TECHNICAL CODE

INFORMATION AND NETWORK SECURITY - CYBER INSURANCE ACQUISITION

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date:

4 October 2019

MCMC MTSFB TC G020:2019

Development of technical codes

The Communications and Multimedia Act 1998 ('the Act') provides for Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirement for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd (MTSFB) as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
http://www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Malaysian Communications & Multimedia Commission (MCMC)
Off Persiaran Multimedia
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8320 0300
Fax: +60 3 8322 0115
http://www.mtsfb.org.my

Contents

Committee representation

This technical code was developed by Trust and Privacy Sub Working Group which supervised by Security, Trust and Privacy Working Group under the Malaysian Technical Standards Forum Bhd (MTSFB) consists of representatives from the following organisations:

Celcom Axiata Berhad

CyberSecurity Malaysia

Jardine Lloyd Thompson Specialty Pte Ltd

K2 Baseline Sdn Bhd

KPMG Management & Risk Consulting Sdn Bhd

Malaysia Digital Economy Corporation Sdn Bhd

Maxis Communications Berhad

MIMOS Berhad

Ministry of Energy, Science, Technology, Environment and Climate Change

Provintell Technologies Sdn Bhd

Telekom Applied Business Sdn Bhd

Telekom Malaysia Berhad

Foreword

This technical code for Information and Network Security - Cyber Insurance Acquisition (‘this ‘Technical Code’) was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Security, Trust and Privacy Working Group.

This Technical Code provides a requirement based on ISO/IEC DIS 27102.

This Technical Code shall continue to be valid and effective until reviewed or cancelled.

INFORMATION AND NETWORK SECURITY - CYBER INSURANCE ACQUISITION

0. Introduction

The threat of a cyber-attack against an organisation is very real and an organisation is not easily able to predict when a cyber security attack will occur. An organisation's information assets are under constant attack as cyber security threats become more pervasive, persistent and sophisticated. Adverse events including cyber hacktivism, cyber extortion and cyber terrorism continue to cause disruptions to organisations and are publicly scrutinised.

The adoption of cyber insurance is to reduce the impacts of a cyber incident that shall be considered by organisations in addition to information security controls as part of effective risk management and risk treatment approach.

This Technical Code specifies the adoption of cyber insurance as a risk treatment option to manage the impact of a cyber security incident with an insurer within the framework of the organisation's information security risk management framework.

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

1. Scope

This Technical Code specifies requirements for:

a) assisting information security professionals to use cyber insurance as an option for risk treatment;

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

c) leveraging cyber insurance to help manage the impact of a cyber incident; and

d) leveraging a risk assessment results to share relevant data and information with insurers.

This Technical Code is applicable to organisations of all types, sizes and nature.

2. Normative references

The following normative references are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

MCMC MTSFB TC G009, *Information and Network Security - Requirement*s

3. Abbreviations

For the purposes of this technical code, the following abbreviations apply.

IT Information Technology

OT Operation Technology

PR Public Relationship

PII Personal Identifiable Information

NDA Non-Disclosure Agreement

4. Terms and definitions

For the purposes of this Technical Code, the following terms and definitions apply.

4.1 Cyber incident

Any cyber act or circumstance that produces a consequence resulting in a loss of preservation of confidentiality, integrity, or availability of an organisation's information technology, information processing systems and Operational Technology (OT).

NOTE: OT is the hardware and software that forms industrial control systems.

4.2 Cyber insurance

Insurance that covers loss to an insured caused by cyber incidents.

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

4.3 Excess

Sum of money that the organisation will pay in an insurance claim before the insurance coverage starts paying out. The sum of money is known as retention amount, which is to be borne by the insured, and shall remain uninsured.

4.4 Insured

Organisation covered by insurance.

4.5 Insurer

A company that underwrites an insurance risk which the party in an insurance contract undertaking to pay compensation.

