International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1208

(01/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Cybersecurity

A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies

Recommendation ITU-T X.1208

Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1208 2014

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	
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	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	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
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

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

Documents
Document Sharing Hub

Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS

Licensee=/, User=,
Not for Resale,

Full document details: ITU-T X.1208 2014

Recommendation ITU-T X.1208

A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies

Summary

Recommendation ITU-T X.1208 describes a methodology for organizations to use cybersecurity indicators when computing a risk measure and it provides a list of potential cybersecurity indicators.

Recommendation ITU-T X.1208 is intended to help organizations that implement or operate a portion of the global infrastructure of information and communication technologies to evaluate their own cybersecurity capability and risk. These guidelines are intended to facilitate the decision-making process within organizations on how to lower their risks and how to identify where they could/should invest resources to improve their cybersecurity capabilities.

Recommendation ITU-T X.1208 does not propose the use of an index or a single indicator to express the cybersecurity capabilities of an organization.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1208	2014-01-24	17	11.1002/1000/11950

Keywords

Cybersecurity indicator, cybersecurity indicator of risk

* 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.

Documents
Document Sharing Hub
Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1208 2014

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, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

© ITU 2014

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

Documents
Document Sharing Hub

Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1208 2014

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation	3
4	Abbreviations and acronyms	3
5	Conventions	4
6	Cybersecurity indicator	4
6.1	Introduction	4
6.2	General principles for cybersecurity indicators	5
6.3	Guidelines for selecting cybersecurity indicators	6
6.4	Classification of indicators	6
7	Cybersecurity indicator development process	7
7.1	Introduction	7
7.2	Methodology for the construction of a cybersecurity indicator suite	7
7.3	Cybersecurity indicators' development process	8
8	Potential cybersecurity indicators	9
Appendix I – Examples of indicators of information security risk measures and metrics		25
Appendix II – Classifying indicators by nature		26
Appendix III – Experimental indicators		29
Bibliography		33

--`,,```,,,,````-`-`,,`,,`,`,,`---
Documents
Document Sharing Hub
Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1208 2014

Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Full document details: ITU-T X.1208 2014

Licensee=/, User=,
Not for Resale,

Documents
Document Sharing Hub

Recommendation ITU-T X.1208

A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies

1 Scope

This Recommendation provides a guideline to assist organizations in the development, selection and identification of the data to be captured (based on selected indicators) and shows how this information can be used to compute a cybersecurity indicator of risk (CSIR). Note that an organization may generate a cybersecurity indicator of risk with respect to a specific set of cybersecurity indicators (CSI) while departments within an organization may also generate a cybersecurity indicator of risk with respect to their specific set of cybersecurity indicators (CSI). The purpose of the cybersecurity indicator is to allow for the evaluation of the level of cybersecurity competency at a particular point in time of an organization and, when this process is repeated at other points in time, it allows the status of an organization's cybersecurity programme's progress over time to be determined.

This Recommendation also provides a list of potential indicators and describes a methodology to be used when these cybersecurity indicators are used to compute a cybersecurity indicator of risk.

This Recommendation is intended to help organizations that implement or operate a portion of the global infrastructure of information and communication technologies to evaluate their own cybersecurity capabilities and calculate their cybersecurity indicator of risk. These guidelines are intended to facilitate the decision-making process within organizations on how to improve cybersecurity and how to lower their cybersecurity risks. Furthermore, these guidelines provide an indication of where organizations could/should invest resources to improve their cybersecurity.

This Recommendation is not to be used to generate a cybersecurity indicator of risk on a country-level basis. Furthermore, this Recommendation does not propose the use of an index or a single indicator to express the cybersecurity capabilities of an organization (see clause 6.1).

NOTE 1 – Comparisons of the calculated cybersecurity indicator of risk between organizations should not be made. This is because each organization or community is supposed to select what they deem to be an appropriate set of cybersecurity indicators for their organization. Furthermore, they are expected to develop their own measurement methodology and criteria to address their risks and concerns. In some cases subjective information, as opposed to objective data, may be used. Consequently, it is recommended that a cybersecurity indicator of risk for one organization should never be compared to that of another organization, as it is highly context dependent.

