations cover the cost of recovering from loss caused by cyber incidents or cybersecurity events.

NOTE 1 – Cyber insurance can be used as an option for information security risk treatment.

NOTE 2 – Based on [b-ISO/IEC 27102].

3.2.2 excess; retention amount: Sum of money that an organization pays in an insurance claim before an insurer pays compensation.

3.2.3 insurer: A company that underwrites an insurance risk; the party in an insurance contract undertaking to pay compensation.

3.2.4 premium warranty: The insured is required to pay the premiums charged for the insurance under a premium warranty within the stipulated duration from the effective date of insurance cover, which is shown on the policy, cover note or renewal certificates.

3.2.5 responsible, accountable, consulted and informed (RACI); RACI matrix; linear responsibility chart: A responsibility assignment matrix that describes the various roles in completing tasks or deliverables for a project or business process. 1. responsible, accountable, consult, and inform. 2. a common type of responsibility assignment matrix that uses responsible, accountable, consult, and inform statuses to define the involvement of stakeholders in project activities [*A guide to the project management body of knowledge (PMBOK® Guide)* – fifth edition [b-PMBOK Guide]].

NOTE – Based on [b-ISO/IEC 27102].

3.2.6 silent cyber: Potential cyber exposures contained within traditional property and liability insurance policies, which may not implicitly include or exclude cyber risks.

3.2.7 waiting period: A period before business interruption coverage begins to apply. The length of the waiting period needs to be agreed before its inclusion in a cyber insurance policy.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CLIC Cyber Liability Insurance Coverage

ICT Information and Communication Technology

IT Information Technology

NDA Non-Disclosure Agreement

OT Operational Technology

PII Personally Identifiable Information

PR Public Relations

RACI Responsible, Accountable, Consulted and Informed

5 Conventions

None.

6 Overview

This Recommendation assists organizations that are considering buying cyber insurance by providing guidance on some important requirements of the insured and insurer. The guidelines help organizations of all sizes and across all sectors to better manage their cybersecurity risks with cyber insurance.

Cyber insurance is a risk transfer option that can be used to manage the impact of cyber and data breach incidents. Contractual terms for cyber insurance are given in a cyber insurance policy, which is typically a stand-alone document or a separate section in a more general insurance policy. Cyber insurance should be used to protect an insured against any potential losses associated with a cyber incident or data breach.

Cyber insurance is taken out to assist the insured to minimize the impact and mitigate the losses resulting from cyber incidents and data breaches by providing alternative mechanisms to recover from losses and to return to normal operations.

The organization should be aware that cyber insurance does not reduce the likelihood of occurrence of risks that are being transferred.

7 Cyber insurance considerations

The organization taking out cyber insurance should consider clauses 7.1 to 7.5.

7.1 Identify the cyber risks

There are as many as 12 different types of coverage available for cyber threats. These can include a range of online and offline risks, spanning everything from data breaches to theft of corporate assets. By identifying the cyber threats upfront, the organization should be able to find the right cyber insurance coverage that best meets the needs of the organization.

7.2 Understand the policy coverage

The organization should review existing insurance policies that may be complementary to new cyber insurance policy coverage. Organization should also consider combination of products to get adequate coverage, such as stand-alone cyber insurance and general property insurance policies. It is important for the organization to understand on how each policy benefits the organization.

7.3 Consult cyber insurance expert

The organization should consider seeking guidance from a professional broker or cyber insurance expert who understands the industry, business and cybersecurity risks. Damages resulting from cyber threats and liability can be difficult to understand and quantify. The cyber insurance expert should help the organization to translate cyber risks into a financial model and to ensure adequate coverage.

7.4 Understand the claim process

The organization should understand the claim process and the timeline to recover the cost of cyber incidents. Understanding the claim process when selecting cyber insurance or cyber liability insurance coverage (CLIC) is critical. Each insurer has processes set up for vetting the authenticity of a claim by the insured and a general timeline within which funds are to be paid.

7.5 Understand other insurance benefits

The organization should understand that some insurers provide additional benefits such as cyber investigators or public relations (PR) firms. The organization needs to confirm the coverage includes these additional services as part of the insurance benefits.

8 Cybersecurity risk assessments

The organization should apply an effective cybersecurity risk treatment process to determine the risk to be transferred to cyber insurance policies. The organization may enforce the cyber insurance policies with proper cybersecurity communication and reporting as part of the organization's information and network security controls.