4.6 Premium warranty

Under the premium warranty clause, the insured is required to pay the premiums charged for the insurance within the stipulated duration from the effective date of insurance cover which is shown on the policy, cover note, and/or renewal certificates.

4.7 Silent cyber risk

Silent cyber risk refers to potential cyber exposures contained within traditional property and liability insurance policies, which may not implicitly include or exclude cyber risks.

4.8 Waiting period

Cyber insurance policies that include a waiting period before the business interruption coverage begins to apply. The length of waiting period to be agreed before the inception of cyber insurance policy.

5. Cyber insurance

5.1 Overview

Cyber insurance is a risk transfer option that should be used to manage the impact of cyber and data breach incidents. Contractual terms for cyber insurance are given in a cyber insurance policy. A cyber insurance policy is typically stand-alone policy or together with other insurance policy. Cyber insurance shall be used to protect an insured against any potential losses associated with a cyber incident and data breach.

Cyber insurance is adopted to assist the insured to minimise 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 organisation shall be aware that cyber insurance does not reduce the likelihood of occurrence of risks that are being transferred.

5.2 Silent cyber coverage in other insurance policies

There are cyber related incidents that may already be covered within other insurance policies of the organisation obtained earlier. Therefore, the organisation shall consider potential coverage as well as exclusions of cyber risks in those policies. For example, property damage caused by a cyber incident may be covered within the organisation's property policy.

5.3 Coverage of cyber insurance policy

The coverage varies depending on organisation's needs and its risk profile.

The cyber insurance coverage is grouped into 2 primary types of cyber insurance policy categories which are as follows:

a) first party loss; and

b) third party liability.

5.3.1 First party loss coverage

Any losses incurred by the insured shall include the following coverage but not limited to:

a) Business interruption

To pay for business interruption loss arising from business interruption incident.

b) Incident response

Reasonable and necessary expenses incurred by the insured in a cyber event/incident.

c) Data restoration

To pay for recovery costs by reason of a data asset incident.

d) Legal

An information security incident that results in legal actions which incur defence costs and associated expenses.

e) Cyber extortion

To provide coverage for cyber extortion damages and cyber extortion expenses, by reason of a cyber extortion event.

Incident response costs shall include legal, crisis management, incident handling and cyber forensics.

The organisation should also consider to include the costs of Public Relationship (PR), credit monitoring and customer notification. Annex A provides more information of first party losses.

5.3.2 Third party liability coverage

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

a) Privacy liability

To protect the insured from any legal expenses and damages arising out of a data breach (including Personal Identifiable Information (PII) and/or confidential information).

b) Network security liability

To protect the insured from any legal expenses and damages arising out of a cyber incident.

c) Media liability

To protect the insured from any legal expenses and damages arising out of negligence in insured's online media content and online advertising, including websites, blogs and social media.

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

Cyber insurance will indemnify the insured from any expenses in relation to a regulatory investigation. The organisation shall ensure that this coverage includes and is not limited to legal and forensic expenses.

5.4 Limit of liability

With each of the above areas reviewed and clarified, the organisation shall carefully determine and consider how much cyber insurance coverage to obtain. The amount of cyber insurance that the organisation can obtain varies depending on the organisation's financials, industry, operations, and risk exposures.

Cyber insurance policies should have excess, which is the sum of money the insured shall bear before the insurer begins to make a pay out within the cyber insurance policy.

Cyber insurance policies should have a waiting period, which is the period when the insured organisation shall bear before the insurer begins to make a pay out within the cyber insurance policy.

The excess and/or waiting period shall be agreed prior to the cyber insurance policy inception.

To assist an organisation to benchmark cyber security losses, there are a number of research organisations that regularly publish industry benchmark information on the cost of past cyber incidents around the world which should be evaluated to assist the insured to determine the appropriate amount of coverage to obtain.

