

# 4 Standards for Cybersecurity



**This paper discusses the scope of focus and progress so far** with regards to the development of security standards for addressing the Cybersecurity challenges, including a brief discussion on some of the main standards that are being developed. A secondary aim of this paper is to highlight the practical considerations and challenges in developing such standards, and ask readers for feedback and contributions towards the objectives of this standardisation track.

The scope of this paper is confined to the work of ISO/IEC JTC1 SC27, and ITU-T SG17.

**Kang Meng-Chow**

CISSP, CISA

Regional Chief Security & Privacy Advisor, Microsoft Asia Pacific

Convenor, Security Controls and Services Standards Working Group, ISO/IEC JTC1/SC27/WG4  
Chairman, IT Security and Privacy Standards Technical Committee (SPSTC)

## 1 Background and Motivation

The proliferation of the Internet has enabled new businesses and brought about many benefits to consumers at home and in the workplace. With the inherent openness of the Internet, and the interconnectivity and speed of access that it provides, it has grown to be an effective platform for business and consumers' communications and collaboration. With developments such as Instant Messaging [1], Wiki [2], Real Simple Syndication (RSS) [3], and Blogging[4-6], the Internet has evolved from a mostly one-to-many web based information dissemination platform to a complex interconnected system providing fast changing many-to-many interactions, allowing anyone to actively contribute to its contents using an assortment of mobile and wireless devices rather than just consuming them previously from a fixed wired desktop computer. In recent years, this open, seamlessly interconnected, and highly interactive architecture is increasingly being exploited by cyber criminals, rogue individuals and businesses for financial gains and other criminal purposes, through the use of various forms of malicious software [7-9], SPAM [10], phishing [11], network and systems intrusions [12], social engineering attacks [13] on computing systems, and end-users. However, not all attacks are financially motivated. For example, Hacktivism [14], which also capitalises on network, systems, and applications security weaknesses, exploits them for pursuing specific political purposes.

The implications of such exploitations and related cyber incidents are immense. At the minimum, they undermine users' confidence and trust of computing systems and the Internet, retarding social and economical progress. In many cases, hefty financial and reputation losses had been incurred resulting from such attacks [15]. As such, developing security measures and countermeasures to protect and respond against such attacks are paramount to ensure the trustworthiness, including security and reliability of the Internet.

In this context, at the World Telecommunication Standardization Assembly (WTSA) held in Florianópolis in 2004, three major resolutions were made, requiring actions from ITU-T Study Group 17 to develop new security standards and Recommendations to protect related infrastructure and systems against those Cybersecurity challenges, including addressing the issues of SPAM, the needs for raising users' awareness, and the needs to continue promoting cooperation among appropriate entities to defend information and communication infrastructure and systems against the threat of cyber attacks [16]. In short, new security standards are necessary to support the trust and protection needs of Cybersecurity.

The importance of security standards is also observed from the January 2004 development within the International Organization for Standardization (ISO), in which a high-level strategic Advisory Group on Security (AGS) was formed in the Technical Management Board (TMB) to review ISO's and other organisation's existing standards relating to security and to advise TMB on the need for new standards. In a study report published in January 2005 [17], the AGS recognised that security considerations must become an integral element in products, systems, and operations supporting the day-to-day functioning of society. Cybersecurity was called out as one of the action items for JTC1 to *examine whether standards could play a role in preventing new types of attack, such as viruses, worms, and phishing*. Both the national and international standards-setting communities and organisations recognise that the need for security standards is urgent and overwhelming.

## 2 Purpose

This paper discusses the scope of focus and progress so far with regards to the development of security standards for addressing the Cybersecurity challenges, including a brief discussion on some of the main standards that are being developed. A secondary aim of this paper is to highlight the practical considerations and challenges in developing such standards, and ask readers for feedback and contributions towards the objectives of this standardisation track.

The scope of this paper is confined to the work of ISO/IEC JTC1 SC27, and ITU-T SG17.

## 3 Standards Benefits, Pitfalls, and Relevance to Cybersecurity

In general, standards serve two fundamental requirements, i.e., interoperability and baseline establishment.

With a wide range of technologies and products developed in the open market economies, many end systems could easily be incompatible or not interoperable with other business systems if not for the development and use of open standards. More serious challenges to businesses and end users would follow when their security needs could not be integrated due to non-interoperable technologies and products. Besides increasing business operating cost and inefficiency, incompatible security systems would also create unwanted security gaps, and likely to be ignored by users, resulting in further wastages of resources that are already limited in today's businesses.



In addition to security interoperability, standards help to establish a baseline for achieving common security requirements, which in many ways, help to set basic expectation and ensure known security issues are adequately addressed with proven solutions, or documented best practices. Baseline security standards could also be leveraged to raise the bar on minimum security levels, helping organisations achieve a higher level of trust in today's hostile environment. In the operational environment that constantly needs to deal with changing security threats, standardisation of infrastructure components and system processes provides an effective means to ensure that security updates could be tested and deployed efficiently and effectively to mitigate evolving risks on those systems. An organisation's responsiveness to a changing threat environment is paramount to its success and survival in the world of Internet commerce today.

