INTERNATIONAL STANDARD

ISO/IEC 27032

First edition
2012-07-15

Information technology — Security techniques — Guidelines for cybersecurity

Technologies de l'information — Techniques de sécurité — Lignes directrices pour la cybersécurité

Reference number
ISO/IEC 27032:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27032 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

The Cyberspace is a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical information and communications technology (ICT) devices and connected networks. However there are security issues that are not covered by current information security, Internet security, network security and ICT security best practices as there are gaps between these domains, as well as a lack of communication between organizations and providers in the Cyberspace. This is because the devices and connected networks that have supported the Cyberspace have multiple owners, each with their own business, operational and regulatory concerns. The different focus placed by each organization and provider in the Cyberspace on relevant security domains where little or no input is taken from another organization or provider has resulted in a fragmented state of security for the Cyberspace.

As such, the first area of focus of this International Standard is to address Cyberspace security or Cybersecurity issues which concentrate on bridging the gaps between the different security domains in the Cyberspace. In particular this International Standard provides technical guidance for addressing common Cybersecurity risks, including:

— social engineering attacks;

— hacking;

— the proliferation of malicious software (“malware”);

— spyware; and

— other potentially unwanted software.

The technical guidance provides controls for addressing these risks, including controls for:

— preparing for attacks by, for example, malware, individual miscreants, or criminal organizations on the Internet;

— detecting and monitoring attacks; and

— responding to attacks.

The second area of focus of this International Standard is collaboration, as there is a need for efficient and effective information sharing, coordination and incident handling amongst stakeholders in the Cyberspace. This collaboration must be in a secure and reliable manner that also protects the privacy of the individuals concerned. Many of these stakeholders can reside in different geographical locations and time zones, and are likely to be governed by different regulatory requirements. Stakeholders include:

— consumers, which can be various types of organizations or individuals; and

— providers, which include service providers.

Thus, this International Standard also provides a framework for

— information sharing,

— coordination, and

— incident handling.

The framework includes

— key elements of considerations for establishing trust,

— necessary processes for collaboration and information exchange and sharing, as well as

— technical requirements for systems integration and interoperability between different stakeholders.

Given the scope of this International Standard, the controls provided are necessarily at a high level. Detailed technical specification standards and guidelines applicable to each area are referenced within this International Standard for further guidance.

Information technology — Security techniques — Guidelines for cybersecurity

1 Scope

This International Standard provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular:

— information security,

— network security,

— internet security, and

— critical information infrastructure protection (CIIP).

It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides:

— an overview of Cybersecurity,

— an explanation of the relationship between Cybersecurity and other types of security,

— a definition of stakeholders and a description of their roles in Cybersecurity,

— guidance for addressing common Cybersecurity issues, and

— a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

2 Applicability

2.1 Audience

This International Standard is applicable to providers of services in the Cyberspace. The audience, however, includes the consumers that use these services. Where organizations provide services in the Cyberspace to people for use at home or other organizations, they may need to prepare guidance based on this International Standard that contains additional explanations or examples sufficient to allow the reader to understand and act on it.

2.2 Limitations

This International Standard does not address:

— Cybersafety,

— Cybercrime,

— CIIP,

— Internet safety, and

— Internet related crime.

It is recognized that relationships exist between the domains mentioned and Cybersecurity. It is, however, beyond the scope of this International Standard to address these relationships, and the sharing of controls between these domains.

It is important to note that the concept of Cybercrime, although mentioned, is not addressed. This International Standard does not provide guidance on law-related aspects of the Cyberspace, or the regulation of Cybersecurity.

The guidance in this International Standard is limited to the realization of the Cyberspace on the Internet, including the endpoints. However, the extension of the Cyberspace to other spatial representations through communication media and platforms are not addressed, nor the physical security aspects of them.

EXAMPLE 1 Protection of the infrastructure elements, such as communications bearers, which underpin the Cyberspace are not addressed.

EXAMPLE 2 The physical security of mobile telephones that connect to the Cyberspace for content download and/or manipulation is not addressed.

EXAMPLE 3 Text messaging and voice chat functions provided for mobile telephones are not addressed.

3 Normative references

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

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, and the following apply.

4.1
adware
application which pushes advertising to users and/or gathers user online behaviour

NOTE The application may or may not be installed with the user's knowledge or consent or forced onto the user via licensing terms for other software.

4.2
application
IT solution, including application software, application data and procedures, designed to help an organization's users perform particular tasks or handle particular types of IT problems by automating a business process or function

[ISO/IEC 27034-1:2011]

4.3
application service provider
operator who provides a hosted software solution that provides application services which includes web based or client-server delivery models

EXAMPLE Online game operators, office application providers and online storage providers.

4.4
application services
software with functionality delivered on-demand to subscribers through an online model which includes web based or client-server applications

4.5
application software
software designed to help users perform particular tasks or handle particular types of problems, as distinct from software that controls the computer itself

[ISO/IEC 18019]

4.6
asset
anything that has value to an individual, an organization or a government

NOTE Adapted from ISO/IEC 27000 to make provision for individuals and the separation of governments from organizations (4.37).

4.7
avatar
representation of a person participating in the Cyberspace

NOTE 1 An avatar can also be referred to as the person's alter ego.

NOTE 2 An avatar can also be seen as an "object" representing the embodiment of the user.

4.8
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

[ISO/IEC 27000:2009]

4.9
attack potential
perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation

[ISO/IEC 15408-1:2005]

4.10
attack vector
path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome

4.11
blended attack
attack that seeks to maximize the severity of damage and speed of contagion by combining multiple attacking methods

4.12
bot
robot
automated software program used to carry out specific tasks

NOTE 1 The word is often used to describe programs, usually run on a server, that automate tasks such as forwarding or sorting e-mail.

NOTE 2 A bot is also described as a program that operates as an agent for a user or another program or simulates a human activity. On the Internet, the most ubiquitous bots are the programs, also called spiders or crawlers, which access websites and gather their content for search engine indexes.

4.13
botnet
remote control software, specifically a collection of malicious bots, that run autonomously or automatically on compromised computers

4.14
cookie
<access control> capability or ticket in an access control system

4.15
cookie
<IPSec> data exchanged by ISAKMP to prevent certain Denial-of-Service attacks during the establishment of a security association

4.16
cookie
<HTTP> data exchanged between an HTTP server and a browser to store state information on the client side and retrieve it later for server use

NOTE A web browser can be a client or a server.

4.17
control
countermeasure
means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature

[ISO/IEC 27000:2009]

NOTE ISO Guide 73:2009 defines control as simply a measure that is modifying risk.

4.18
Cybercrime
criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime

4.19
Cybersafety
condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable

NOTE 1 This can take the form of being protected from the event or from exposure to something that causes health or economic losses. It can include protection of people or of assets.

NOTE 2 Safety in general is also defined as the state of being certain that adverse effects will not be caused by some agent under defined conditions.

4.20
Cybersecurity
Cyberspace security
preservation of confidentiality, integrity and availability of information in the Cyberspace

NOTE 1 In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

NOTE 2 Adapted from the definition for information security in ISO/IEC 27000:2009.

4.21
the Cyberspace
complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form

4.22
Cyberspace application services
application services (4.4) provided over the Cyberspace

4.23
cyber-squatter
individuals or organizations that register and hold on to URLs that resemble references or names of other organizations in the real world or in the Cyberspace

4.24
deceptive software
software which performs activities on a user's computer without first notifying the user as to exactly what the software will do on the computer, or asking the user for consent to these actions

EXAMPLE 1 A program that hijacks user configurations.

EXAMPLE 2 A program that causes endless popup advertisements which cannot be easily stopped by the user.

EXAMPLE 3 Adware and spyware.

4.25
hacking
intentionally accessing a computer system without the authorization of the user or the owner

4.26
hactivism
hacking for a politically or socially motivated purpose

4.27
information asset
knowledge or data that has value to the individual or organization

NOTE Adapted from ISO/IEC 27000:2009.

4.28
internet
internetwork
collection of interconnected networks

NOTE 1 Adapted from ISO/IEC 27033-1:2009

NOTE 2 In this context, reference would be made to "an internet". There is a difference between the definition of "an internet" and "the Internet".

4.29
the Internet
global system of inter-connected networks in the public domain

[ISO/IEC 27033-1:2009]

NOTE There is a difference between the definition of "an internet" and "the Internet".

4.30
Internet crime
criminal activity where services or applications in the Internet are used for or are the target of a crime, or where the Internet is the source, tool, target, or place of a crime

4.31
Internet safety
condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Internet which could be considered non-desirable

4.32
Internet security
preservation of confidentiality, integrity and availability of information in the Internet

4.33
Internet services
services delivered to a user to enable access to the Internet via an assigned IP address, which typically include authentication, authorization and domain name services

4.34
Internet service provider
organization that provides Internet services to a user and enables its customers access to the Internet

NOTE Also sometimes referred to as an Internet access provider.

4.35
malware
malicious software
software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user's computer system

EXAMPLES Viruses, worms, trojans.

4.36
malicious contents
applications, documents, files, data or other resources that have malicious features or capabilities embedded, disguised or hidden in them

4.37
organization
group of people and facilities with an arrangement of responsibilities, authorities and relationships

[ISO 9000:2005]

NOTE 1 In the context of this International Standard, an individual is distinct from an organization.

NOTE 2 In general, a government is also an organization. In the context of this International Standard, governments can be considered separately from other organizations for clarity.

4.38
phishing
fraudulent process of attempting to acquire private or confidential information by masquerading as a trustworthy entity in an electronic communication

NOTE Phishing can be accomplished by using social engineering or technical deception.

4.39
physical asset
asset that has a tangible or material existence

NOTE Physical assets usually refer to cash, equipment, inventory and properties owned by the individual or organization. Software is considered an intangible asset, or a non-physical asset.

4.40
potentially unwanted software
deceptive software, including malicious and non-malicious software, that exhibits the characteristics of deceptive software

4.41
scam
fraud or confidence trick

4.42
spam
abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages

NOTE While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, web search engine spam, spam in blogs, wiki spam, mobile phone messaging spam, Internet forum spam and junk fax transmissions.

4.43
spyware
deceptive software that collects private or confidential information from a computer user

NOTE Information can include matters such as websites most frequently visited or more sensitive information such as passwords.

4.44
stakeholder
<risk management> person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

[ISO Guide 73:2009]

4.45
stakeholder
<system> individual or organization having a right, share, claim or interest in a system or in its possession of characteristics that meet their needs and expectations

[ISO/IEC 12207:2008]

4.46
threat
potential cause of an unwanted incident, which may result in harm to a system, individual or organization

NOTE Adapted from ISO/IEC 27000:2009.

4.47
trojan
trojan horse
malware that appears to perform a desirable function

4.48
unsolicited email
email that is not welcome, or was not requested, or invited

4.49
virtual asset
representation of an asset in the Cyberspace

NOTE In this context, currency can be defined as either a medium of exchange or a property that has value in a specific environment, such as a video game or a financial trading simulation exercise.

4.50
virtual currency
monetary virtual assets

4.51
virtual world
simulated environment accessed by multiple users through an online interface

NOTE 1 The simulated environments are often interactive.

NOTE 2 The physical world in which people live, and the related characteristics, will be referred to as the “real world” to differentiate it from a virtual world.

4.52
vulnerability
weakness of an asset or control that can be exploited by a threat

[ISO/IEC 27000:2009]

4.53
zombie
zombie computer
drone
computer containing hidden software that enables the machine to be controlled remotely, usually to perform an attack on another computer

NOTE Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious activities under remote direction.

5 Abbreviated terms

The following abbreviated terms are used in this International Standard.

AS	Autonomous System
AP	Access Point
CBT	Computer Based Training
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CSIRT	Computer Security Incident Response Team
CIIP	Critical Information Infrastructure Protection
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
HIDS	Host-based Intrusion Detection System
IAP	Independent Application Provider
ICMP	Internet Control Message Protocol
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IP	Internet Protocol
IPO	Information Providing Organization
IPS	Intrusion Prevention System
IRO	Information Receiving Organization
ISP	Internet Service Provider
ISV	Independent Software Vendor
IT	Information Technology
MMORPG	Massively Multiplayer Online Role-Playing Game
NDA	Non-Disclosure Agreement
SDLC	Software Development Life-cycle
SSID	Service Set Identifier

TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

6 Overview

6.1 Introduction

Security on the Internet and in the Cyberspace has been a subject of growing concern. Stakeholders have been establishing their presence in the Cyberspace through websites and are now attempting to further leverage the virtual world provided by the Cyberspace.