NOTE 2 – The indicators described in this Recommendation may not be compatible with those developed by other industry sectors due to the different purposes of those industries.

2 References

None.

Documents
Document Sharing Hub
Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1208 2014

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 audit [b-ITU-T X.800]: An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.

3.1.2 bot [b-ITU-T X-Sup.8]: An automated software program used to carry out specific tasks designed for malicious purposes. It is interchangeable with a robot.

3.1.3 cybersecurity [b-ITU-T X.1205]: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

– Availability

– Integrity, which may include authenticity and non-repudiation

– Confidentiality.

3.1. 4 measurement [b-ENISA]: The act or the process of measuring, where the value of a quantitative variable in comparison to a (standard) unit of measurement is determined.

3.1.5 metric [b-ENISA]: A system of related measuring enabling quantification of some characteristic of a system, component or process. A metric is composed of two or more measures.

3.1.6 patch [b-ITU-T X.1206]: A broadly released fix for a product-specific, security-related vulnerability. A method of updating a file that replaces only the parts being changed, rather than the entire file.

3.1.7 personally identifiable information (PII) [b-ITU-T X.1252]: Any information a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains; b) from which identification or contact information of an individual person can be derived; or c) that is or can be linked to a natural person directly or indirectly.

3.1.8 risk [b-ISO/IEC 27000]: Effect of uncertainty on objectives.

3.1.9 risk management [b-ISO/IEC 27000]: Coordinated activities to direct and control an organization with regard to risk.

3.1.10 security certificate [b-ITU-T X.810]: A set of security-relevant data issued by a security authority or a trusted third party, together with security information which is used to provide the integrity and data origin authentication services for the data.

3.1.11 security controls [b-NIST FIPS 199]: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

3.1.12 security incident [b-ITU-T E.409]: A security incident is any adverse event whereby some aspect of security could be threatened.

Documents
Document Sharing Hub
Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1208 2014

3.1.13 spam [b-ITU-T X.1242]: The electronic information delivered from senders to recipients by terminals such as computers, mobile phones, telephones, etc., which is usually unsolicited, unwanted, and harmful for recipients.

3.1.14 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.15 vulnerability [b-ITU-T X.1500]: Any weakness that could be exploited to violate a system or the information it contains. (Aligned with Annex A of [b-ITU-T X.800].)

3.1.16 weakness [b-ITU-T X.1500]: A shortcoming or imperfection that, while not itself being recognized as a vulnerability, could, at some point become a vulnerability, or could contribute to the introduction of other vulnerabilities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cybersecurity indicator: Any one of a collection of indicators used to calculate or measure the risk status of a cybersecurity capability or competence for an organization or community.

NOTE − Selected cybersecurity indicators are indicators that are selected because they are relevant, i.e., they are related in some fashion to the risk concerns.

3.2.2 cybersecurity indicator of risk: The result from implementing a methodology that computes a cybersecurity indicator of risk.

3.2.3 cybersecurity indicator suite: A selected set of cybersecurity indicators that will be used to compute a cybersecurity indicator of risk.

NOTE – There is not one unique cybersecurity indicator suite.

3.2.4 indicator: It is interchangeable with metric in clause 3.1.5.

3.2.5 information security management system: Part of the overall management system, based on a business risk approach to establish, implement, operate, monitor, review, maintain and improve information security, see clause 3.2.1 of [b-ISO/IEC 27000].

NOTE − The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

3.2.6 programme: A series of coordinated activities aimed at achieving a clear business objective.

3.2.7 program: A set of coded instructions that enables a machine, especially a computer, to perform a desired sequence of operations.

3.2.8 threat source: It is either the intent and method which makes use of an intentional exploitation of a vulnerability or the situation and method that may accidentally trigger a vulnerability.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AS Autonomous System

BSA Business Software Alliance

C&A Certified and Accredited

CIS Center for Internet Security

CSI Cybersecurity Indicator

Documents
Document Sharing Hub
Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1208 2014

CSIR	Cybersecurity Indicator of Risk
CVE	Common Vulnerabilities and Exposures
CYBEX	Cybersecurity information Exchange
DB	Database
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DoS	Denial-of-Service
DNS	Domain Name System
GDP	Gross Domestic Product
ICT	Information and Communication Technology
ID	Identifier
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISMS	Information Security Management System
IT	Information Technology
PCA	Principal Components Analysis
PII	Personally Identifiable Information
SSL	Secure Socket Layer
TLS	Transport Layer Security
TTP	Trusted Third Party

5 Conventions

In this Recommendation, the term organization is intended to be interpreted in a broad sense. It is to be understood that a community should be considered as being included in the term organization. However, organization should never be considered to be equivalent to country.

