



木

Section Two

Guidelines for Cybersecurity

ISO/IEC 27032 – Guidelines for Cybersecurity is a work-in-progress that aims to provide an overview of the unique security challenges in Cyberspace. Cyberspace, while not existing in any physical form, is a complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it. This complex environment is build on interconnecting networks and systems, as well as any ICT devices, belonging to different organisations and service providers that allow for the flow of information. However, there are security issues that are not covered by current information security, Internet security, network security and ICT security best practices because of gaps between these domains. Cyberspace security, or Cybersecurity, is about the security of the Cyberspace. It provides guidance to address issues arising from the gaps between the different security domains in the Cyberspace environment. At the same time, Cybersecurity provides an infrastructure for collaboration between security stakeholders in the Cyberspace.

“ **Aloysius Cheang**
Head of Security Services, Asia, Cable & Wireless
Co-Editor, ISO/IEC 27032 – Guidelines for Cybersecurity
Member, Security and Privacy Standards Technical Committee ”

1 INTRODUCTION

The Internet, the Cyberspace and the virtual worlds that reside in the Cyberspace, the many web applications that support activities on the cyberspace and breath life into the virtual worlds, and the pervasiveness of mobile devices connect the world into a global village. As a result, the boundary of enterprises and their IT assets are not clearly defined when the relationship of businesses, customers and supplies are all but one major supply chain.

Cyberspace, while not existing in any physical form, is a complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it. This complex environment is build on interconnecting networks and systems, as well as any ICT devices, belonging to different organisations and service providers that allow for the flow of information. However, there are security issues that are not covered by current information security, Internet security, network security and ICT security best practices because of gaps between these domains. Cyberspace security, or Cybersecurity, is about the security

of the Cyberspace. It provides guidance to address issues arising from the gaps between the different security domains in the Cyberspace environment. At the same time, Cybersecurity provides an infrastructure for collaboration between security stakeholders in the Cyberspace.

Cybersecurity has been a subject of growing concern, especially since 9-11 where it was discovered that terrorists use the Internet extensively in communications, counter-intelligence, research of targets and dissemination of their doctrines [1]. Recently, the importance of Cybersecurity reached the heights of its concern with the appointment of a Cybersecurity Czar [2] in US that collaborated directly with the President himself with other countries such as UK following. The focus of building and integrating the function of IT security in the government and according it to the same status with other age-old profession such as accounting and medicine pave the way for private companies to follow suit. Furthermore, a survey conducted by Gartner on top 10 business and technology priorities in 2008 [3] on 1,500 Chief Information Officer ("CIO") worldwide revealed that Asian CIO ranked security as the 2nd most important priority as compared with a worldwide priority ranking of 6th. The reason for the growing concern is Cybersecurity issues arising from the new way of doing business today - reaching out to customers on the Internet, or even doing business on the Internet. Thus, the demand for Cybersecurity is obvious.

2 THE CAUSE FOR CONCERN

Besides being represented on the Internet by their websites, enterprise corporations, governments, and individuals have been establishing presence and attempting to leverage the virtual world in the Cyberspace such as "Second Life" [4] and social networking sites. Increasingly, businesses are conducted on the Cyberspace and many business initiatives are driven by Cyberspace exposure, which see the rise of Internet giants such as Amazon and Google, who engages in online shopping and online advertisements respectively. These developments, from communication, entertainment, transportation, shopping, financial, insurance, and healthcare, create new risks to organisations (either as a provider or consumer), and companies, in particular privacy and copyrights, on the Cyberspace.

The convergence of information and communication technologies, the ease of getting onto the Cyberspace, and the narrowing of personal space are similarly gaining the attention of individual miscreants and criminal organisations, developing newer attack techniques such as identity theft, phishing, spam and spyware to exploit any weaknesses they can discover on the Cyberspace, be it technical or social. In recent years, security attacks on the Cyberspace have evolved from hacking for personal fame to organised crime [5], or Cybercrime where a plethora of tools and processes previously observed in isolated Cybersecurity incidents are now being used together in multi-blended attacks that are orchestrated and often with a far reaching (malicious) objectives, from personal attacks (such as Cyber-bullying), to financial frauds/thefts, to political hactivism. Specialist forums to highlight potential security issues have also served to showcase attack techniques and criminal opportunities.

Key services that often become the target of these Cybercrime syndicates are the multiple modes of business transactions that are carried out in the Cyberspace. Ranging from business-to-business, business-to-consumer to consumer-to-consumer, the complexity of the risks posed is inherently complex. 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, which may eventually lead to potential security risks such as information leakage. While current

progress to address these challenges has been hampered by many issues such as legal and technical challenges, Cybersecurity issues are increasing and continuing to evolve. Their potential is boundless and limited only by human imagination.