EXAMPLE Increasing numbers of individuals spend increasing amounts of time with their virtual avatars on MMORPGs.

While some individuals are careful in managing their online identity, most people are uploading details of their personal profiles to share with others. Profiles on many sites, in particular social networking sites and chat rooms, can be downloaded and stored by other parties. This can lead to the creation of a digital dossier of personal data that can be misused, disclosed to other parties, or used for secondary data collection. While the accuracy and integrity of this data are questionable, they create links to individuals and organizations that often cannot be completely erased. These developments in the communication, entertainment, transportation, shopping, financial, insurance, and healthcare domains create new risks to stakeholders in the Cyberspace. Thus, risks can be associated with loss of privacy.

The convergence of information and communication technologies, the ease of getting into the Cyberspace, and the narrowing of personal space between individuals are gaining the attention of individual miscreants and criminal organizations. These entities are using existing mechanisms, such as phishing, spam and spyware, as well as developing newer attack techniques, to exploit any weaknesses they can discover in the Cyberspace. In recent years, security attacks in the Cyberspace have evolved from hacking for personal fame to organized crime, or Cybercrime. A plethora of tools and processes previously observed in isolated Cybersecurity incidents are now being used together in multi-blended attacks, often with far reaching malicious objectives. These objectives range from personal attacks, identity theft, financial frauds or thefts, to political hactivism. Specialist forums to highlight potential security issues have also served to showcase attack techniques and criminal opportunities.

The multiple modes of business transactions that are carried out in the Cyberspace are becoming the target of Cybercrime syndicates. Ranging from business-to-business, business-to-consumer to consumer-to-consumer services, the risks posed are inherently complex. Concepts such as what constitute a transaction or an agreement are dependent on the interpretation of the law and how each party in the relationship manages their liability. Often, the issue of usage of data collected during the transaction or relationship is not addressed adequately. This can eventually lead to security concerns such as the leakage of information.

The legal and technical challenges posed by these Cybersecurity issues are far-reaching and global in nature. The challenges can only be addressed by having the information security technical community, legal community, nations and community of nations coming together through a coherent strategy. This strategy should take into account the role of each stakeholder and existing initiatives, within a framework of international cooperation.

EXAMPLE An example of a challenge sprouts from the fact that the Cyberspace affords virtual anonymity and stealth of attack, making detection difficult. This makes it increasingly difficult for individuals and organizations to establish trust and transact, as well as for law enforcement agencies to enforce related policies. Even if the source of attack can be determined, cross-border legal issues often prevent further progress for any investigation or legal repatriation.

Current progress to address these challenges has been hampered by many issues, and Cybersecurity issues are increasing and continuing to evolve.

While there is no lack of Cybersecurity threats, and as many, albeit not standardized, ways to counter them, the focus of this International Standard is on the following key issues:

— attacks by malicious and potentially unwanted software;

— social engineering attacks; and

— information sharing and coordination.

In addition, some Cybersecurity tools will be discussed briefly in this International Standard. These tools and areas closely relate to Cybercrime prevention, detection, response, and investigation. Further details can be found in Annex A.

6.2 The nature of the Cyberspace

The Cyberspace can be described as a virtual environment, which does not exist in any physical form, but rather, a complex environment or space resulting from the emergence of the Internet, plus the people, organizations, and activities on all sort of technology devices and networks that are connected to it. Cyberspace security, or Cybersecurity, is about the security of this virtual world.

Many virtual worlds have a virtual currency, such as used to purchase in-game items. There is an associated real world value to the virtual currency and even in-game items. These virtual items are frequently traded for real currency on online auction sites and some games even have an official channel with published virtual or real currency exchange rates for the monetization of virtual items. It is often these monetization channels which make these virtual worlds a target for attack, usually by phishing or other techniques for stealing account information.

6.3 The nature of Cybersecurity

Stakeholders in the Cyberspace have to play an active role, beyond protecting their own assets, in order for the usefulness of the Cyberspace to prevail. The applications within the Cyberspace are expanding beyond the business-to-consumers, and consumers-to-consumers models, to a form of many-to-many interactions and transactions. The requirements are expanding for individuals and organizations to be prepared to address the emerging security risks and challenges to effectively prevent and respond to misuse and criminal exploitations.

Cybersecurity relates to actions that stakeholders should be taking to establish and maintain security in the Cyberspace.

Cybersecurity relies on information security, application security, network security, and Internet security as fundamental building blocks. Cybersecurity is one of the activities necessary for CIIP, and, at the same time, adequate protection of critical infrastructure services contributes to the basic security needs (i.e., security, reliability and availability of critical infrastructure) for achieving the goals of Cybersecurity.

Cybersecurity is, however, not synonymous with Internet security, network security, application security, information security, or CIIP. It has a unique scope requiring stakeholders to play an active role in order to maintain, if not improve the usefulness and trustworthiness of the Cyberspace. This International Standard differentiates Cybersecurity and the other domains of security as follows:

— Information security is concerned with the protection of confidentiality, integrity, and availability of information in general, to serve the needs of the applicable information user.

— Application security is a process performed to apply controls and measurements to an organization's applications in order to manage the risk of using them. Controls and measurements may be applied to the application itself (its processes, components, software and results), to its data (configuration data, user data, organization data), and to all technology, processes and actors involved in the application's life cycle.

— Network security is concerned with the design, implementation, and operation of networks for achieving the purposes of information security on networks within organizations, between organizations, and between organizations and users.

— Internet security is concerned with protecting Internet-related services and related ICT systems and networks as an extension of network security in organizations and at home, to achieve the purpose of security. Internet security also ensures the availability and reliability of Internet services.

— CIIP is concerned with protecting the systems that are provided or operated by critical infrastructure providers, such as energy, telecommunication, and water departments. CIIP ensures that those systems and networks are protected and resilient against information security risks, network security risks, Internet security risks, as well as Cybersecurity risks.

Figure 1 summarizes the relationship between Cybersecurity and other security domains. The relationship between these security domains and Cybersecurity is complex. Some of the critical infrastructure services, for example water and transportation, need not impact the state of Cybersecurity directly or significantly. However, the lack of Cybersecurity can have a negative impact on the availability of critical information infrastructure systems provided by the critical infrastructure providers.

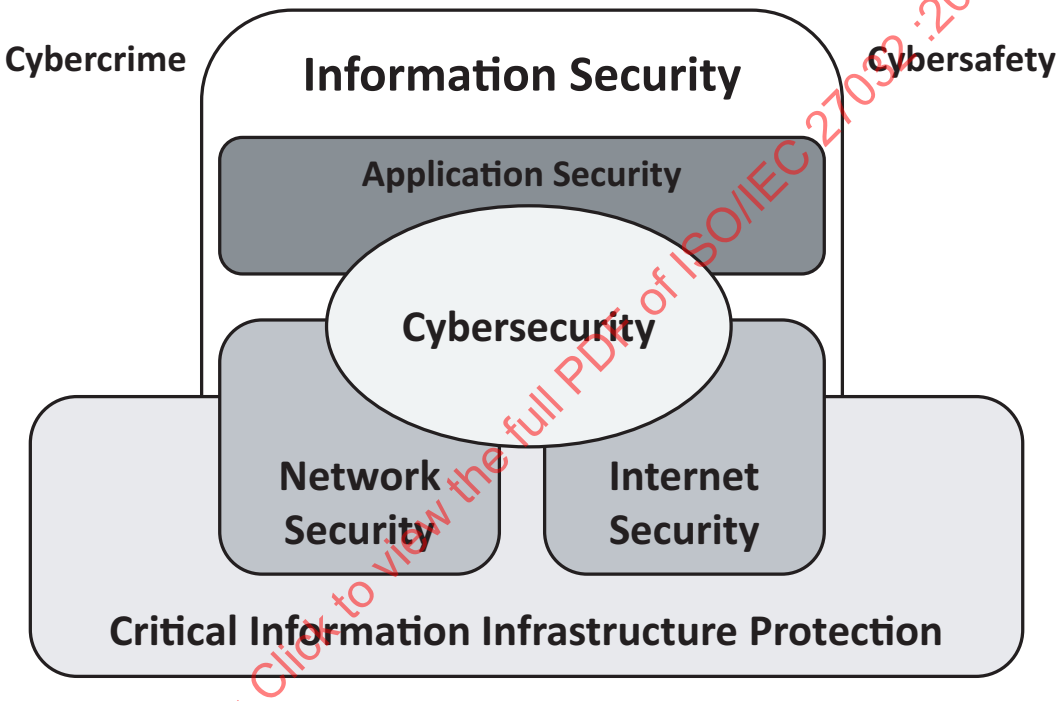

Figure 1 — Relationship between Cybersecurity and other security domains

On the other hand, the availability and reliability of the Cyberspace in many ways rely on the availability and reliability of related critical infrastructure services, such as the telecommunications network infrastructure. The security of the Cyberspace is also closely related to the security of the Internet, enterprise/home networks and information security in general. It should be noted that the security domains identified in this section have their own objectives and scope of focus. To deal with Cybersecurity issues, therefore requires substantial communications and coordination between different private and public entities from different countries and organizations. Critical infrastructure services are regarded by some governments as national security related services, and therefore may not be discussed or disclosed openly. Furthermore, knowledge of critical infrastructure weaknesses, if not used appropriately, can have a direct implication on national security. A basic framework for information sharing and issue or incident coordination is therefore necessary to bridge the gaps and provide adequate assurance to the stakeholders in the Cyberspace.

6.4 General model

6.4.1 Introduction

This clause presents a general model used throughout this International Standard. This clause assumes some knowledge of security and does not propose to act as a tutorial in this area.

This International Standard discusses security using a set of security concepts and terminology. An understanding of these concepts and the terminology is a prerequisite to the effective use of this International Standard. However, the concepts themselves are quite general and are not intended to restrict the class of IT security problems to which this International Standard is applicable.

6.4.2 General security context

Security is concerned with the protection of assets from threats, where threats are categorised as the potential for abuse of protected assets. All categories of threats should be considered; but in the domain of security greater attention is given to those threats that are related to malicious or other human activities. Figure 2 illustrates these high level concepts and relationships.

NOTE Figure 2 is adapted from ISO/IEC 15408-1:2005, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*.