5.5 Policy exclusion

The organisation shall be aware that a cyber insurance policy cannot cover all situations, as the coverage of protection may vary according to insurers. Some common exclusions of cyber insurance are as follows:

a) War, invasion and insurrection

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

b) Patent, software and copyright infringement

Patents, software, and copyright are covered by an intellectual property insurance policy, and not by a cyber policy.

c) Bodily injury and property damage

Data breach does not mean that the person is directly injured physically because of it and hence the claim is excluded. However, some policies do cover emotional distress and anguish caused by such events.

d) Infrastructure

Cyber incidents and data breaches due to any utilities and/or facilities failure.

e) Criminal actions

Cyber incident from actions by the insured that violate legal or regulatory requirements such as an unauthorised or wrongful collection of personal data.

f) Act of God

Natural disaster, including but not limited to flood, earthquake, landslide, lightning, wind or even fire are commonly excluded because that is not the intention of cyber insurance.

6. Cyber security risks assessments

The organisation shall conduct business impact analysis and risk assessment aligned with MCMC MTSFB TC G009. The organisation shall apply effective cyber security risk treatment process to determine the risk to be transferred to cyber insurance policies.

If the organisation is processing and storing data in the cloud and/or co-locate data centre, ensure that risk assessment covers the risks related to cloud and outsourcing**.**

7. Selection of insurer

The organisation shall select the insurer through an internal procurement process when selecting an insurer, the organisation shall consider the following but not limited to:

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

b) the insurer has the capability to issue local insurance policy;

c) claims payment ability and process;

d) financial stability and performance rating, shareholders;

e) referenced clients; and

f) other applicable internal, regulatory and legislative requirements.

8. Assessment by the insurer

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

The organisation should be assessed by the insurer, this is so that the insurer can understand the context of the organisation and how does the organisation manage the cyber risks. The assessment should include a number of questions regarding the steps that the organisation has taken to safeguard the data, such as:

a) internal governance procedures;

b) risk profile;

c) extend and nature of cyber risk;

d) frequency of attack;

e) country and location of business operations;

f) cyber incidents history; and

g) other underwriting information.

Annex B is the sample contents of underwriting form.

The organisation shall implement the security measures that have been declared in the assessment to avoid denial of claim when the policy is effective.

The organisation shall ensure the insurer sign Non-Disclosure Agreement (NDA) before exchanging information.

The organisation may request the insurer to appoint an independent certified professional and/or counsel for the purposes of insurer's verifications.

9. Evaluation

9.1 Insurance coverage, exclusion, excess and premium

When evaluating the cyber insurance proposal from the insurers, the organisation shall consider the following items but not limited to:

a) Insurance coverage

The organisation shall ensure the following insurance coverage is included in the evaluation:

i) first party loss coverage in 5.3.1;

ii) third party liability coverage in 5.3.2; and

iii) other associated risks that shall be transferred to the insurer.

b) Exclusion

The exclusion clauses vary from insurers. The organisation shall evaluate the clauses provided by the insurers other than the common exclusions stated in 5.5.

c) Excess

The excess varies due to a range of factors. The organisation should obtain multiple options with different excess for considerations. In general, the higher the excess and/or the waiting period, the lower the premium.

d) Premium

The organisation shall be aware of the premium warranty period and to pay in full before the end of premium warranty period.

e) Claim information

The information submitted by the insured during the claim process may include descriptions of:

i) the cyber incident;

ii) incident response; and

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

The insured shall maintain such information as necessary to facilitate the claims process.

9.2 Renewal and termination

The insured shall conduct risk assessment as stated in Clause 6 as well as selection of insurer as per Clause 7 before the policy renewal. The insured shall also include their own performance review of the insurer periodically.

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

Annex A
(informative)

Type of cost - First party loss

A.1 Extortion payment costs

An information security incident may involve demands for a ransom which involves 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.

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 personally identifiable information, stored on the insured's computer system;

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

c) introduce any malware which 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 the insured's computer system that depletes the system's resources or impedes system access available through the internet to authorised users of the system;

e) introduce malware or other material for the purpose of denying authorised users' access to the insured's computer system; or

f) restrict or inhibit access to your computer system.