From an information sharing and communication perspective, standards in security would further provide a means to narrow if not close the communication and collaboration gaps between security professionals and security organisations. Through the use of standards, a common platform and language for identifying and sharing best practices could be achieved, which in turn provide for better interaction within the security community. This is indeed a critical aspect in improving the overall security environment.

These benefits of standardisations are similarly relevant in the Cyberspace, and applicable to support the needs of Cybersecurity. In the area of interoperability, standardisation of data formats and semantics over security related information, for example, security advisories, and patch information, provide the structure for improving communications amongst various security technologies and services providers, intermediaries (such as ISP<sup>1</sup>), applications, and consumers. Such interoperability standards improve automation of security systems, facilitate better protection, enable more accurate detection, rapid alert and escalation, and faster resolution of emerging security issues across different technologies platforms and applications.

In the area of baseline standardisation, minimum security requirements could be consistently established to eliminate known security weaknesses, particularly, in technology deployment and operations, raising the bar that a perpetrator would need to overcome in order to compromise Cybersecurity. Baseline standards also provide for the sharing of best practices amongst similar vertical industries, for example, secure web hosting services amongst ISPs, as well as horizontal practices across different industries, such as, incident response handling and management.

It is also important to note that standards are not a silver bullet to Cybersecurity, or any other security challenges. As discussed in [18], some possible pitfalls of security standards include standardising weak or insecure mechanisms or processes when the standardisation process failed to apply sufficient rigor to or could not assure the security of the underlying design involved; and possible bypassing of crucial design or analysis steps by systems designers when standards are available but may not be fully compatible to the problem area. These pitfalls could potentially result in mass deployment of weak security mechanisms and creation of a false sense of security when a generic security standard has been deployed.

<sup>1</sup> Internet Service Providers (ISP).

## 4 ITU-T Study Group 17

In ITU-T Study Group 17, a meeting was held in November 2004 in Tokyo to begin deliberation on the possible approaches to the development of standards for Cybersecurity. Question<sup>2</sup> 6 was assigned as the lead working group responsible for this task. In the follow-up meeting in April 2005, Question 17 was formed to focus on the standards for 'Countering SPAM by Technical Means'. The development of an ITU-T Recommendation on 'Incident Handling and Management' was also started in Question 5, based on ISO/IEC TR 18044:2004, a similar standard that was published by ISO/IEC JTC1 SC27.

### 4.1 Cybersecurity Overview

While the benefits and applicability of standards are clear, the definition and scope of Cybersecurity as a subject of concerns are not consistent amongst researchers and also practitioners. Defining Cybersecurity and providing an overview of its security challenges, current issues and dilemmas, and available solutions is therefore undertaken as one of the first steps in ITU-T Study Group 17 Question 6 (Q6/17) working group. In April 2006, a working definition was developed, which defines the term Cybersecurity as follows:

*Cybersecurity means the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect organisation and user's assets on the cyber environment. Organisation and user's assets include connected computing devices, computing users, applications/services, communications systems, multimedia communication, and the totality of transmitted and/or stored information in the cyber environment.*

*Cybersecurity ensures the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the cyber environment. The security properties include one or more of the following:*

- *Availability;*
- *Integrity, which may include authenticity and non-repudiation; and*
- *Confidentiality.*

The definition set the stage for the development of an overview document describing the various aspects of Cybersecurity covered in it. This includes risk management strategies and techniques, values of training and education in protecting network, and various Cybersecurity technologies that are available to remedy the security risks involved. A discussion of Cybersecurity standards, Cybersecurity implementation issues and certification is also planned for the overview document.

While this document is being developed, it is important to also note that many existing security standards are still applicable for Cybersecurity needs. The question is what new standards are required given the changes of the risk environment on the Internet.

<sup>2</sup> In ITU-T, standards development working groups are known as Questions, as each working group is assigned a set of questions for review, evaluation, and identify and development suitable standards to resolve them.



## 4.2 Anti-SPAM Standards

In the past few years, SPAM has been one of the biggest concerns amongst businesses and end-users. Besides using up network bandwidth and email storages, SPAM has been a popular carrier of malicious contents for phishing attacks, Botnet propagation, and Spyware and other deceptive software proliferations. As such, addressing the SPAM problem is one of the requirements for improving Cybersecurity.

In ITU-T Q17/SG17, the Recommendations currently being developed to support the anti-SPAM initiative includes the following:

- Requirements for countering SPAM;
- Technical framework for countering email SPAM;
- Guideline documents on countering email SPAM;
- Overview of countering SPAM for Internet Protocol (IP) enabled multimedia applications; and
- Technical means for countering SPAM.

These Recommendations focused on providing the baseline standards to address the SPAM issues in the various technology contexts. The interoperability requirements for the different anti-SPAM techniques available are however not considered for development at this stage.

## 4.3 Spyware and Other Deceptive Software

Following closely alongside the SPAM issue is the proliferation of Spyware and various kinds of deceptive software such as Keystroke Logger and Trojans programs that disrupt usability and compromise the security of personal and/or sensitive information in end-users' computing systems.