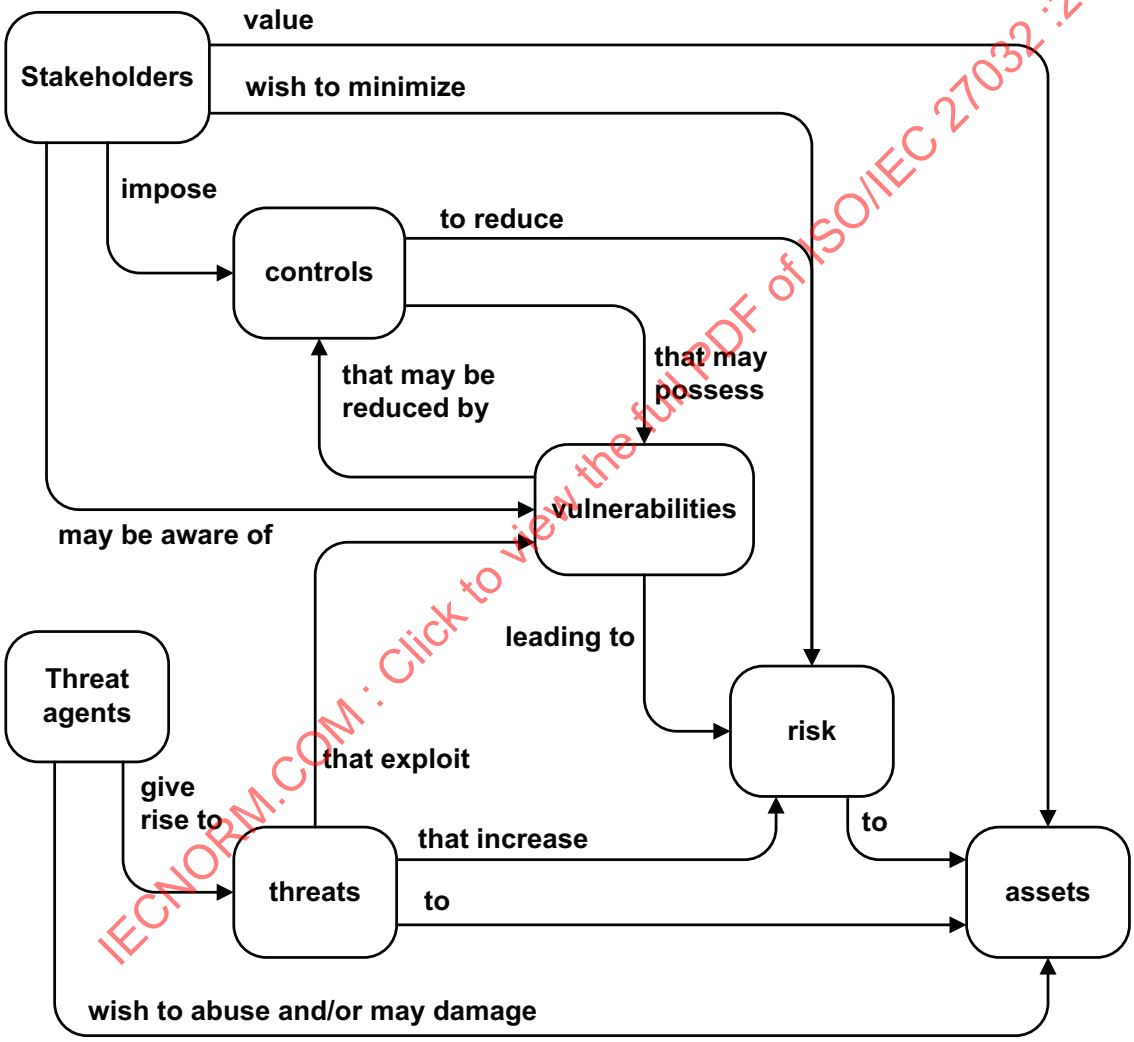

Figure 2 — Security concepts and relationships

Safeguarding assets of interest is the responsibility of stakeholders who place value on those assets. Actual or presumed threat agents may also place value on the assets and seek to abuse assets in a manner contrary to the interests of the applicable stakeholders. Stakeholders will perceive such threats as potential for impairment of the assets such that the value of the assets to the stakeholders would be reduced. Security specific impairment commonly includes, but is not limited to, damaging disclosure of the asset to unauthorised recipients (loss of confidentiality), damage to the asset through unauthorised modification (loss of integrity), or unauthorised deprivation of access to the asset (loss of availability).

Stakeholders assess risks taking into account threats that apply to their assets. This analysis can aid in the selection of controls to counter the risks and reduce it to an acceptable level.

Controls are imposed to reduce vulnerabilities or impacts, and to meet security requirements of the stakeholders (either directly or indirectly by providing direction to other parties). Residual vulnerabilities may remain after the imposition of controls. Such vulnerabilities may be exploited by threat agents representing a residual level of risk to the assets. Stakeholders will seek to minimise that risk given other constraints.

Stakeholders will need to be confident that the controls are adequate to counter the threats to assets before they will allow exposure of assets to the specified threats. Stakeholders may not themselves possess the capability to judge all aspects of the controls, and may therefore seek evaluation of the controls using external organizations.

6.5 Approach

An effective way to confront Cybersecurity risks involves a combination of multiple strategies, taking into consideration the various stakeholders. These strategies include:

— industry best practices, with collaboration of all stakeholders to identify and address Cybersecurity issues and risks;

— broad consumer and employee education, providing a trusted resource for how to identify and address specific Cybersecurity risks within the organization as well as in the Cyberspace; and

— innovative technology solutions to help protect consumers from known Cybersecurity attacks, to stay current and be prepared against new exploitations.

This guideline focuses on providing industry best practices and broad consumer and employee education to assist stakeholders in the Cyberspace in playing an active role to address the Cybersecurity challenges. It includes guidance for:

— roles;

— policies;

— methods;

— processes; and

— applicable technical controls.

Figure 3 provides an overview of the salient points in the approach taken in this International Standard. This International Standard is not intended to be directly used to provide broad consumer education. Instead, it is intended to be used by providers of services in the Cyberspace, as well as organizations providing Cyberspace related education to consumers, to prepare materials for broad consumer education.

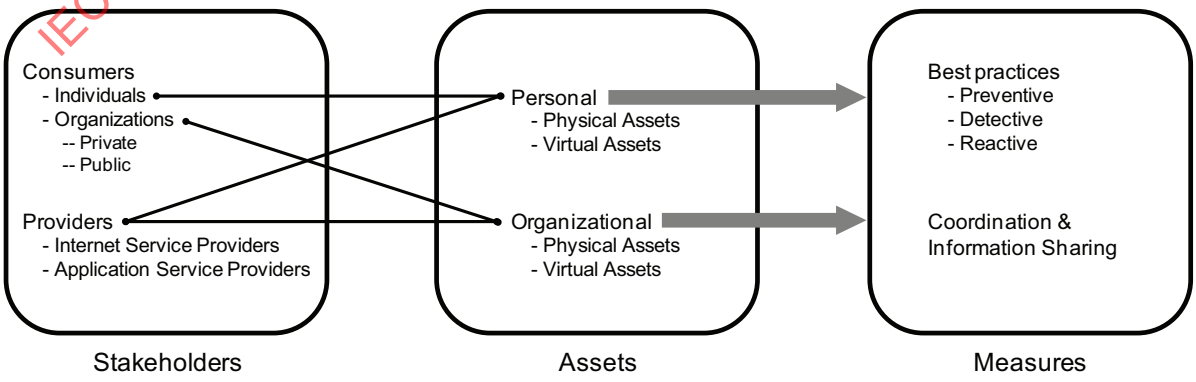

Figure 3 — Overview of the approach

7 Stakeholders in the Cyberspace

7.1 Overview

The Cyberspace belongs to no one; everyone can participate and has a stake in it.

For the purpose of this International Standard, stakeholders in the Cyberspace are categorized in the following groups:

- consumers, including
  - individuals; and
  - both private and public organizations;
- providers, including but not limited to
  - Internet service providers; and
  - Application service providers.

7.2 Consumers

As described in Figure 3, consumers refer to individual users as well as private and public organizations. Private organizations include small and medium enterprises (SMEs), as well as large enterprises. Government and other public agencies are collectively referred to as public organizations. An individual or an organization becomes a consumer when they access the Cyberspace or any services available in the Cyberspace.

A consumer can also be a provider if it in turn provides a service in the Cyberspace or enables another consumer to access the Cyberspace. A consumer of a virtual world service may become a provider by making available virtual products and services to other consumers.

7.3 Providers

Providers refer to providers of services in the Cyberspace, as well as Internet service providers that enable consumers to access the Cyberspace and the various services available in the Cyberspace.

Providers might also be understood as carriers or wholesalers, versus distributors and retailers of access services. This distinction is important from a security and, especially, law enforcement perspective, because, in the event that a distributor or retailer is unable to provide adequate security or lawful access, support services will often default back to the carrier or wholesaler. Understanding the nature of a given service provider is a useful element in Cyberspace risk management.

Application service providers make services available to consumers through their software. These services take many forms and include combinations of the following non-exhaustive list:

- document editing, storage, distribution;
- online virtual environments for entertainment, communications and interaction with other users;
- online digital media repositories with aggregation, indexing, search, store-front, catalogue, shopping cart and payment services; and
- enterprise resource management functions such as human resource, finance and payroll, supply chain management, customer relationship, invoicing.

8 Assets in the Cyberspace

8.1 Overview

An asset is anything that has value to an individual or an organization. There are many types of assets, including but not limited to:

a) information;

b) software, such as a computer program;

c) physical, such as a computer;

d) services;

e) people, their qualifications, skills, and experience; and

f) intangibles, such as reputation and image.

NOTE 1 Often, assets are simplistically seen only as information or resources.

NOTE 2 ISO/IEC 15408-1:2005 defines an asset as information or resources to be protected by controls of a TOE (target of evaluation).

NOTE 3 ISO/IEC 19770-1 has been developed to enable an organization to prove that it is performing Software Asset Management (SAM) to a standard sufficient to satisfy corporate governance requirements and ensure effective support for IT service management overall. ISO/IEC 19770 is intended to align closely to, and to support, ISO/IEC 20000.

NOTE 4 ISO/IEC 20000-1 promotes the adoption of an integrated process approach when establishing, implementing, operating, monitoring, measuring, reviewing and improving a Service Management System (SMS) to design and deliver services which meet business needs and customer requirements.

For the purpose of this International Standard, assets in the Cyberspace are classified into the following classes:

— personal; and

— organizational.

For both classes, an asset can also be further classified as

— a physical asset, whose form exists in the real world, or

— a virtual asset, which only exists in the Cyberspace and cannot be seen or touched in the real world.

8.2 Personal assets

One of the key virtual assets is an individual consumer's online identity and his online credit information. Online identity is considered an asset, since it is the key identifier for any individual consumer in the Cyberspace.

Other individual consumer virtual assets include references in virtual worlds. In virtual worlds, members often use virtual avatars to represent or identify themselves, or to act on their behalf. Often a virtual currency is used for virtual transactions. These avatars and currencies can be considered as assets belonging to an individual consumer.

EXAMPLE Some banks operate in virtual worlds and recognize the virtual world's money as an official currency.

IT hardware and software, as well as personal digital devices or endpoints that allow a consumer to connect to and communicate in the Cyberspace, are also considered as assets in the context of this International Standard.

8.3 Organizational assets

A key aspect of the Cyberspace is the infrastructure that makes it all possible. This infrastructure is a meshed interconnection of networks, servers and applications which belongs to many service providers. However, the reliability and availability of this infrastructure is crucial in ensuring that the Cyberspace services and applications

are available to anyone in the Cyberspace. While any infrastructure that allow any consumer to connect to the Cyberspace, or allow any consumer to access services in the Cyberspace, is considered a physical asset that must be addressed in this International Standard, there may be overlaps with security measures that are proposed in, for example, CIIP, Internet security and network security. However, this International Standard shall focus on ensuring that security issues that may affect these organizational assets are appropriately addressed without overly emphasizing other issues that are not within the scope of this International Standard.

Besides physical assets, virtual organizational assets are increasingly becoming more valuable. The online brand and other representations of the organization in the Cyberspace uniquely identify the organization in the Cyberspace and are as important as the brick and mortar of that organization.

EXAMPLE 1 An organization's URL and website information are assets.

EXAMPLE 2 Countries have even set up embassies in a major virtual world to protect the representation of the country.

Other organizational assets which are exposed through vulnerabilities in the Cyberspace include intellectual property (formulas, proprietary processes, patents, research results) and business plans and strategies (product launch and marketing tactics, competitive information, financial information and reporting data).

9 Threats against the security of the Cyberspace

9.1 Threats

9.1.1 Overview

The threats that exist in the Cyberspace are discussed in relation to assets in the Cyberspace.

Threats to the Cyberspace can be divided into two key areas:

— threats to personal assets:

— threats to organizational assets;

9.1.2 Threats to personal assets

Threats to personal assets revolve mainly around identity issues, posed by the leakage or theft of personal information.

EXAMPLE 1 Credit information can be sold on the black market, which can facilitate online identity theft.

If a person's online identity is stolen or masqueraded, that person can be deprived of access to key services and applications. In more serious scenarios, the consequences can range from financial to national level incidents.

Unauthorized access to a person's financial information also opens up the possibility of theft of the person's money and fraud.

Another threat is the possibility of the endpoint being made a zombie or bot. Personal computing devices can become compromised and so become part of a larger botnet.

Besides the above, other virtual assets that are being targeted are personal assets in virtual worlds and online games. Assets in a virtual world or the world of online games are subject to attack and exploitation as well.