A.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 defined period of time on behalf of each of its impacted customers.

A.3 External entity payment costs

An information security incident can result in financial obligations to external entities, for example paying the costs of a supplier to remediate any damage to the supplier's Information Technology (IT) and Operation Technology (OT) after an information security incident. An information security incident impacted a supplier that disrupted the insured's business and resulting in possible business impact.

A.4 Customer notification costs

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

Where such an information security incident occurs, an insured will incur 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 calls from the notified individuals.

A.5 Specialist expertise costs

An information security incident can raise complex issues that would incur costs associated with the engagement of a specialist individual or team to assist the insured respond adequately. For example, an information security incident can be associated with national and international legislative requirements which 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.

A.6 Incident or crisis management response costs

Costs can be incurred to manage a response to the cyber incident and contain the business impact of the incident, for example:

a) with the redirection of existing IT experts away from normal duties across 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 calls from the notified individuals.

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

An information security incident can result in legal actions which incur 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.

A.8 Investigation and financial penalty costs

An information security incident can result in an insured being subjected 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.

A.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 credit or identity theft monitoring program decrease this exposure in providing such monitoring services for a defined 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 program costs and public relations media assistance can also be incurred.

A.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.

A.11 Consequential costs

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

Annex B
(informative)

Example of underwriting contents

1. Policy schedule

    a) Name of insured: _____

    b) Principal address: _____

    c) Policy period (effective date/time applicable to the principal address): From __ to __

    d) Aggregate limit of liability: RM _____

    e) Limit of liability: List of insured item and sub-limits if applicable

    f) Deductible: List of insured item and sub-limits if applicable

    g) Waiting period: _____

    h) Premium: RM _____

2. Insurance policy

    a) Insuring clauses.

    b) Extensions.

    c) General definitions.

    d) General exclusions.

    e) General conditions.

Bibliography

[1] ISO/IEC 27001, *Information security management*

[2] ISO/IEC 27005, *Information technology - Security techniques - Information security risk management*

[3] ISO/IEC DIS 27102, *Information technology - Security techniques - Information security management guidelines for cyber insurance*

[4] *Commonality of risk assessment language in cyber insurance - Recommendations on Cyber Insurance,* ENISA

[5] *Cyber Insurance: Recent Advances, Good Practices and Challenges,* ENISA

[6] *Cyber Insurance Buying Guide,* FSSCC

[7] *Purchasers' Guide to Cyber Insurance Products,* FSSCC

[8] *Supporting an Effective Cyber Insurance Market - OECD Report for the G7 Presidency*, OECD

Acknowledgements

Members of the Trust and Privacy Sub Working Group

Mr Ong Yew Seng (Chairman)	Provintell Technologies Sdn Bhd
Ms Norkhadhra Nawawi/	Malaysian Technical Standards Forum Bhd
Ms Nor Iratul Munirah Mazani (Secretariat)	
Mr Raaj Kamal Kapoor	Celcom Axiata Berhad
Mr Lee Hwee Hsiung	CyberSecurity Malaysia
Ms Menaka Muthu	Jardine Lloyd Thompson Specialty Pte Ltd
Mr Cheng Wai Kok	K2 Baseline Sdn Bhd
Mr Azlan Mohamed Ghazali	KPMG Management & Risk Consulting Sdn Bhd
Ms Azurah Norahim/	Malaysia Digital Economy Corporation Sdn Bhd
Ms Nas Fatehah Mahadi/	
Ms Norlizawati Ghazali	
Mr Alan Neelagordan/	Maxis Communications Berhad
Mr Edymainoe Mohd Noh	
Mr Alwyn Goh	MIMOS Berhad
Ms Faridah Ibrahim	Ministry of Energy, Science, Technology, Environment and Climate Change
Mr Thaib Mustafa	Telekom Applied Business Sdn Bhd
Mr Muhamad Azahar Saidan Ahmad	Telekom Malaysia Berhad