3 THE INTERNATIONAL STANDARD

In recognition of the need, ISO/IEC approved the creation of a new International Standard, ISO/IEC 27032 [6] that will provide Guidelines for Cybersecurity. Currently the standard is into its 3rd working draft after two years of work incorporating the views and best practices provided by experts representing countries worldwide.

This International Standard define and provide the scope for Cybersecurity while differentiating Cybersecurity from Internet security, network security, ICT security, and information security in general, choosing to focus on bridging the gaps not addressed by best practices and standards in these areas. Another aspect of importance is collaboration, since 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 protects also the privacy of 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.

However, the Cyberspace belongs to no one. Everyone can be part of the Cyberspace, and have a stake in the Cyberspace, which makes it even more difficult to define and draft his International Standard. Hence, for the purpose of this International Standard, stakeholders in the Cyberspace are categorised in the following groups:

- Consumers, including
 - individuals;
 - organisations; and
 - governments
- Providers, including service providers.

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 organisational roles within their personal or organisation networks. The term organisation network refers to the combination of an organisation's private networks (typically the intranet), extranets and publicly visible networks. Publicly visible networks are those networks exposed to the Internet, for example to host the website. Because of this overlap, these roles can appear to have insignificant or no direct benefit to the individual and organisation concerned. They are, however, significant to enhancing Cybersecurity when all involved act accordingly.

This International Standard takes a multi-front approach to address Cybersecurity risks that 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 organisation as well as in the Cyberspace;

- Innovative technology solutions to help protect users from known Cybersecurity attacks, stay current and be prepared against new exploitations; and
- Legislation and enforcement by government, with assistance from industry, to discourage the development of Cybersecurity attack methods and tools, including malicious software, and potentially unwanted software.

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

- Key roles involved;
- Policies;
- Methods;
- Processes; and
- Applicable technical controls.

4 THREATS AGAINST THE SECURITY OF THE CYBERSPACE

To arrive at the relevant Cybersecurity controls, the International Standards will have to identify the threats posed against the security of the Cyberspace first. However, the threats that Cyberspace faces are extensive and complex. These threats are discussed in relation to assets in the Cyberspace.

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

- Threats to personal assets;
- Threats to organisational assets;
- Threats to virtual assets; and
- Threats to infrastructure.

Personal threats revolve mainly around privacy and identity issues, posed by the leakage or theft of personal information or information pertaining to credit information. If a person's online identity is stolen or used in a masquerade, 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. Unauthorised 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 being made a zombie or bot. Personal computing devices can become compromised and so become part of a larger botnet.

On the other hand, organisations' online presence and online business are often threatened or held at ransom. Organisations are often threatened by organised cybercrime syndicate [7] that their websites will be brought down, or that they will be caused embarrassment through actions such as website defacement.

Virtual world today is worth a lot of money. Online currencies are actually worth their dime in real world money. And the avatars, weapons and items in an online game can be sold and bartered in the real world as well. However,

how to we protect such items in the absence of safes and locks that we are used to in the real world? And how to prove ownership and to prevent identity theft?

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 Cyberspace, specifically the difficulty of defining boundaries and borders, it is difficult to regulate and control the way that it can be used. They are the key threats to critical infrastructure as well as national owned infrastructure. 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.

5 CYBERSECURITY CONTROLS

This International Standard provides technical guidance for addressing common Cybersecurity risks, including:

- Social engineering attacks;
- The proliferation of malicious software ("malware");
- Spyware; and
- Other potentially unwanted software.

Some of the key technical issues that will and may be covered includes:

- Web 2.0 including true network applications offering Software As A Service and potentially Security As A Service;
- Peer-to-peer networking;
- Instant messaging;
- Voice and video over IP and other IP-based services that are replacing traditional services; and
- Phishing and risks from social networking sites.

This International Standard provides controls for addressing these risks, including controls for:

- Preparing for attacks by, for example malware, individual miscreants, or criminal organisations on the Internet;
- Monitoring possible attacks; and
- Responding to attacks.

6 FRAMEWORK OF INFORMATION SHARING AND COORDINATION

Cybersecurity incidents are often cross national, geographical and organisational boundaries, and the speed of information flow and changes to an incident that is unfolding often give limited time for the responding individuals and organisations to act. Establishing a system for information sharing and coordination in preparation for

responding to Cybersecurity events and incidents is therefore an important step that organisations should take as part of their Cybersecurity controls. Such a system for information sharing and coordination should be secure, effective, reliable and efficient.

It should be secure to ensure that the information being shared and actions being coordinated are protected against unauthorised access, in particular, by the perpetrator of the incident concerned. Security of information relating to Cybersecurity events and information 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 that they are accurate and reliable whether such information are shared within a closed group, or disclosed publicly. It should be effective and efficient so that it serves its purpose with minimum resources and within the required time and space.