EXAMPLE 2 Avatar details and virtual currency which can, in some cases, be traced and converted back to the real world, would be the prime targets.

Virtual theft and virtual mugging are some of the newly coined terms for this type of attack. Security, in this case, will depend on how much of the real world information is accessible, as well as the security framework of the virtual world itself as defined and implemented by its administrator.

As rules and regulations for the protection of real physical assets, in connection with the Cyberspace, are still being written, those pertaining to virtual assets are almost non-existent. Extra care and caution must be undertaken by prospecting participants to ensure proper protection of its virtual assets.

9.1.3 Threats to organizational assets

Organizations' online presence and online business are often targeted by miscreants whose intent is more than plain mischief.

EXAMPLE 1 Organized Cybercrime syndicates often threaten organizations that their websites will be brought down, or that they will be caused embarrassment through actions such as website defacement.

EXAMPLE 2 If an organization's URL is registered or stolen by cyber-squatters and sold to organizations not related to the real world organization, the online trust accorded to the victimised organization can be misplaced.

In the event of a successful attack, personal information from employees, clients, partners or suppliers could be disclosed and result in sanctions, against the organizations, if it was found to have been managed or protected insufficiently, contributing to the loss.

Financial filing regulations could also be breached if organizational results are disclosed in an unauthorized manner.

Governments hold information on national security, strategic, military, intelligence issues among many other elements relating to the government and state, but also a vast array of information on individuals, organizations and society as a whole.

Governments must protect its infrastructure and information from undue access and exploitation. With a growing and expanding trend of offering e-government services through the Cyberspace, this is a new channel, among others, to launch attacks and access the above information which, if successful, may result in serious risks to a nation, its government and its society.

On a larger scale, the infrastructure that supports the Internet, and thus the Cyberspace, can be targeted as well. While this will not affect the functioning of the Cyberspace permanently, it will affect the reliability and availability of the infrastructure, which contributes to the security of the Cyberspace.

On a national or international level, the Cyberspace is a grey area in which terrorism thrives. One of the reasons is the ease of communication provided by the Cyberspace. Due to the nature of the Cyberspace, specifically the challenges in defining boundaries and borders, it is difficult to regulate and control the way that it can be used.

Terrorist groups can either legitimately buy the applications, services and resources that facilitate their cause, or they can resort to illegal means of securing these resources to avoid detection and tracking. This can include acquiring massive computing resources through botnets.

9.2 Threat agents

A threat agent is an individual or group of individuals who have any role in the execution or support of an attack.

Thorough understanding of their motives (religious, political, economic, etc.), capabilities (knowledge, funding, size, etc.) and intentions (fun, crime, espionage, etc.) is critical in the assessment of vulnerabilities and risks, as well as in the development and deployment of controls.

9.3 Vulnerabilities

A vulnerability is a weakness of an asset or control that can be exploited by a threat. Within the context of an information system, ISO/IEC TR 19791:2006 also defines vulnerability as a flaw, weakness or property of the design or implementation of an information system (including its security controls) or its environment that could be intentionally or unintentionally exploited to adversely affect an organization's assets or operations.

Vulnerability assessment must be an on-going task. As systems receive patches, updates or new elements are added, new vulnerabilities may be introduced. Stakeholders require a thorough knowledge and understanding of the asset or control in question, as well as the threats, threat agents and risks involved, in order to perform a comprehensive assessment.

NOTE ISO/IEC 27005 provides guidelines on identifying vulnerabilities.

An inventory of known vulnerabilities should be kept with the strictest access protocol and preferably separate, physically and logically, from the asset or control it is applicable to. Should a breach of access occur and the vulnerability inventory be compromised, the vulnerability inventory would be one of the most effective tools in the arsenal of a threat agent to use to perpetrate an attack.

Solutions to vulnerabilities must be sought, implemented and, when a solution is not possible or feasible, controls must be put in place. This approach should be applied on a priority basis so the vulnerabilities posing a higher risk are addressed first. Vulnerability disclosure procedures could be defined under the framework of information sharing and coordination in clause 13 of this International Standard.

NOTE A future International Standard, ISO/IEC 29147, will provide guidance on vulnerability disclosure.

9.4 Attack mechanisms

9.4.1 Introduction

Many of the attacks in the Cyberspace are carried out using malicious software, such as spyware, worms and viruses. Information is often gathered through phishing techniques. An attack can occur as a singular attack vector or carried out as a blended attack mechanism. These attacks can be propagated via, for example, suspicious websites, unverified downloads, spam emails, remote exploitation, and infected removable media.

The attacks can come from two major categories:

— Attacks from inside the private network; and

— Attacks from outside the private network.

There are cases though that attacks are a combination of both inside and outside of a private network. Other mechanisms growing in use and sophistication, for carrying out attacks, are those based on social networking websites and the use of corrupted files on legitimate websites.

Individuals tend to implicitly trust messages and content received from contacts previously accepted in their profiles on their social networking websites. Once an attacker, through identity theft, can disguise him/herself as a legitimate contact, the attacker can engage others, and a new avenue is open for launching the various types of attacks previously discussed.

Legitimate websites can also be hacked into and have some of its files corrupted and used as a means for perpetrating attacks. Individuals tend to implicitly trust commonly visited websites, often bookmarked in their Internet browsers for a long time, and even more those which use security mechanisms such as SSL (Secure Sockets Layer). While party authentication and integrity of the information being transmitted or received are still in place, SSL does not differentiate between the original content and the new corrupted content, planted by an attacker, thus exposing users of that website to attacks.

Despite the perceived legitimate source, such as in instances like the above, individuals must still take the precautions outlined in clause 11 to better protect themselves.

9.4.2 Attacks from inside the private network

These attacks are normally launched inside an organization's private network, typically the local area network, and can be initiated by employees or someone who gets access to a computer or network within an organization or individual's premises.

EXAMPLE 1 One possible case is that system administrators might take advantage of the system access privileges that they hold, such as access to users' password information, and use that to initiate an attack. On the other hand, system administrators themselves can become the initial target of an attack, as a means for the attacker to obtain additional information (usernames, passwords, etc.), before proceeding to their originally intended target or targets.

The attacker can use mechanisms such as packet sniffer software to obtain passwords or other identity information. Alternatively, the attacker can masquerade as an authorized entity and act as man-in-the-middle to steal identity information.

EXAMPLE 2 One example is the use of rogue Access Points (AP) to steal identities. In this case, the attacker might sit in an airport, coffee shop or other public places that offer free Wi-Fi access to the Internet. In some cases, the attacker may even masquerade as the legitimate owner of the wireless access point on the premise by using the Service Set IDentifier (SSID) of the premise. If a user accesses this rogue AP, the attacker can act as man-in-the-middle and obtain valuable password and or identity information from the user, for example, bank account information and password, email account password, etc.

EXAMPLE 3 Often, it is sufficient to be only near to a non-protected Wi-Fi network, such as sitting in a car outside a house, to be able to steal information on the network.

Besides the attacks launched by human attackers, malware infected computers also launch various attacks to surrounding computers inside the private network.

EXAMPLE 4 Many malwares often send scanning packets to the private network to find surrounding computers, and then try to exploit discovered computers.

EXAMPLE 5 Some malware uses the promiscuous mode of a network interface of its infected computer in order to eavesdrop on traffic flowing through the private network.

EXAMPLE 6 Key loggers are hardware or software applications that capture all key presses on the target system. This can be done in secret to monitor a user's actions. Key loggers are often utilized to capture authentication information from application login pages.

9.4.3 Attacks from Outside the Private Network (e.g. Internet)

There are many different attacks that can be launched from outside the private network, including the Internet.

While the initial attack will always target a publicly facing system (e.g. router, server, firewall, website, etc.), attackers may also be seeking to exploit assets residing inside the private network.

Old attack methods are improved and new ones are developed on an on-going basis. Attackers are increasingly sophisticated and normally combine different attack techniques and mechanisms to maximize their success, which makes attack detection and prevention even more difficult.

Port scanners are one of the oldest, and still very effective, tools used by attackers. They scan all ports available on a server to confirm which ports are "open". This normally is one of the first steps executed by a prospective attacker on the target system.

These attacks can manifest into various DoS attacks to either the application servers or other networking equipment by exploiting protocol or application design vulnerabilities.

EXAMPLE With the help of a botnet, large scale DoS attacks can be launched that can bring down a country's access to the Cyberspace.

With the proliferation of peer-to-peer applications, commonly used to share files such as digital music, video, photos, etc., attackers are becoming increasingly sophisticated in how to disguise themselves and their malicious code using the exchanged files as a trojan horse for their attacks.

Buffer overflows (a.k.a. buffer overruns) are another popular method of compromising servers on the Internet. By exploiting coding vulnerabilities and sending much longer than expected strings of character, attackers cause the server to operate outside its normal (controlled) environment, thus facilitating the insertion/execution of malicious code.

Another technique is IP Spoofing, which consists in the attacker manipulating the IP address associated with his/her messages in an attempt to disguise as a known, trusted source, thus gaining unauthorized access to systems.

10 Roles of stakeholders in Cybersecurity

10.1 Overview

To improve the state of Cybersecurity, stakeholders in the Cyberspace need to play an active role in their respective use and development of the Internet. These roles may at times overlap with their individual and organizational roles within their personal or organization networks. The term organization network refers to the combination of an organization's private networks (typically an intranet), extranets and publicly visible networks. For the purpose of this International Standard, publicly visible networks are those networks exposed to the Internet, for example to host a website. Because of this overlap, these roles can appear to have insignificant or no direct benefit for the individual and organization concerned. They are, however, significant to enhancing Cybersecurity when all involved act accordingly.

10.2 Roles of consumers

10.2.1 Introduction

Consumers can view or collect information, as well as provide certain specific information within a Cyberspace application's space, or open to limited members or groups within the application's space, or the general public. Actions taken by consumers in these roles can be passive or active, and can contribute directly and indirectly to the state of Cybersecurity.

10.2.2 Roles of individuals

Individual consumers of the Cyberspace may assume different roles in different context and applications.

Consumer roles can include, but are not limited to, the following:

— General Cyberspace application user, or general user, such as online game player, instant messenger user, or web surfer;

— Buyer/seller, involved in placing goods and services on online auction and marketplace sites for interested buyers, and vice versa;

— Blogger and other contents contributor (for example, an author of an article on a wiki), in which information in text and multimedia (for example, video clips) are published for general public or limited audience's consumption;

— IAP within an application context (such as an online game), or the Cyberspace in general;

— Member of an organization (such as an employee of a company, or other form of associating with a company);

— Other roles. It is possible that a user can be assigned a role unintentionally or without his or her consent.

EXAMPLE When a user visits a site which requires authorization, and unintentionally gains access, the user may be labelled as an intruder.

In each of these roles, individuals can view or collect information, as well as provide certain specific information within a Cyberspace application's space, or open to limited members or groups within the application's space, or the general public. Actions taken by individuals in these roles can be passive or active, and can contribute directly and indirectly to the state of Cybersecurity.

EXAMPLE 1 If an IAP provides an application that contains security vulnerabilities, these vulnerabilities can be used by Cyber miscreants as a channel to reach users of the application.

EXAMPLE 2 Bloggers or other forms of content contributors can receive a request in the form of innocent questions about their contents. In their reply, they can unintentionally reveal more personal or company information to the public than desired.

EXAMPLE 3 An individual, acting as buyer or seller, can unknowingly participate in criminal transactions of selling stolen goods or money laundry activities.

Consequently, as in the real world, individual consumers need to exercise caution in each and every role they play in the Cyberspace.

10.2.3 Roles of organizations

Organizations often use the Cyberspace to publicise company and related information, as well as market related products and services. Organizations also utilize the Cyberspace as part of their network for delivery and receipt of electronic messages (for example, emails) and other documents (for example, file transfer).

In line with the same principles of being a good corporate citizen, these organizations should extend their corporate responsibilities to the Cyberspace by proactively ensuring that their practices and actions in the Cyberspace do not introduce further security risks into the Cyberspace. Some proactive measures include:

— proper information security management by implementing and operating an effective information security management system (ISMS);

NOTE 1 ISO/IEC 27001 provides requirements for information security management systems.