The organization should establish proper governance, roles and responsibilities (e.g., RACI) on their current cybersecurity strategy, practice and requirements for cyber risk management, including cyber insurance. The organization should conduct business impact analysis and risk assessment aligned with the organization's requirements on information and network security controls.

The organization should consider the overall data breach risks and risk management options cross-functionally involving stakeholders such as those responsible for information technology (IT), risk management, privacy, compliance, legal and security. The organization should accurately quantify risks, evaluate options and develop a cost-benefit analysis to determine whether cyber insurance is the right investment.

If the organization is processing and storing data in a cloud or a co-located data centre, ensure that risk assessment covers the risks related to such hosts. Based on the cyber risk factors, the organization should be able to consider the value of cyber insurance in managing its cyber risks.

9 Cyber insurance policy

The organization should establish a cyber insurance policy that provides a list of critical cyber risks and activities to be covered in the cyber insurance. The policy should be based on cybersecurity risk assessments. The potential list in a cyber insurance policy should include, but is not limited to, the following.

– Network security coverage (hardware, software, physical and staff status).
– Data breach incident response (attack recognition, planning for response and recovery).
– Multimedia liability.
– Endpoint device insurance (desktop, laptop, tablet, mobile, Internet of things).
– Cyber business interruption coverage.
– Cyber extortion and terrorism coverage.
– Litigation and enforcement proceedings (excluding government or regulatory fines).
– Loss in association with third party systems.
– Lost or stolen data and digital assets.
– Crisis management and PR.
– Forensics.

10 Cyber insurance policy coverage

An optimal cyber risk insurance policy or CLIC of an organization should include both first party and third party coverage to ensure full coverage of the cyber risk liabilities. Organizations should understand the difference between the two coverage pies and plan for the right coverage.

Understanding the cyber risks of the organization should help it to plan for the right coverage. The coverage varies depending on the z needs and risk profile of the organization. The cyber insurance cover two primary types of cyber insurance policy categories:

a) first party loss;
b) third party liability

10.1 First party loss coverage

First-party loss coverage refers to insurance that most organizations take out for cyber liability coverage. This coverage is adequate for organizations to protect against everyday cyber risks including data breaches. For example, a comprehensive policy should be created to cover the costs of recouping lost data and records management, notifying stakeholders, providing identity theft protection, offering credit monitoring, managing brand damage, updating systems, etc.

First party losses that are incurred by the insured should include, but are not limited to, those specified in clauses 10.1.1 to 10.1.5.

10.1.1 Business interruption

Business interruption loss arising from a disruptive incident.

10.1.2 Incident response

Reasonable and necessary expenses incurred by the insured in responding to a cyber incident result in a loss.

NOTE – Incident response costs should include PR, legal, crisis management, incident handling, cyber forensics, credit monitoring and customer notification.

10.1.3 Data restoration

A loss is incurred due to recovery costs arising from a data asset incident.

10.1.4 Legal

A loss is incurred due to an information security incident that results in defence costs and associated expenses for legal action.

10.1.5 Cyber extortion

A loss is incurred to provide coverage for cyber extortion damage and cyber extortion expenses due to a cyber extortion event.

Appendix I provides more information on the types of cost of first party losses.

10.2 Third party liability coverage

A third party cyber insurance policy is designed for individuals and organizations responsible for information and communication technology (ICT) services that are exposed to cyber threats such as cyberattack or data breach. Third party liability coverage insurance protects mostly ICT companies, software firms, and providers of cloud and managed services that are also responsible for the security management of their ICT services.

Third party liability coverage protects the insured against claims from third parties such as customers or partners, which should include coverage of data privacy liability, media liability, network security liability and regulatory investigation.

10.2.1 Privacy liability

It is necessary to protect the insured for any legal expenses and damages arising out of a data breach (including personally identifiable information (PII) or confidential information).

10.2.2 Network security liability

It is necessary to protect the insured for any legal expenses and damages arising out of a cyber incident.

10.2.3 Media liability

It is necessary to protect the insured for any legal expenses and damages arising out of negligence in its online media content and online advertising, including websites, blogs and social media.

10.2.4 Regulatory investigation expenses (including fines and penalties to the extent that is insurable by law)

Cyber insurance indemnifies the insured against any expenses in relation to a regulatory investigation. The organization should ensure that this coverage includes and is not limited to legal and forensic expenses.