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; and
- Necessary processes for collaboration and information exchange and sharing as well as technical requirements for systems integration and interoperability between different stakeholders.

7 CONCLUSION

In developing this International Standard, we have made reference to work done by ITU-T Study Group 17 Question 6/17 [8], especially from their efforts on Cybersecurity [9] and their recommendations to address spywares and other unwanted software [10]. This International Standard intentionally takes a stand to put a definition to Cybersecurity, excluding references to critical information infrastructure protection, network security etc., which are already addressed by other standards. It also takes an effort not to be influenced strongly by any stance adopted by any single country. Instead, this International Standard adopt a work by consensus among ISO member countries that participate in the working group meetings so as come to an agreement to an acceptable definition and scope by most member countries. While some may not agree to all decisions made during the ISO/IEC meetings, but at this point in time we are moving ahead by decision of the majority. We have decided that the focus of this International Standard is not to list all the actual controls that will resolve threats, current or future to Cybersecurity, but to identify the process that we hope that countries, organisations and responsible individuals will assume to safeguard and protect our cyberspace, which is a virtual representation of our world. The process which we are so hopeful cumulate into the framework for information sharing and coordination that we propose in the last clause of the International Standard.

Thus, the controversies delayed the progress of this International Standard for the last two years. Fortunately, we managed to move into third working draft status and we are on track for the first committee draft by the ISO/IEC fall meeting in November this year, representing results of the enormous effort that we undertake to bring the status of the International Standard to this level after the initial impasse since the ISO/IEC Spring meeting in 2008. Our work has also attracted attention from CEN and we have sent them a liaison statement, besides updating ITU-T of our progress, thus hoping that we can address each other shortcomings in our work as well avoiding duplication of work while finding each other a niche area that we can focus so as to complement each other's work.

8 REFERENCES

- [1] Internet empowered 9/11 terrorists, too, says Pulitzer.
- http://my.brandeis.edu/news/item?news_item_id=100550&tshow_release_date=1
- [2] Obama Set to Create A Cybersecurity Czar With Broad Mandate.
- <http://www.washingtonpost.com/wp-dyn/content/article/2009/05/25/AR2009052502104.html>
- [3] CIOs in Asia expect IT budget growth of 8.3 percent in 2008 compared to worldwide average of 3.3 percent.
- <https://www.gartner.com/it/page.jsp?id=604408>
- [4] Sweden is the first country to set up an official embassy in "Second Life".
- <http://www.sweden.se/secondlife>
- [5] Organised crime and Cyber-crime: Implications for businesses.
- <http://www.cert.org/archive/pdf/cybercrime-business.pdf>
- [6] ISO/IEC 27032 Guidelines for Cybersecurity.
- http://www.iso.org/iso/catalogue_detail.htm?csnumber=44375
- [7] Symantec Internet Security Threat Report.
- <http://www.symantec.com/business/theme.jsp?themeid=threatreport>
- [8] ITU-T Study Group 17 Question 6/17.
- <http://www.itu.int/ITU-T/studygroups/com17/sg17-q6.html>
- [9] ITU-T X.1205, Series X: Data Networks, Open System Communications and Security, Telecommunication Security - Overview of Cybersecurity.
- [10] ITU-T X.1207 (04/2008), Series X: Data Networks, Open System Communications and Security, Telecommunication Security - Guidelines for Telecommunication Service Providers for Addressing the Risk of Spyware and Potentially Unwanted Software

BIOGRAPHY OF AUTHOR



Aloysius Cheang

Head of Security Services, Asia, Cable & Wireless
Co-Editor, ISO/IEC 27032 - Guidelines for Cybersecurity
Member, Security and Privacy Standards Technical Committee

Aloysius Cheang is a senior information technology (IT) executive with extensive experience in managing and delivering direct business values in strategic and complex multi-million dollar IT programmes and business projects for top Global 500 organisations across Asia, USA and Europe. He has substantial experience working on a wide variety of complex technology and business solutions, specialising in information risk management and IT security, where he has developed information security strategies, frameworks, policies and controls as well as rolling out large scale security programmes worldwide in many consulting engagements.

An active business leader and a member of the Singapore government's Chief Security Officer roundtable, Aloysius have supported many security awareness movement and cultivated many security groups. He was instrumental in setting up the Association of Information Security Professionals (AISP) backed by the Singapore government, where he was protem chairman from 2006-2007. Besides being one of the Co-Editors for ISO/IEC 27032 "Guidelines for Cybersecurity", he had previously contributed towards the development of SS 507 "Business Continuity/Disaster Recovery Industry Standard" that was adopted as ISO/IEC 24762. Aloysius holds B. Sc (Hons) and Masters in Computer Science and is a Doctor of Business Administration candidate. His professional certifications include CISA, CISSP and GCIH. He is the first Microsoft Security MVP in South Asia and a member of the Microsoft SEA MVP Hall of Fame.