— proper security monitoring and response;

— incorporating security as part of the Software Development Life-cycle (SDLC) where the level of security built into systems needs to be determined based on the organization's criticality of data;

— regular security education of users in the organization through continuous technology updates and keeping track of latest technology developments; and

— understanding and using proper channels in communicating with vendors and service providers on security issues discovered during usage.

NOTE 2 A future International Standard, ISO/IEC 29147, will provide guidelines on vulnerability disclosure.

NOTE 3 ISO/IEC 27031 provides guidelines for ICT readiness for business continuity.

NOTE 4 ISO/IEC 27035 provides guidelines for information security incident management.

NOTE 5 ISO/IEC 27034-1 provides guidelines for application security.

The government, primarily law enforcement agencies and regulators, may have the following important roles to play:

— advise organizations of their roles and responsibilities in the Cyberspace;

— share information with other stakeholders on the latest trends and developments in technology;

— share information with other stakeholders on the current prevalent security risks;

— be a conduit for receiving any information, whether close or open, with regard to security risks to the Cyberspace; and

— be the primary coordinator for information dissemination and orchestrating any required resources, both at national level or corporate level, in times of crisis arising from a massive cyber-attack.

10.3 Roles of providers

Service providing organizations can include two categories:

— providers of access to employees and partners to the Cyberspace, and

— providers of services to consumers of the Cyberspace, either to a closed community (for example, registered users), or the general public, through the delivery of Cyberspace applications

EXAMPLE Examples of services are online trading marketplaces; discussion forum platform services; blogging platform services; and social networking services.

Service providers are also consumer organizations. They are thus are expected to observe the same roles and responsibilities as consumer organizations. As service providers, they have additional responsibilities in maintaining or even enhancing security of the Cyberspace by:

— providing safe and secure products and services;

— providing safety and security guidance for end-users; and

— providing security inputs to other providers and to consumers about trends and observations of traffic in their networks and services.

11 Guidelines for stakeholders

11.1 Overview

The guidance in this clause focuses on three main areas:

— security guidance for consumers;

— internal information security risk management of an organization; and

— security requirements that providers should specify for consumers to implement.

The recommendations are structured as follows:

a) an introduction to risk assessment and treatment;

b) guidelines for consumers; and

c) guidelines for organizations, including service providers:

   — management of information security risk in the business; and

   — security requirements for hosting services and other application services.

11.2 Risk assessment and treatment

ISO 31000, *Risk management – Principles and guidelines*, provides principles and generic guidelines on risk management while ISO/IEC 27005, *Information technology – Security techniques – Information security risk management*, provides guidelines and processes for information security risk management in an organization, supporting in particular the requirements of an ISMS according to ISO/IEC 27001. These guidelines and processes are considered sufficient for addressing risk management in the context of the Cyberspace.

ISO/IEC 27005:2011 does not provide any specific methodology for information security risk management. It is up to the consumers and providers to define their approach to risk management. A number of existing methodologies can be used under the framework described in ISO/IEC 27005 to implement the requirements of an ISMS.

The following aspects have to be taken into account when defining an approach to risk management:

— Identification of critical assets: Connecting to or utilizing the Cyberspace broadens the scope of defining assets. As it is not cost-effective to protect all assets, it is essential that the critical assets be identified so that particular care may be taken to protect them. The designation should be made from the business context, through consideration of the impact of the loss or degradation of an asset on the business as a whole.

— Identification of risks: Stakeholders should properly consider and address the additional risks, threats and attacks that become relevant when participating in the Cyberspace.

— Responsibility: By participating in the Cyberspace, a stakeholder should accept the added responsibility towards other stakeholders. This includes:

   — Acknowledgement: Recognizing the possible risk that the stakeholder's participation may introduce in the Cyberspace in general and specifically in other stakeholders' information systems.

- Reporting: It may be necessary to include stakeholders outside the organization when distributing reports related to risks, incidents and threats.
- Information sharing: As with reporting, it may be necessary to share relevant information with other stakeholders.
- Risk assessment: It is necessary to determine the extent to which a stakeholder's actions and presence in the Cyberspace becomes, or contributes to, a risk for another stakeholder.
- Regulatory/Legislative: By connecting to the Cyberspace, the legal and regulatory boundaries become difficult to distinguish, and more, sometimes contradictory, requirements are applicable.

— System or service retirement: Once a system or service is no longer needed, it should be retired in a way that ensures that related services or interfaces are not impacted. All security-related information must be invalidated to ensure that the systems to which it interfaced or are related to are not compromised.

— Consistency: The approach to risk management applies across the entire Cyberspace. Within this approach or methodology, Cyberspace consumers and providers are assigned responsibilities for specific activities, such as contingency planning, disaster recovery, and the development and implementation of protective programs for the systems under their control and/or ownership.

In general, the risk management methodology in ISO/IEC27005 covers the full life-cycle of a generic system, thus making it usable for new security systems as well as for legacy systems. Since it deals with the treatment of systems, it is applicable to all business models. The processes within the framework may treat the service providers' networks and services as an integrated system, consisting of subsystems that provide public services and private subsystems that support internal services, or it may treat each of the individual services (e.g., web hosting) separately, and describe their provision in terms of separate interacting systems. It may be advantageous, for simplicity, to consider everything that is needed to support the provider's services as a large system that can be decomposed into smaller systems, each of which provides a marketable service or forms part of the infrastructure.

Important aspects to remember when considering the goals and objectives of Cybersecurity are:

a) protect the overall security of the Cyberspace;

b) plan for emergencies and crises through participation in exercise, and update response plans and plans for continuity of operations;

c) educate stakeholders on Cybersecurity and risk management practices;

d) ensure timely, relevant and accurate threat information sharing between law enforcement and intelligence communities and key decision makers relevant to the Cyberspace; and

e) establish effective cross-sector and cross-stakeholder coordination mechanisms to address critical interdependencies, including incident situational awareness and cross-sector and cross-stakeholder incident management.

Goals and objectives a) to c) flow down directly to the service providers, who are responsible for the equipment and services under their control. For goals and objectives d) and e), the service providers are involved as active participants in the information sharing and coordination activities.

Specific service provider goals, such as what services to supply, flow down from the business context.

11.3 Guidelines for consumers

This International Standard is not directed at individuals of the Cyberspace specifically, but focuses on organizations providing services to consumers, and organizations that require their employees or end-users to practice secure use of the Cyberspace to manage the Cybersecurity risk effectively. The guidance on the roles and security of users in the Cyberspace and how they could positively influence the state of Cybersecurity aims to serve as a guide for the design and development contents by these organizations, in the context of their service provisioning and awareness and training programs for delivery to their end-users.

As explained in clause 10.2, consumers can view or collect information, as well as provide certain specific information within a Cyberspace application's space, or open to limited members or groups within the application's space, or the general public. Actions taken by consumers in these roles can be passive or active, and can contribute directly and indirectly to the state of Cybersecurity.

For example, as an IAP, if the application provided contains security vulnerabilities, they could result in exploitation by cyber-miscreants leveraging them as a channel to reach innocent users of the application. As bloggers or other forms of contents contributors, they can receive a request in the form of innocent questions on their contents in which they can unintentionally reveal more personal or company information to the public than desired. As a buyer or seller, a consumer can unknowingly participate in criminal transactions of selling stolen goods or money laundering activities. Consequently, as in the physical world, consumers need to exercise caution in each and every role they play in the Cyberspace.

In general, consumers should take note of the following guidance:

a) Learn and understand the security and privacy policy of the site and application concerned, as published by the site provider.

b) Learn and understand the security and privacy risks involved and determine appropriate controls applicable. Participate in related online discussion forums or ask someone who knows about the site or application before providing personal or organization information, or participating and contributing information to the discussion.

c) Establish and practice a personal privacy policy for identity protection by determining the categories of personal information available and sharing principles relating to that information.

d) Manage online identity. Use different identifiers for different web applications, and minimize the sharing of personal information to each website or application requesting such information. Register one's online identity on popular social networking sites even if the account is left dormant.

EXAMPLE Single sign on is a form of online identity management.

e) Report suspicious events or encounters to the relevant authorities (see Annex B for as an example of a publicly available list of contacts).

f) As a buyer or seller, read and understand the online marketplace's site security and privacy policy, and take steps to verify the authenticity of the interested parties involved. Do not share personal data, including banking information, unless a genuine interest to sell or buy has been established. Use a trustworthy payment mechanism.

g) As an IAP, practice secure software development and provide a hash value of the code online so that receiving parties can verify the value if necessary to ensure integrity of the code. Provide documentation of the code security and privacy policies and practices and respect the privacy of code users.

h) As a blogger or other content contributor (including website maintainers), ensure that applicable stakeholder privacy and sensitive information are not disclosed through the blogs or online publications. Review comments and postings received on the site and ensure that they do not contain any malicious content such as links to phishing websites or malicious downloads.

i) As a member of an organization, an individual consumer should learn and understand the organization's corporate information security policy and ensure that classified and/or sensitive information are not released intentionally or by accident on any websites in the Cyberspace, unless prior authorization for such disclosure has been formally granted.

j) Other roles. When a consumer visits a site which requires authorization, and unintentionally gains access, the user may be labelled as an intruder. Exit the site immediately and report to the relevant authority, since the fact that it was possible to gain access can be an indication of a compromise.

11.4 Guidelines for organizations and service providers

11.4.1 Overview

Controls for managing Cybersecurity risks depend significantly on the maturity of the security management processes within organizations (including service providers). While the guidelines suggested here are mainly discretionary for organizations, it is recommended that service providers treat the guidelines as baseline mandatory measures.

The guidelines in this clause can be summarized as:

— Manage information security risk in the business.

— Address security requirements for hosting web and other cyber-application services.

— Provide security guidance to consumers.

11.4.2 Manage information security risk in the business

11.4.2.1 Information security management system

At the enterprise level, organizations connecting to the Cyberspace should implement an information security management system (ISMS) to identify and manage related information security risk to the business. The ISO/IEC 27000 series of International Standards for information security management systems provides the required guidance and best practices for implementing such a system.

A key consideration in implementing an ISMS is to ensure that the organization has a system to continuously identify, assess, treat, and manage information security risk relating to its business, including the provision of services on the Internet, directly to end-users or subscribers, should it be a service provider.

NOTE 1 ISO/IEC 27005, Information technology – Security techniques – Information security risk management, provides guidelines for information security risk management in an organization, supporting in particular the requirements of an ISMS according to ISO/IEC 27001.

NOTE 2 ISO 31000, Risk management – Principles and guidelines, provides principles and generic guidelines on risk management.

Organizations may also consider a formal certification of its compliance with ISMS requirements, such as ISO/IEC 27001.

As part of the implementation of an ISMS, an organization should also establish a security incident monitoring and response capability and coordinate their incident response activities with external CIRT, CERT, or CSIRT organizations in the country. The incident and emergency response provision should include monitoring and assessing the security status of th use of the organization's services by end-users and customers, and provide guidance to assist the affected parties in responding to security incidents effectively.

NOTE ISO/IEC 27035, Information technology – Security techniques – Information security incident management, provides guidance on information security incident management.

11.4.2.2 Provide secure products

Some organizations develop[1)] and release their own web browser toolbars, diallers, or code to provide value-added services to end-users, or facilitate ease of access to the organization's services or applications. In such instances, there should be a proper end-user agreement in a suitable language, incorporating statements about the organization's coding policy, privacy policy, and means whereby users can change their acceptance later or escalate any issues they might have regarding the policy and practices. When such an agreement is used, it should be placed under version control and the organization should make sure that end-users sign it consistently.

1) Either internally or through a third party provider.

Where there is a high degree of reliance on the security of software products, these should be independently validated under the Common Criteria scheme, as described at ISO/IEC 15408.

Organizations should document code behaviour and make an assessment as to whether the behaviour can fall in potential areas that might be considered as spyware or deceptive software. In the latter case, it should engage a suitably qualified assessor to evaluate whether the code fall within anti-spyware vendors objective criteria that adheres to best practices so that the organization-provided software tools for the end-users, would not be labelled as spyware or adware by anti-spyware vendors. Many anti-spyware vendors publish the criteria by which they rate software.