10.3 Limit of liability

With each of the areas in clauses 10.1 and 10.2 reviewed and clarified, the organization should carefully determine and consider how much cyber insurance coverage to obtain. The amount of cyber insurance that the organization can obtain varies depending on its turnover, industry, operations and risk exposures.

10.4 Cyber insurance excess

Cyber insurance should protect individuals and organizations from cybersecurity risks and cyber threats specifically related to IT infrastructure, information and data privacy, information governance liability, etc. Cyber insurance excess covers against losses such as data destruction, extortion, theft, hacking and the costs associated with notifying stakeholders.

Cyber insurance policies may have an excess, which is the sum the insured should bear before the insurer pays out within the terms of cyber insurance policy. Cyber insurance policies may have a waiting period, which is the time the insured organization should wait before the insurer pays out within the terms of the cyber insurance policy.

The excess and waiting period should be agreed during negotiation of the terms of the cyber insurance policy. To assist an organization, there are a number of research organizations that regularly publish industry benchmark information on losses due to past cyber incidents around the world that should be evaluated to assist the insured to determine the appropriate amount of coverage to obtain.

10.5 Policy exclusion

The organization should be aware that a cyber insurance policy cannot cover all situations and terms vary by insurers. Some common exclusions of cyber insurance are specified in clauses 10.5.1 to 10.5.7.

10.5.1 War, invasion and insurrection

Most cyber policies exclude damage resulting from these events, as well as terrorism with a carve-back to cyber terrorism.

10.5.2 Patent, software and copyright infringement

Patents, software and copyright are covered by an intellectual property insurance policy, not a cyber policy. In some cases, however, a detailed written cyber policy can cover legal costs and copyright infringement claims. However, such claims should be the result of actions by a non-management employee or an outside third party.

10.5.3 Bodily injury and property damage

Data breach does not involve a person being directly injured physically and hence such claims are excluded. However, some policies do cover emotional distress and anguish caused by such events.

10.5.4 Infrastructure

Cyber incidents and data breaches due to failure of utilities or facilities are excluded.

10.5.5 Misdeed

A cyber incident caused by top management or a member of the board of directors in collusion with a third party or employee is excluded.

10.5.6 Criminal action

Cyber incidents arising from actions by the insured that violate legal or regulatory requirements, such as an unauthorized or wrongful collection of personal data, are excluded.

10.5.7 Natural disaster and *force majeure*

Natural disaster, *force majeure* or an extraordinary event or circumstance beyond the reasonable control of the parties, including, but not limited to, a strike, riot, crime, epidemic, sudden legal change, flood, earthquake, landslide, lightning, wind or even fire are commonly excluded because such events lie outside the coverage of a cyber insurance policy.

11 Silent cyber coverage

Silent cyber refers to potential cyber-related losses stemming from traditional property and liability policies that were not specifically designed to cover cyber risk. Unlike cyber insurance, traditional liability policies were not designed with cyber exposures in mind and therefore may not implicitly include or exclude cyber risks. This coverage ambiguity can result in a silent cyber coverage scenario, whereby an insurer may have to pay claims for cyber losses under the terms of a policy not designed for that purpose.

Traditional commercial insurance policies, such as property, casualty, crime, kidnap or ransom; may not be designed to explicitly address, either to include or exclude, cyber-related losses. If a policy does not affirmatively grant or exclude cyber coverage, this is termed "silent cyber" and there is no guarantee that it will actually cover a loss. Silent cyber risks refer to cyber-related losses that can be incurred via traditional property and liability policies that do not specifically cover damage caused by cyberattacks.

Among the threats of cyberattack are financial losses or exposure of data through social engineering or phishing scams, online fraud, physical damage to property, ransomware, data breaches, business disruptions, and damage of brand and reputation. An organization should not just be dependent on silent cyber coverage in their existing property and casualty portfolio, but may need to consider affirmative coverage grants for cyber loss or a stand-alone cyber insurance policy to cover such losses.

There are cyber-related incidents that may already be covered within other insurance policies of the organization. Therefore, the organization should consider potential coverage of silent cyber and understand the exclusions of cyber risks in those policies. For example, property damage caused by a cyber incident may or may not be covered within the organization's property policy.

12 Selection of insurer

The understanding of cyber risk exposure and cyber insurance coverage should help organizations to select the best insurer and to get real value from its cyber insurance policy. The selection of insurer is part of the internal processes of the organization and should be effectively becomes part of its risk management strategy.