6 Cybersecurity indicator

6.1 Introduction

Numerous efforts have been made to measure information and communication technology (ICT) performance, track progress and evaluate the impact of the use of ICTs on governments, operators, researchers and industries. Examples of these sector-specific indicators include the Global Cloud Computing Scorecard [b-BSA] and the security metrics published by the Center for Internet Security [b-CIS]. The indicators in this Recommendation are focused on some aspects of cybersecurity.

Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1208 2014
Documents
Document Sharing Hub

The cybersecurity indicator of risk described in this Recommendation consists of multiple cybersecurity indicators combined into a risk measure describing the current risk posture of cybersecurity capabilities and their effectiveness, as well as the efficiency of the implementation of security controls for an organization or a community.

There are two separate conditions under which a cybersecurity indicator of risk measure could be calculated, a self-evaluation of its cybersecurity capabilities or the collection of indicators calculated by some external third party organization. This Recommendation is intended for use for self-evaluation by organizations.

The indicators in this Recommendation may be selected by taking into account International Standards on the information security management system [b-ISO/IEC 27001], [b-ISO/IEC 27002], [b-ISO/IEC 27003], network security [b-ISO/IEC 27033-1], [b-ISO/IEC 27033-2], [b-ISO/IEC 27033-4] and other specifications [b-NIST SP 800-27], [b-NIST SP 800-30], [b-NIST SP 800-53]. The management related international standards allow organizations to design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk. The network security related international standards define and describe the concepts associated with, and provides management guidance on, network security. The other specifications provide the basic concept of controls to mitigate the risks for the information asset and how to manage the risks in the organizations' ICT environment.

The indicators may be grouped according to business functions: incident management, vulnerability management, patch management, application security, configuration management, and a financial category.

This Recommendation does not propose the use of an index or a single indicator to express the cybersecurity capabilities of an organization. This is because the security of an organization is only as good as its weakest link and the use of an index to express the organization cybersecurity capabilities does not properly identify the potential impacts resulting from the weakest link. If a cybersecurity indicator of risk is presented as a single number it can mislead those who are expected to use the number, it could also create false expectations in those who are expected to use this number in decision-making processes. Specifically, when a number of indicators are aggregated and normalized to a single number (i.e., index), the existence and significance of cybersecurity weaknesses of an organization are no longer obvious. Thus it would be inappropriate to use this index to either indicate that the cybersecurity capabilities of an organization are satisfactory or to consider using this cybersecurity index to compare the cybersecurity capabilities of different organizations.

6.2 General principles for cybersecurity indicators

This clause describes the general principles that should be considered when developing cybersecurity indicators.

- Preference should be given to the use of a globally agreed-upon set of indicators when calculating a cybersecurity indicator of risk.
- Cybersecurity indicators should be selected so that they can be used to measure the current status of cybersecurity competence against threats or to measure the progress of an information security programme for an organization or a community.
- Cybersecurity indicators should be selected that allow for accuracy and confidentiality of the raw data which is to be collected and used as a basis for the computation of the cybersecurity indicator of risk.
- Collection processes must retain the integrity of the raw data, which is to be used as a basis for the computation of the cybersecurity indicator of risk.

Documents
Document Sharing Hub
Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1208 2014

- Preference should also be given to the use of indicators that may help policy makers measure the performance of information security policy implementation and track the progress of a cybersecurity programme.
- New additional indicators should be developed or existing ones should be updated in a timely fashion in response to fast changing ICT services and technologies.

6.3 Guidelines for selecting cybersecurity indicators

When selecting indicators which are to be used to calculate a cybersecurity indicator of risk, it may be necessary for an organization to select indicators that facilitate meeting the goals and objectives of an organization. For example, organizations can select indicators based on the business functions of high priority.