Organizations should implement digital code signing for their binaries so that anti-malware and anti-spyware vendors could easily determine the owner of a file, and ISVs, who consistently produce software that follows best practices, would be categorized as being likely secure even prior to analysis.

Should an organization discover useful software techniques that could help to reduce the spyware or malware problem, the organization should consider partnering and working with the vendor to make them broadly available.

In order to fulfill these requirements, security education of developers is very important. A secure software development life cycle should be used where software vulnerabilities can be minimized hence providing a more secure software product.

NOTE ISO/IEC 27034, Information technology – Security techniques – Application security, provides guidelines to define, develop, implement, manage, support and retire an application.

11.4.2.3 Network monitoring and response

Network monitoring is commonly used by organizations to ensure reliability and quality of their network services. At the same time, this capability can be leveraged to look for exceptional network traffic conditions and detect malicious activities emerging on the network. In general, organizations should perform the following:

— Understand the traffic on the network – what is normal, what is not normal.

— Use a network management tool to identify spikes in traffic, “unusual” traffic/ports and ensure that there are tools available to pinpoint and respond to the cause.

— Test the response capability before they are needed for an actual event. Refine the response techniques, processes and tools based on the result of regular drills.

— Understand the constituents on an individual basis – if someone who is normally an inactive user suddenly starts capping out at 100 percent of available bandwidth, it may be necessary to isolate the contravening user until the reason can be found. Network isolation can prevent the spread of malware though some implementations can require user consent or updates to a Terms of Service.

— Consider monitoring of activity from intelligence points in the network such as DNS and messaging filters, which can also serve to flag devices that have been compromised with malware but, for a variety of reasons, are not detected by anti-virus or IDS services.

EXAMPLE Due to the volume of information on the network, tools such as IDS and IPS can be used to monitor for reportable exceptions.

11.4.2.4 Support and escalation

Businesses, including service providers and government organizations normally have a support service to answer customers queries and provide technical assistance and support to address end-users’ problems. With the increasing proliferating of malware on the Internet, a service providing organization can receive reports relating to malware and spyware infections and other Cybersecurity issues. Such information are important and useful for relevant vendors to assess the risk and malware situation, and provide updates to necessary tools to ensure that any new malware or spyware detected can be removed or disabled effectively. In this regard, an organization should establish contact with security vendors and submit relevant reports and malware samples to the vendors for follow-up – particularly if there appears to be a spike in prevalence. Most vendors maintain an email list for receiving such reports or samples for analysis and follow-up. For example, see Table B.1 in Annex B.

11.4.2.5 Keeping up-to-date with latest developments

As part of the ISMS implementation to manage the enterprise information security risk, and also ensure that organizations continue to follow-up industry best practices and keep tap with the latest vulnerabilities and exploits/attacks situation, organizations should participate in relevant community or industry forums to share their best practices and learn from other fellow providers.

11.4.3 Security requirements for hosting web and other cyber-application services

Most service providers provide hosting services on their network and data centre as part of their business services. These services, which include websites and other online applications, are often re-packaged and re-sold by hosting subscribers to other consumers, such as small businesses and end-users. Should the hosting subscribers set up an insecure server, or host malicious contents in their sites or applications, the security of the consumers will be adversely affected. As such, it is important that services, at a minimum, meet best practices standards by complying with policy or terms of agreements.

Where multiple providers are used, the interaction between the providers should be analysed and the respective service agreements should address any critical interaction. For example, updates or patches to one provider's systems should be coordinated with other providers, should the update result in a negative interaction.

The terms of agreements should at least cover the following:

a) Clear Notices, describing the online site or application security and privacy practices, data collection practices, and the behaviour of any code (for example, Browser Helper Object) that the online site or application can distribute and execute in end-user desktops or web browser environments.

b) User Consent, facilitating user's agreement or disagreement with the terms of services described in the Notices. This would allow a user to exercise discretion and determine whether he/she can accept the terms of services accordingly.

c) User Controls, facilitating users to change their settings or otherwise terminate their acceptance anytime in the future after the initial agreement.

The terms are important to ensure that the end-users are clear about the behaviour and practices of the online site or application, in relation to the end-users' privacy and security. The terms should be developed with the aid of a legal professional to ensure that they will also indemnify the service provider from potential legal action from the end-users, as a result of specific losses or harm incurred due to malicious contents or unclear policies and practices on the website.

In addition to the data protection and personal privacy provisions on the online site or application, service providers should require online sites or applications hosted on their networks to implement a set of best practices security controls at the application level before they could go live. These should include but are not limited to examples given in clause 12.2.

As part of a service provider's hosting infrastructure, servers should be protected against unauthorized access and the ability to host malicious content. See clause 12.3 for examples of controls.

To permit the enforcement of these security controls, in particular, those relating to the online site and application security, service providers should consider incorporating these provisions in the terms of services agreements.

11.4.4 Security guidance for consumers

Service providers should provide guidance to consumers on how to stay secure online. Service providers may either create the guidance directly, or refer the users to available guidance sites that could provide the contents. It is critical to educate end-users on how they can contribute to a secure Internet in relation to the multiple roles that they can play in the Cyberspace, as described in clause 7. In addition, end-users should be advised to take necessary technical security controls in which service providers could also play an active role, as described in clause 11.3. Examples of guidance activities may include:

a) Periodic (for example, monthly) security newsletters to advise on specific security techniques (for example, how to choose a good password); updates on security trends; and to provide notices of security

webcasts, other on-demand videos, audio broadcasts, and security information that are available from the organization's web portal or other security content providers.

b) Direct broadcasts of on-demand security education videos or webcasts covering a variety of security topics to improve end-users' security practices and awareness.

c) Incorporating a security column in the service provider's hard-copy newsletter that are sent to end-users' resident or office addresses to highlight key security events or contents.

d) Annual or other periodic end-user security seminars or road shows, possibly in partnership with other industry players, vendors, and governments.

Service providers using email as the primary way of communicating with end-users should do so in a way that helps end-users resist social engineering attacks. In particular, end-users should be consistently reminded that unsolicited emails from the service provider will never ask for

— personal information;

— user names;

— passwords; and

— will never include security related links for the reader to click on.

When a service provider wishes a user to go to its site for information they should tell the user how to safely connect to the required URL. For example, they might ask a user to type a quoted URL into their browser and make sure that the quoted URL does not contain a clickable link.

As part of the user security education and guidance against deceptive software and spyware, organizations and service providers should advise their end-users on the use of suitable technical security controls to protect their systems against known exploits and attacks. As a general guide, consumers should be encouraged to implement the controls in clause 12.4.

Annex B provides an example list of references and online resources that could be used to support the implementation of the above recommendations.

12 Cybersecurity controls

12.1 Overview

Once the risks to Cybersecurity are identified and appropriate guidelines are drafted, Cybersecurity controls that support the security requirements can be selected and implemented. This clause gives an overview of the key Cybersecurity controls that can be implemented to support the guidelines laid out in this International Standard.

12.2 Application level controls

Application level controls include the following:

a) Display of short notices, which provide clear, concise one-page summaries (using simple language) of the company's essential online policies. With this, users are able to make more informed choices about sharing their information online. The short notices should conform to all regulatory requirements and provide links to full legal statements and other relevant information, so customers who want more detail can easily click through to read the longer version. With a single notice, customers can have a more consistent experience across all of the company's properties, with the same privacy standards and expectations extended to many sites.

b) Secure handling of sessions for web applications; this can include online mechanisms such as cookies.

c) Secure input validation and handling to prevent common attacks such as SQL-Injection. Based on the fact that websites, which are generally considered as trustworthy, are increasingly used for malicious code distribution, input and output validation have to be carried out by active content as well as by dynamic content.

d) Secure web page scripting to prevent common attacks such as Cross-site Scripting.

e) Code security review and testing by appropriately skilled entities.

f) The organization's service, whether provided by the organization or by a party representing the organization, should be provided in a fashion that the consumer can authenticate the service. This may include having the provider use a sub-domain from the organization's branded domain name and possibly the use of HTTPS credentials registered to the organization. The service should avoid the use of deceptive methods where the consumer may have difficulty determining with whom they are dealing.

12.3 Server protection

The following controls can be used to protect servers against unauthorized access and the hosting of malicious content on servers:

a) Configure servers, including underlying operating systems in accordance to a baseline security configuration guide. This guide should include proper definition of server users versus administrators, enforcement of access controls on program and system directories and files, and enabling of audit trails, in particular, for security and other failure events on the system. Furthermore it is recommended to install a minimal system on a server in order to reduce the attack vector.

b) Implement a system to test and deploy security updates, and ensure the server operating system and applications are kept up-to-date promptly when new security updates are available.

c) Monitor the security performance of the server through regular reviews of the audit trails.

d) Review the security configuration.

e) Run anti-malicious software controls (such as anti-virus and anti-spyware) on the server.

f) Scan all hosted and uploaded content regularly using up to date anti-malicious software controls. Recognize that a file can, for example, still be spyware or malware even if not detected by the current controls due to the constraints of imperfect information.

g) Perform regular vulnerability assessments and security testing for the online sites and applications to ensure that their security is adequately maintained.

h) Regularly scan for compromises.

12.4 End-user controls

The following is an incomplete list of controls that end-users can use to protect their systems against known exploits and attacks:

a) Use of supported operating systems, with the most updated security patches installed. Organizational consumers have a responsibility to be aware of, and follow, organizational policy regarding supported operating systems. Individual consumers should be aware of, and consider using, provider recommended operating systems. In all cases, the operating system should be kept up to date regarding security patches.

b) Use of the latest supported software applications, with the most updated patches installed. Organizational consumers have a responsibility to be aware of, and follow, organizational policy regarding supported application software. Individual consumers should be aware of, and consider using, provider recommended application software. In all cases, the application software should be kept up to date regarding security patches.

c) Use anti-virus and anti-spyware tools. If feasible, a service provider such as an ISP should consider partnering with trusted security vendors to offer end-users these tools as part of the service subscription package so that the security controls are made available upon signing-up the subscription, or upon renewal. Organizational consumers have a responsibility to be aware of, and follow, organizational policy regarding the use of security software tools. Individual consumers should use security software tools. They should look to the provider for any recommended, provided, or discontinued security software. In all cases, the security software should be kept up to date regarding security patches and signature databases.

d) Implement appropriate anti-virus and anti-spyware safeguards. Common web browser and browser toolbars have now incorporated capabilities such as pop-up blockers, which will prevent malicious websites from displaying windows that contain spyware or deceptive software that could exploit system or browser weaknesses, or use social engineering to trick users into downloading and installing them on their systems. Organizations should establish a policy to enable the use of such tools. Service providing organizations should collate a list of recommended tools, and their use should be encouraged to end-users, with guidance on their enablement and permission granting for websites that users would like to allow.

e) Enable script blockers. Enable script blockers or a higher web security setting to ensure that only scripts from trusted sources are executed on a local computer.

f) Use phishing filters. Common web browser and browser toolbars often incorporates this capability, which could determine whether a site that a user is visiting is found within a database of known phishing websites, or contains script patterns that are similar to those found typical phishing websites. The browser would provide alerts, normally in the form of colour-coded highlights, to warn users of the potential risk. Organizations should establish a policy to enable the use of such tool.

g) Use other available web browser security features. From time to time, as new Cybersecurity risk emerges, web browsers and browser toolbar providers add new security capabilities to protect users against risks. End-users should keep abreast of these developments by learning about such updates that are normally provided by the tool providers. Organizations and service providers should similarly review these new capabilities and update related policies and services to better serve the needs of their organizations and customers, and address related Cybersecurity risk.

h) Enable a personal firewall and HIDS. Personal firewalls and HIDS are important tools for controlling network services accessing the user systems. A number of newer operating systems have personal firewalls and HIDS incorporated. While they are enabled by default, users or applications might disable them, resulting in undesirable network security exposures. Organizations should adopt a policy on the use of a personal firewall and HIDS and evaluate suitable tools or products for implementation so that their use is enabled by default for all employees. Service providers should encourage the use of a personal firewall and HIDS functions, and/or suggest other third-party personal firewall and HIDS products that has been evaluated and considered as trusted, and educate and help users in enabling basic network security at the end-user system level.

i) Enable automated updates. While the above technical security controls are capable of dealing with most malicious software at their respective operating levels, they are not very effective against exploitation of vulnerabilities that exist in operating systems and application products. To prevent such exploits, the updating function available in operating systems, as well as those provided by user-trusted applications (for example, trusted third-party evaluated anti-spyware and anti-virus products), should be enabled for automated updates to be performed. This would then ensure that systems are updated with the latest security patches whenever they are available, closing the time gap for exploits to take place.