The selection of insurer requires organizations to understand cyber insurance coverage and to ensure their cyber insurance policy meets their business needs before negotiations begin. It is crucial for an organization to look at cyber insurance coverage because:

– it may vary and may affect how an insurance policy responds in the event of a specific cyber breach;

– it helps clarify potential gaps and overlaps between the coverage under a cyber insurance policy and other types of insurance cover.

The organization should select the insurer through an internal procurement process. When selecting an insurer, the organization should consider the following non-exhaustive list:

a) technical capability of the insurer, its track record, experience in cyber insurance, retention, capacity and their reinsurance partners;

b) ensure the insurer has the capability to issue a local insurance policy:

c) claims payment ability and process;

d) financial stability and performance rating, shareholders;

e) referenced clients;

f) other applicable internal, regulatory and legislation requirements.

13 Assessment by the insurer

Wherever applicable, the organization should select a policy based on an assessment of its context and its management of applicable cyber risks.

The insurer should perform an assessment to understand the context of the organization and how it manages cyber risks. The assessment may include a number of questions regarding the steps that the organization has taken to safeguard the data, such as:

a) internal governance procedures;

b) risk profile;

c) extent and nature of cyber risk;

d) frequency of attack;

e) country and location of business operations;

f) cyber incident history;

g) other underwriting information.

The insurer could build its assessment using cyber rating information that needs to be certified by a relevant national accreditation body and to be commonly agreed between the parties. Moreover, for transparency and integrity purposes, it is recommended that the organization delivering the cyber rating benefit from a certification according to [b-ISO 9001] on its quality management and to [b-ISO/IEC 27001] on its information security management, within the scope of the concerned processes.

The organization should implement the security measures that have been declared in the assessment to avoid refusal of a claim when the policy is effective.

The organization should ensure the insurer sign a non-disclosure agreement (NDA) before exchanging information.

The organization may request the insurer to appoint an independent certified professional or counsel for the purposes of insurer verification.

Appendix II is an example of the contents of an underwriting form.

14 Evaluation of insurer

When evaluating a cyber insurance proposal from an insurer, the organization should consider at least the issues specified in clauses 14.1 to 14.5.

14.1 Insurance coverage

The organization should ensure that insurance coverage includes:

a) first party loss coverage (see clause 10.1);

b) third party liability coverage (see clause 10.2);

c) other associated risks that should be transferred to the insurer.

14.2 Exclusion

The exclusion clause varies according to insurer. The organization should evaluate the clauses specified by insurers containing exclusions other than the common ones listed in clause 10.5.

14.3 Excess or waiting period

In general, the higher the excess and waiting period, the lower is the insurance premium.

14.4 Premium

The organization should be aware of the premium warranty period and pay in full before the end of the premium warranty period.

14.5 Claim information

The insurer should specify the claim information to be provided by the organization when filing a claim after a cyber incident. The claim information can be subject to refinement during negotiation of a cyber insurance policy. The insured should update such information as necessary to facilitate the claim process. Claim information may include descriptions of:

a) the cyber incident;

b) incident response;

c) financial aspects (including payment of excess or deductibles) and other impacts on the insured and third parties.

15 Renewal and termination

The insured should conduct risk assessment as stated in clause 8, as well as selection of insurer as in clause 12 before policy renewal.

The insured should also include their own performance review of the insurer periodically.

The insured should serve a written notice to the insurer in the event of termination of policy. The insurer should refund any prorated premium based on the remaining policy period.

Appendix I

Types of cost of first party loss

(This appendix does not form an integral part of this Recommendation.)

I.1 Extortion payment costs

An information security incident may involve demands for a ransom that constitutes extortion against the insured. The insured may have to pay a ransom demand in exchange for a decryption key to unlock the information asset or to stop the publication of information stolen or copied from the insured.

A cyber extortion event means any credible threat or connected series of threats made by a third party against the insured for the purpose of demanding monies from the insured by expressing their intent to:

a) release, divulge, disseminate, destroy or use confidential or proprietary information, or PII, stored on a computer system of the insured;

b) alter, corrupt, damage, manipulate, misappropriate, delete or destroy data, instructions or any electronic information transmitted or stored on a computer system of the insured;

c) introduce any malware that is designed to modify, alter, damage, destroy, delete, contaminate or degrade the integrity, quality or performance of data, applications, network or operating system and related software;

d) initiate an attack on a computer system of the insured that depletes its resources or impedes system access available through the Internet to authorized users of the system;

e) introduce malware or other material for the purpose of denying access by authorized users to a computer system of the insured; or

f) restrict or inhibit access to a computer system of the insured.