In particular, a cybersecurity indicator should allow for:

- the measurement of the major impact on performance results;
- its use to address issues at the system level, the programme level and both levels, as appropriate;
- the measurement of the progress in implementing a cybersecurity programme, specific security controls and associated cybersecurity policies and procedures;
- the measurement of aspects which would allow for the identification of effectiveness and efficiency in a cybersecurity programme;
- the measurement of the positive or negative impact of a cybersecurity programme on an organization's mission;
- the measurement of the status of cybersecurity policy performance, with the ability to obtain results at the system level, the programme level or both levels;
- the measurement of the positive and negative impacts on the daily life of users.

Furthermore, a cybersecurity indicator should be selected which would allow for the collection of raw data in an accurate and reliable manner. In the entire measurement process, there is a need for ensuring that raw data can be made available, the integrity of the data being used and that privacy protection of the data is available.

6.4 Classification of indicators

There are three types of indicators according to the nature of indicators: implementation, effectiveness/efficiency and impact. Implementation indicators are used to demonstrate the progress in implementing an information security programme, specific security countermeasures and associated security policies and procedures. They can be grouped into two sub-types: programme-level implementation indicators and system-level indicators. Examples of implementation indicators related to the system level include the percentage of information systems security personnel who have received security training.

Effectiveness/efficiency indicators can used to check if programme-level processes and system-level security controls are implemented properly, whether they are operating as intended and if they satisfy the desired goals and objectives. They deal with two aspects of security control implementation results: effectiveness and efficiency of the result, i.e., effectiveness addresses robustness and efficiency addresses timeliness. Examples of the effectiveness indicator include the percentage of information security incidents caused by improperly configured access control; examples of the efficiency indicators include the percentage of system components that undergo maintenance on schedule.

Documents
Document Sharing Hub
Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1208 2014

Impact indicators can be used to specify the impact of information security on the mission of an organization. They can be used to quantify the cost saving produced by the information security programme or the costs incurred in addressing the information security incident, the degree of public trust obtained by the information security programme, or other mission-related impacts of information security. Examples of the impact indicators include the percentage of an organization's information security expenditure to the total information system expenditure.

In addition, indicators can be grouped according to business functions: incident management, vulnerability management, patch management, application security, configuration security, financial metrics, data and network security, etc.

7 Cybersecurity indicator development process

7.1 Introduction

The suite of cybersecurity indicators should be regarded as a key toolkit that can be used to evaluate the validity of enforcing the information security policy and to figure out the current status of information security in an organization.

7.2 Methodology for the construction of a cybersecurity indicator suite

The development of a cybersecurity indicator suite is a complex task and it needs to be undertaken by highly skilled professionals with knowledge of economics, cybersecurity and statistics. The development of the list of cybersecurity indicators needs to be based on the context of the organization and the different aspects of the risk(s) to be measured.

A developer of cybersecurity indicators should take into account that a given indicator may experience significant variability, unlike indicators with large samples, due to the scarce nature of samples being measured, e.g., incidents, which may be observed in a limited scale. Consequently, macroscopic analysis would have to be applied with extreme care.

The following steps can be used for the development of a cybersecurity indicator suite and to make the information ready for use:

- identification of the key indicators to be selected and used to compute the cybersecurity indicator of risk;
- identification of data sources;
- dealing with missing observations;
- making the indicators comparable to each other;
- converting the indicators into risk measurement values;
- leveraging a collection of the risk measurement values.

7.2.1 Selection of indicators to construct a risk measure

The selection of indicators to construct a risk measure is dependent on what is being measured, as well as the practicality of collecting the raw data.

NOTE – Although it may not be currently practical to make a measurement, an indicator may still be given serious consideration for selection. It is possible that this process can be used to identify a new work activity to allow for the capture of data so that risk can be properly evaluated.

The number of indicators may depend on the mission and objectives of the organization or the type of technologies being used by the organization. The use of a broad selection of indicators (for example, 10 to 30 indicators) to construct the risk measure of a cybersecurity indicator of risk is recommended. Mixing subjective indicators with objective measurements can influence the validity of the resultant computation. Therefore, avoiding the use of subjective indicators in the construction of a cybersecurity indicator of risk is recommended. However, in some areas of risk management a

Documents
Document Sharing Hub
Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1208 2014