12.5 Controls against social engineering attacks

12.5.1 Overview

Cybercriminals are increasingly resorting to psychological or social engineering tactics in order to succeed.

EXAMPLE 1 The use of emails carrying URI directing unsuspecting users to phishing websites.

EXAMPLE 2 Scam mails requesting users to provide personal identification information, or information relating to corporate intellectual property.

The proliferation of social networking and community sites provides new vehicles that further enable more believable scams and frauds to be conducted. Increasingly, such attacks are also transcending technology, beyond the PC systems and traditional network connectivity, leveraging mobile phones, wireless networks (including Bluetooth), and voice-over-IP (VoIP).

This clause provides a framework of controls applicable for managing and minimizing the Cybersecurity risk in relation to social engineering attacks. The guidance provided in this clause is based on the notion that the only effective way to mitigate the threat of social engineering is through the combination of:

— security technologies;

— security policies that set ground rules for personal behaviour, both as an individual and as an employee; and

— appropriate education and training.

The framework therefore covers:

— policies;

— methods and processes;

— people and organizations; and

— applicable technical controls.

12.5.2 Policies

In line with common practices for information security risk management, basic policies governing the creation, collection, storage, transmission, sharing, processing and general use of organizational and personal information and intellectual property on the Internet and in the Cyberspace should be determined and documented. In particular, this relates to applications such as instant messaging, blogging, P2P file sharing, and social networking, which are normally beyond the scope of enterprise network and information security.

As part of corporate policies, statements and penalties relating to the misuse of Cyberspace applications should also be incorporated to deter against practices of misuse by employees and third-parties on the corporate network or systems accessing the Cyberspace.

Administrative policies promoting awareness and understanding of Cybersecurity risks, and encouraging, if not mandating, the learning and development of skills against Cybersecurity attacks, in particular, social engineering attacks, should be developed and promulgated. This should include requirements for regular attendance to such briefings and training.

By promoting suitable policies and awareness on social engineering risks, employees can no longer claim ignorance of such risks and requirements, and at the same time develop an understanding of best practices and policies expected of external social networking and other Cyberspace applications, for example, the security policy agreement of the service provider.

12.5.3 Methods and processes

12.5.3.1 Categorization and classification of information

To support policies to promote awareness and protection of corporate classified and personal sensitive information, including intellectual properties, processes for categorization and classification of information should be implemented.

For each category and classification of information involved, specific security controls for protection against accidental exposure, and intended unauthorized access should be developed and documented.

Users in organizations could then differentiate between the different categories and classification of information that they generate, collect, and handle. Users can then exercise the required caution and protective controls when using the Cyberspace.

Procedures on how to handle company intellectual properties, personal data, and other confidential information should also be developed and promulgated.

12.5.3.2 Awareness and training

Security awareness and training, including regular updating of relevant knowledge and learning are an important element for countering social engineering attacks.

As part of an organization's Cybersecurity program, employees and third-parties contractors should be required to undergo a minimum number of hours of awareness training in order to ensure that they are aware of their roles and responsibilities in the Cyberspace, and technical controls that they should implement as individuals using the Cyberspace. In addition, as part of the program to counter social engineering attacks, such awareness training should include contents such as the following:

a) The latest threats and forms of social engineering attacks, for example, how phishing has evolved from fake websites alone to a combination of Spam, Cross Site Scripting, and SQL Injection attacks.

b) How individual and corporate information can be stolen and manipulated through social engineering attacks, providing understanding on how attackers can take advantage of human nature, such as a tendency to comply to requests that are made with authority (even though it can be unreal), friendly demeanour, posing as a victim, and reciprocation by first giving something of value or help.

c) What information needs to be protected and how to protect it, in accordance with the information security policy.

d) When to report or escalate a suspected event or malicious application to approach authorities or response agency, and information on these contacts available. For example, see Annex B.

Organizations providing Cyberspace applications and services online should provide awareness materials to subscribers or consumers covering the above contents within the context of their applications or services.

12.5.3.3 Testing

Employees should sign an acknowledgement that they accept and understand the contents of the organization's security policy. As part of the process to improve awareness and ensure due attention to such risk, an organization should consider conducting periodic tests to determine the level of awareness and compliance with related policies and practices. Employees can perform a written test or undergo CBT to determine if they understand the contents of the organization's security policy. Such tests may include but are not limited to the creation of targeted but controlled phishing sites, Spam, and scam mails using believable social engineering contents. When conducting such tests, it is important to ensure that:

a) the test servers and contents are all within the control and command of the testing team;

b) professionals who have prior experience of running such a test are engaged where possible;

c) users are prepared for such tests through the awareness and training programs; and

d) all test results are presented in aggregated format in order to protect an individuals' privacy as the content presented in such tests can embarrass individuals and cause privacy concerns if not adequately managed.

NOTE: The ethics and legislation of each country must be taken into consideration.

12.5.4 People and organization

While individuals are the primary targets of social engineering attacks, an organization can also be the intended victim. People, however, remain the main entry point for social engineering attacks. As such, people need to be aware of related risks in the Cyberspace, and organizations should establish relevant policies and take proactive steps to sponsor related programs to ensure people's awareness and competency.

As a general guide, all organizations (including enterprise, service providers, and government) should encourage consumers in the Cyberspace to learn and understand social engineering risks in the Cyberspace, and the steps they should take to protect themselves against potential attacks.

12.5.5 Technical

In addition to establishing policies and practices against social engineering attacks, technical controls should also be considered and where possible, adopted to minimize exposure and potential for cyber miscreants' exploitations.

At the personal level, Cyberspace users should adopt the guidance discussed in clause 11.3.

Organizations and service providers should undertake relevant steps described in clause 11.4.4 to facilitate users' adoption and use of technical security controls.

Organizations and service providers should also adopt the guidance provided in clause 11.4, which are important as baseline controls against social engineering attacks in the Cyberspace.

In addition, the following technical controls that are useful against specific social engineering attacks should be considered:

a) Where personal or corporate sensitive information are involved in online applications, consider the provision of strong authentication solutions either as part of the login authentication, and/or when critical transactions are being executed. Strong authentication refers to the use of two or more additional factors of identity verification, over and above the use of a user ID and password. The second and additional factors may be provided using smartcard, biometrics, or other hand-held security tokens.

b) For web-based services, organizations should consider the use of a "High Assurance Certificate" to provide added assurance to online users. Most commercial Certification Authorities (CA) and Internet browsers are capable of supporting the use of such certificates, which reduce the threat of phishing attacks.

c) To ensure the security of users' computers connecting to the organization or service provider's site or application in the Cyberspace, additional controls to ensure a minimum level of security, such as installation of latest security updates, should be considered. Use of such controls should be published in the End-user Service Agreement and/or the Site Privacy and Security Policy whichever is applicable.

12.6 Cybersecurity readiness

Annex A describes additional technical controls that are applicable for improving an organization's Cybersecurity readiness in the area of event detection, through Darknet Monitoring, investigation, through Traceback, and response, through Sinkhole Operation.

12.7 Other controls

Other controls may include controls related to alerting and quarantine of devices which are engaging in suspicious activity as observed through correlation of events from service provider and/or enterprise elements such as DNS servers, router net flow, outbound message filtering and peer-to-peer communications.

13 Framework of information sharing and coordination

13.1 General

Cybersecurity incidents often cross national geographical and organizational boundaries, and the speed of information flow and changes from the unfolding incident often gives limited time for the responding individuals and organizations to act. A system needs to be established for information sharing and coordination to help prepare and respond to Cybersecurity events and incidents. This is an important step that organizations should take as part of their Cybersecurity controls. Such a system for information sharing and coordination should be secure, effective, reliable and efficient.

The system should be secure to ensure that the information being shared, including details about the coordination of activities, are protected against unauthorized access, in particular by the perpetrator of the incident concerned. Security of information relating to Cybersecurity events is also necessary to prevent misinterpretation and causing undue panic or alarms to the public. At the same time, integrity and authenticity

of information are critical to ensure its accuracy and reliability irrespective of whether such information is shared within a closed group, or disclosed publicly. The system should be effective and efficient so that it serves its purpose with minimum resources and within the required time and space.

This clause provides a basic framework for implementing a system for information sharing and coordination. The framework includes four areas for consideration, namely, policies, methods and processes, people, and technical elements.

NOTE ITU-T's Study Group 17 is undertaking extensive work on Cybersecurity information exchange. Refer to Table C.17 — Cybersecurity information exchange for further information.

13.2 Policies

13.2.1 Information providing organizations and Information receiving organizations

For the purpose of this framework, two types of information sharing organizations are introduced:

— IPO, and

— IRO.

As IPO, basic policies with regard to the classification and categorization of information, the severity of events and incidents, and the form of sharing possible should be determined prior to the occurrence of any Cybersecurity incidents, or any sharing takes place (in the case of an IPO turning into an IRO to share received information with other authorized entities in the information chain).

At the receiving end, IRO should agree to enforce the security protection and relevant procedures upon receiving information from the IPO, in accordance with the agreement previously reached, and based on the classification and categorization of information involved.

13.2.2 Classification and categorization of information

IPOs should determine the different categories of information that they collect, collate, safe-keep, and distribute. Examples of information categories can include security events, security threats, security vulnerabilities, suspected/confirmed perpetrators' profiles, organized groups, victims' information, and ICT system profile categories.

For each category, it should be further broken down into two or more classifications based on the contents of the information involved. The minimum classification may be sensitive and unrestricted. If information contains personal data, privacy classifications may also be applied.

13.2.3 Information minimization

For each category and classification, IPO should exercise caution to minimize the information to be distributed. The minimization is necessary to prevent information overload at the receiving end, to ensure efficient use of the sharing system, without compromising effectiveness. Another objective of the minimization is omitting sensitive information to preserve the privacy of people in IPO and IRO. In this regards, IPO and IRO should determine the desired level of details, wherever possible, for each category and classification of information that can be identified prior to the actual sharing.

13.2.4 Limited audience

In line with the minimization principle, a policy to limit the audience, which may be to a specific contact person, group, or organization, for distribution is necessary when sharing information containing private or confidential data. For less sensitive information, such a policy should be considered to prevent information overload, unless the benefits of maximum distribution (such as the sharing of critical security alerts) outweigh the impact of information overload for the IRO.

13.2.5 Coordination protocol

A high-level policy for coordinating the request and distribution (whether it is IPO or IRO initiated) should be established. Such a policy formalizes the protocol involved, which provides a means for the IPO and IRO to respond effectively and efficiently. Mutual authentication and verification procedures could then be built upon such a protocol to ensure the authenticity of origin and proof of delivery where desired, in particular, for sensitive, personal, and/or confidential information.

13.3 Methods and processes

13.3.1 Overview

To effect the information sharing policies, and ensure consistency of practice, effectiveness, efficiency, and reliability of execution, related methods and processes should be developed and implemented. Such methods and processes should be based on available standards. Otherwise, upon operational validation, they may be formalized for standardization. The following clauses provide guidance on the methods and processes that are commonly used by organizations in the industry for achieving relevant objectives and policies of information sharing and coordination in the context of Cybersecurity.

13.3.2 Classification and categorization of information

Information to be shared will come from both open and closed sources. Open source information is often to be found on the internet or from other public sources, such as newspapers. Open source information is generally of the lowest classification because the originators of the information can be multiple or unknown, the age of the information can be undetermined and the accuracy subject to question. Closed source information is not publicly available, often attributable to a source and of known age. Examples of closed source information are proprietary research and analytics, or empirically gathered intelligence.

NOTE the guidance for this clause may be based on the outcome of the Study Period on this topic, referencing the standard if the SP proceeds to development, or adopting a summary of the text from the SP if it terminates without further development.

