

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

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

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/>.

© ITU 2021

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms	2
5	Conventions	2
6	Overview	2
7	Cyber insurance considerations	3
	7.1 Identify the cyber risks	3
	7.2 Understand the policy coverage	3
	7.3 Consult cyber insurance expert	3
	7.4 Understand the claim process.....	3
	7.5 Understand other insurance benefits	3
8	Cybersecurity risk assessments	3
9	Cyber insurance policy	4
10	Cyber insurance policy coverage.....	4
	10.1 First party loss coverage.....	4
	10.2 Third party liability coverage	5
	10.3 Limit of liability	6
	10.4 Cyber insurance excess.....	6
	10.5 Policy exclusion.....	6
11	Silent cyber coverage.....	7
12	Selection of insurer	7
13	Assessment by the insurer	8
14	Evaluation of insurer.....	8
	14.1 Insurance coverage	8
	14.2 Exclusion	8
	14.3 Excess or waiting period	9
	14.4 Premium	9
	14.5 Claim information	9
15	Renewal and termination	9
	Appendix I – Types of cost of first party loss.....	10
	I.1 Extortion payment costs	10
	I.2 Customer protection costs	10
	I.3 External entity payment costs.....	10
	I.4 Customer notification costs	10

	Page
I.5 Specialist expertise costs	11
I.6 Incident or crisis management response costs.....	11
I.7 Legislative and regulatory litigation, expense, and settlement costs.....	11
I.8 Investigation and financial penalty costs.....	11
I.9 Credit or identity theft monitoring costs	11
I.10 Loss of external information costs	11
I.11 Consequential costs	11
Appendix II – Example of underwriting contents.....	12
II.1 Policy schedule	12
II.2 Insurance policy.....	12
Bibliography.....	13

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].