I.2 Customer protection costs

An information security incident that results in loss of customer information can result in a requirement for the insured to provide a form of external protection service (i.e., credit watch) for a specified period of time on behalf of each of its impacted customers.

I.3 External entity payment costs

An information security incident can result in financial obligations to external entities, e.g., paying the costs of a supplier to remediate any damage to its IT and operational technology (OT) after an information security incident. An information security incident can impact on a supplier resulting in disruption to the business of the insured with possible damaging effects.

I.4 Customer notification costs

Often an information security incident involves customer data and could potentially impact on the customers of an organization. Where customer information is involved, it is likely that customers, as well as regulators, will seek responses to questions about the extent of the information security incident and the steps taken to minimize the damage that has already been done.

Where such an information security incident occurs, an insured incurs costs associated with notifying the affected individuals when their information has been impacted. These costs can include the need to establish a special information security incident customer call centre to handle enquiries from notified individuals.

I.5 Specialist expertise costs

An information security incident can raise complex issues that incur costs associated with the engagement of a specialist individual or team to assist the insured to respond adequately. For example, an information security incident can be associated with national and international legislative requirements that require specialist knowledge to determine how best to comply. Another example could be to assist the insured in drafting incident communication documents and notification letters to impacted customers.

I.6 Incident or crisis management response costs

Costs can be incurred to manage a response to a cyber incident and contain the business impact of the incident, e.g:

a) with the redirection of existing IT experts away from normal duties to being part of a rapid response team to consult with the insured; and

b) special resources to assist the insured through an information security incident, including the establishment of a special information security incident 24/7 hotline and associated call centre to handle enquiries from notified individuals.

I.7 Legislative and regulatory litigation, expense, and settlement costs

An information security incident can result in legal action that incurs defence costs and associated expenses arising from regulatory proceedings not related to compensatory awards. An information security incident can also result in costs associated with civil penalties and other compensatory awards decided by a legal system.

I.8 Investigation and financial penalty costs

An information security incident can result in an insured being subject to forensic investigation costs, defence costs, regulatory penalties and fines resulting from an investigation or enforcement action by a regulator as a result of security and privacy liability.

I.9 Credit or identity theft monitoring costs

When an information security incident occurs, customers are more susceptible to risks such as identity or medical fraud. Expenses incurred to provide a credit- or identity theft-monitoring programme decrease this exposure in providing such monitoring services for a specified period of time. Additionally, legal, postage and advertising expenses, where there is a legal or regulatory requirement to notify individuals of a security or privacy incident, including credit-monitoring programme costs and PR media assistance can also be incurred.

I.10 Loss of external information costs

An information security incident can result in liability for damage to, or corruption or loss of, an external information vendor or supplier, including payment of compensation to customers for denial of access, or other errors in the integrity of the information assets.

I.11 Consequential costs

Consequential (also termed "indirect") costs are those associated with the inability to use business property or equipment after an information security incident and the associated PR expenses. The organization can also be involved in lawsuits brought by stakeholders, customers or other parties as a result of cyber incidents and data breaches, which can result in legal and compensation costs.

Appendix II

Example of underwriting contents

(This appendix does not form an integral part of this Recommendation.)

II.1 Policy schedule

a) Name of insured.
b) Principal address.
c) Policy period: effective date or time applicable to the principal address.
d) Aggregate limit of liability.
e) Limit of liability: List of insured items and sub-limits, if applicable.
f) Deductible: List of insured items and sub-limits, if applicable.
g) Waiting period.
h) Premium.

II.2 Insurance policy

a) Insuring clauses.
b) Extensions.
c) General definitions.
d) General exclusions.
e) General conditions.

Bibliography

[b-ITU-T X.1051] Recommendation ITU-T X.1051 (2016) | ISO/IEC 27011:2016, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations*.

[b-ISO 9001] ISO 9001:2015, *Quality management systems – Requirements*.

[b-ISO/IEC 27001] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*.

[b-ISO/IEC 27002] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*.

[b-ISO/IEC 27102] ISO/IEC 27102:2019, *Information security management – Guidelines for cyber insurance*.

[b-PMBOK Guide] Project Management Institute (2013). *A guide to the project management body of knowledge* (PMBOK® Guide), fifth edition. Newtown Square, PA: Project Management Institute.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021