13.3.3 Non-disclosure agreement

An NDA may be used for at least two purposes in the context of information sharing and coordination for improving Cybersecurity. A typical use of an NDA is to ensure adequate handling and protection of sensitive, personal, and/or confidential information shared among IPO and IRO, and pre-establishing the condition of sharing and further distribution and use of such information.

In the context of responding to Cybersecurity events, the pre-establishment of an NDA enables swift sharing and distribution amongst authorized entities to take place efficiently even if the information classification has not been clearly defined.

13.3.4 Code of practice

One commonly used method to ensure adequate sharing and handling of sensitive information is the establishment of a code of practice, covering detailed procedures, responsibilities, and commitments from stakeholder organizations (i.e., IPO and IRO) for responses and actions to be taken by respective entities involved for each category and classification of information.

EXAMPLE See the future International Standard ISO/IEC 29147, Information technology – Security techniques – Vulnerability disclosure.

13.3.5 Testing and drills

To ensure effectiveness and reliability and to achieve the desired level of efficiency, methods and processes should be developed for conducting regular testing and exercising scenario drills.

A standard methodology should be used as a reference for security testing, in order to fit it down and match with the organization's goals and needs.

Security tests can be performed on high risk assets. This can be assisted by using the organization's own data classification nomenclature.

Security assessments should be performed on a regular basis on the:

— Application

— Operating System

— Database Management System

13.3.6 Timing and scheduling of information sharing

The requirement to share information either proactively or during an incident response will vary from entity to entity. Some organizations will have a requirement for real-time information: the moment an alert or alarm occurs they will want the intelligence for further analysis. Other entities will not possess the resources to manage real-time information sharing. In fact, many organizations may not have the ability to manage schedule information sharing on any interval.

Information sharing timing and schedules should be defined clearly, with specific service level objectives defined for voluntary relationships and service level agreements for commercial relationships.

13.4 People and organizations

13.4.1 Overview

People and organizations are the key determinants to the success of Cybersecurity. People refer to individuals involved in executing the methods and processes for information sharing and coordinating to make a positive difference to the outcomes of Cybersecurity events. Organizations refer to groups of people within a company up to entire company involved in such activities. For effectiveness and efficiency, the needs of both people and organizations should to be considered.

13.4.2 Contacts

A list of contacts should be compiled by the IPO and IRO and mutually exchanged so that each entity can identify the person who requested or sent information on the sharing community.

More granular contact lists may also be developed and shared in accordance with a limited audience (clause 13.2.4) and information classification and categorization (clause 13.2.2) policies.

The contact list should not contain sensitive personal information, in accordance with the information minimization policy (clause 13.2.3). For privacy purposes, an alias may also be considered in place of full name. The minimum information for the contact list should include name (or alias), contactable numbers (mobile phone if possible), and email address. An alternative contact may also be established for each key person in the contact list.

In addition to a contact list for information sharing and coordination, a separate contact list for incident escalation may also be compiled to facilitate swift escalation. Such a list usually includes external contacts that are not in the sharing network. For example, see Annex B.

At the minimum, the contact list should be protected against unauthorized modification to prevent corruption and maintain integrity. Technical controls (clause 13.5) should be applied as appropriate.

13.4.3 Alliances

To facilitate information sharing, and establish common and consistent practices governed by an agreed code of practice, and/or NDA, organizations and groups of individuals may form alliances based on their areas of interest, which may be industry, technology, or other special interest areas. See Annex B for a sample list of existing alliances and non-profit organizations that serve such a purpose.

13.4.4 Awareness and training

People in organizations should be made aware of emerging and new Cybersecurity risks and trained so that they develop the required skills and expertise to respond effectively and efficiently when they encounter specific risk involved, or received information requiring their actions to mitigate or improve a given situation. To achieve these objectives,

— Regular briefings on Cybersecurity risk status and findings concerning the organization and the industry should be provided.

— Focused training sessions Table Top simulated cyber-attack scenarios and workshops on specific required areas of action should be designed, organized, and delivered, to both new comers to the group/organization, with updates on a regular basis.

— Regular testing, with walkthroughs of relevant scenarios to ensure comprehensive understanding and ability to execute procedures and specific tools.

This awareness, training and testing may be performed by internal experts involved, external consultants, or other experts from members of the related alliances involved in the information sharing and coordination efforts.

The use of scenarios as part of the training and testing processes is strongly recommended as such an approach enables individuals to gain near real-life experience of relevant situations and learn and practice the responses required. In addition, past incidents may be used as part of the scenarios to maximize sharing of lessons learnt and understanding gained from those situations.

13.5 Technical

13.5.1 Overview

Technical controls and standardization may be used to improve efficiency, reduce human error, and enhance security involved in the information sharing and coordination processes. A number of technical systems and solutions may be designed, developed and implemented. This International Standard provides some of the commonly used approaches and techniques that have been adopted by some organizations, and may be further adapted for improving the information sharing and coordination needs and processes to deal with the changing Cybersecurity risk environment.

13.5.2 Data standardization for automated system

As part of the sharing network, automated systems may be developed and deployed amongst coordinating organizations to collect data on evolving Cybersecurity events for real-time and offline analysis and assessment, in order to determine the latest security status in the Cyberspace within the boundary of the organizations involved. Such data may include network traffic data, security updates for software systems and hardware devices, security vulnerabilities data, and malware, spam, and spyware data, including their payloads and intercepted information. Automated systems supporting the first responders and incident escalation, as described in clause 13.4.2, would also contain data relating to organizations and people. In view of the sensitivity and volume of the contents of the data involved in these systems, organizations (in particular, alliances of organizations) should evaluate the data schemas and contents to determine suitable technical controls for improving efficiency, effectiveness, and security. These can include, but are not limited to the following:

a) standardization of the data schema for each category and classification of data collected enforcing the information minimization and privacy policy, and providing technical assurance to all participating entities, and data owners of such a practice;

b) standardization of data format to ease sharing and improve storage, transmission, handling and interoperability between systems. For example, see ITU-T X.1205; and

c) standardization of basic data processing functionality and algorithms used, for example, hash function and procedures for IP address anonymization and other pre-processing requirements.

13.5.3 Data visualization

Consider using data visualization techniques to present events information, which helps to improve visibility of changes and the emerging security incident taking place without the need for the operators to read the details of each event as it emerges. For example, see Annex A, which presents a visual representation of Darknet activities, which facilitates a more efficient response to the changes.

13.5.4 Cryptographic key exchange and software/hardware backups

To facilitate sharing of confidential information, a cryptographic system, including a system for key exchange that could be quickly deployed should be considered for implementation. The system should include adequate backups for the software and hardware, as well as the keys used in preparation for the sharing purposes and emergency recovery needs.

13.5.5 Secure file sharing, instant messaging, web portal, and discussion forum

To facilitate online interaction and quick and secure information sharing, which may include sharing of digital contents such as text and multimedia files, and both online and offline discussions, the sharing organizations (IPO and IRO) should consider adopting suitable file sharing tools, instant messenger, and online discussion forum tools that could meet the security, effectiveness, efficiency, and reliability needs.

Web portal provision feeds on Cybersecurity events and status should be implemented as a form of communication for both public and private community interested and involved, respectively. Where such a web portal is used, there should be clear administrative ownership and responsibility to ensure its security and availability, and private areas should be provided for limited audience information where necessary.

13.5.6 Testing systems

While each technical system and related methods and processes should be tested rigorously to ensure their reliability and integrity, one or more technical systems dedicated for improving the efficiency and effectiveness of testing, in particular, scenarios testing, should be considered. Such a system may be in the form of a simulation system to simulate the operating environments as perceived by each organization of the Cyberspace, and evolving Cybersecurity situation, providing the capability for introducing a series of security events to facilitate required test to be performed.

13.6 Implementation guidance

The implementation of such a framework requires collaborating organizations and individuals to get together (virtually or physically) to determine specific policy, controls and steps to take in order to achieve its objectives of secure, effective, reliable, and efficient information sharing and coordination in response to emerging Cybersecurity incidents. The following high-level steps are recommended as a guide for the implementation:

a) Identify and gather relevant organizations and individuals to form the required information sharing and coordination network community, either informally or formally;

b) Determine the role(s) of each organization/individual involved either as IPO, IRO, or both (clause 13.2.1).

c) Establish the kind of information and coordination required that would be beneficial to the community;

d) Perform information categorization and classification to determine if any sensitive and/or privacy information are involved (clause 13.2.2);

e) Establish policies and principles governing the community and the information involved (clause 13.2);

f) Determine the methods and processes required for each category and classification of information involved (clause 13.3);

g) Determine performance requirements and criteria, and establish Code of Practice and sign NDA as necessary (clauses 13.3.3 and 13.3.4);

h) Identify required and suitable standards and technical systems to support the implementation and operations of the community (clause 13.5);

i) Prepare for operation; collate contact list; and conduct awareness and training workshops to prepare stakeholders;

j) Conduct regular testing, including scenarios walkthrough and simulation, as necessary (clauses 13.3.5 and 13.5.6);

k) Conduct periodic, post-test, and post-incident reviews to improve the sharing and coordination systems, including people, processes, and technology involved; expand or reduce the size of the community as necessary.

NOTE ISO/IEC 27001, Information technology – Security techniques – Information security management systems requirements and ISO/IEC 27003, Information technology – Security techniques – Information security management system implementation guidance provide requirements and implementation guidance respectively.

Annex A
(informative)

Cybersecurity readiness

A.1 Overview

The Cybersecurity controls described in clause 12 minimize organizations and end-users' exposure and risk to most of the known Cybersecurity attacks. Upon the emergence of Cybersecurity incidents, the framework for information sharing and coordination described in clause 11 provides for establishing a system for information sharing and coordination in preparation for responding to Cybersecurity events and incidents. Such information is adequately protected between the IPO and IRO.

While these controls reduce risk and improve incident handling and management, cyber criminals or other miscreants will continue to develop new or evolve current attacks to overcome existing protections. It is therefore also important for organizations to implement systems and infrastructures that enable a more dynamic and rigorous approach to security attack detection, investigation and response.

ISO/IEC 27031 provides guidance on management systems and related processes to prepare an organization's ICT systems to detect and respond to emerging security events, including Cybersecurity events. This guideline highlights additional technical approaches that are applicable for improving an organization's Cybersecurity readiness in the area of event detection, through Darknet Monitoring, investigation, through Traceback, and response, through Sinkhole Operation.

Organizations, in particular CIIPs should consider leveraging these approaches to improve their Cybersecurity readiness and therefore status.

A.2 Darknet monitoring

A.2.1 Introduction

The Darknet is a set of IP addresses that are not used in organizations. IP addresses in Darknet are not assigned to any operational servers/PC systems. By using monitored packets in the Darknet IP domains, organizations could observe emerging network attacks, including malware-initiated network scanning, malware infection behaviour and DDoS Backscatters. Since IP addresses of the Darknet are public, but are not assigned to legitimate hosts, all incoming traffic belonging to Darknet IP domains can be inferred as a consequence of either malicious activities, or that of incorrect configurations.

There are, in general, three methods commonly used in Darknet to observe malicious activities related traffics on the Internet, namely, Black Hole Monitoring, and Low and High Interaction Monitoring.

A.2.2 Black hole monitoring

Black Hole monitoring refers to monitoring systems which do not respond to anything against incoming packets found within the Darknet IP domains. This type of monitoring system is often used to quietly observe network ports scanning by malware, and malware infection behaviour (UDP with payload including shell code) and DDoS Backscatters. Network port scanning is often the initial step taken by attackers to search for vulnerable host systems that can be exploited. The malware infection behaviours are normally the follow-up steps taken by the attackers after identifying the vulnerable host systems. Such infection actions are often observed to use UDP with payload on the black hole monitoring. Furthermore, DDoS Backscatters are also observed by means of Black Hole monitoring in the case of spoofing source IP addresses (attackers) and the target of DDoS can be recognized by this Backscatters traffic. Figure A.1 depicts a screen capture of a visualization of the malware activities detected by a Black Hole monitoring system. A sample video link can be found here: https://www.youtube.com/watch?v=asemvKgkib4&feature=related.