Besides the use of anti-spyware and other anti-malware tools for preventing and eradicating such attacks at the users' systems, Q6/SG17 identified that there are steps that ISPs and end-users may also adopt and practice to address the risks of spyware and deceptive software. As such, a 'Guidelines for Internet Service Providers and End-users for Addressing the Risk of Spyware and Deceptive Software' was proposed and currently being developed. The draft Recommendation currently defines Spyware and Deceptive Software as follows:

- 'Deceptive software' is software which performs activities on a user's computer without: 1) notifying the user as to exactly what the software will do on the user's computer, or 2) asking the user whether they consent to the software doing these things. (Examples of deceptive software include programmes which hijack user configurations, or programmes, which cause endless pop-up advertisements which cannot be easily clicked out of by the user).
- 'Spyware' is a particular type of deceptive software that collects personal information from a computer user. The personal information may include matters such as web sites most frequently visited or more sensitive information such as passwords.

The Recommendation promotes best practices around principles of clear notices, users' consents, and controls for ISP web hosting services. The Recommendation also promotes best practices to Internet users on the techniques and measures available for securing their computing devices and information against the risks of Spyware and deceptive software.

#### 4.4 Vulnerability Information Management and Data Exchange Format

From the perspectives of protection and response when dealing with Cybersecurity issues, one of the common challenges in enterprises is identifying appropriate security patches for testing and deployment before any exploitation of related vulnerabilities have taken place. However, the coding, depth of patch, and vulnerabilities information provided by technology vendors vary from vendor to vendor. As most enterprises have a heterogeneous technology environment, translating the security advisories are often a challenge. To manage this effectively, enterprises need to establish a management system complementing the information security management system focusing on vulnerability management. In addition, a system for translating security advisories of different vendors into a standard structure would facilitate the patch identification, testing, and deployment processes as part of the vulnerability management system. In view of these requirements, two Recommendations have been initiated in ITU-T Q6/17 in April and October 2005, respectively:

- 1) Guidelines on Cybersecurity Vulnerability Life-cycle Management - This Recommendation provides a framework for the provision of monitoring, discovering, responding and post-analysis of vulnerabilities. Service providers can use this Recommendation to complement their existing Information Security Management System process in the aspect of regular vulnerability assessment, vulnerability management, incident handling and incident management.
  
- 2) A Vendor-Neutral Framework For Automatic Checking Of The Presence Of Vulnerabilities Information Update - This Recommendation provides a framework for automatic notification on vulnerability information. The key point of the framework is that it is a vendor-neutral framework. Once users register their software, updates on the vulnerabilities and patches of the registered software will automatically be made available to the users. Upon notification, users can then apply patch management procedure to update their software.

#### 4.5 Remarks

In addition to the above new development in support of the standards needs for Cybersecurity, a number of Recommendations that have been published by ITU-T are also relevant for addressing their respective aspects of Cybersecurity. This includes, but not necessarily limited to the following Recommendations:

- 1) X.805 (2003) - Security Architecture, for end-to-end communications.
  
- 2) X.1501 (2004) - Security Management Systems, for risk assessment, identification of assets, and implementation of a system for information security management in the telecommunication industry sector.



- 3) X.1121 (2004) and X.1122 (2004) – Mobile Security, for end-to-end data communications security in mobile network.

In the April 2006 SG17 meeting in Jeju, Korea, the standardisation needs to deal with the security interoperability and baseline security requirements on digital identity and identity management systems were also discussed. Q6/SG17 has been tasked to take lead in this area. New work item in this aspect will likely be initiated in the near future.

## 5 ISO/IEC JTC1 SC27 – Security Techniques

In April 2006, ISO/IEC JTC1 SC27 completed its re-organisation with the creation of two new working groups. Working group 4 (WG4), named as 'Security Controls and Services', is chartered to develop and maintain security controls and services related standards in support of the implementation of ISO/IEC 27001 (Information Security Management Systems) and ISO/IEC 17799 (Code of Practice for Information Security Management). This includes identifying and developing suitable standards for Cybersecurity requirements, in coordination with other standards bodies, such as ITU-T SG17. Another working group (WG5) was also formed in SC27, focusing on the security standards needs of privacy technology, biometrics systems, and identity management.

As part of this development, WG1 and WG4 of SC27 will be holding a planning workshop in Singapore on 31 October 2006, followed by a Cybersecurity Symposium on 1 November 2006. The two-day event will focus on identifying new work items for meeting the standards needs of Cybersecurity, amongst other things.

### 5.1 Remarks

While the plan for Cybersecurity standards is being developed in ISO/IEC JTC1 SC27, it is important to note that a number of existing ISO/IEC security standards remain applicable and important for addressing the various aspects of Cybersecurity. This includes:

- 1) ISO/IEC 18028 series of standards on network security:
  - ISO/IEC 18028-1:2006 - 'Network security management'
  - ISO/IEC 18028-2:2006 - 'Network security architecture'
  - ISO/IEC 18028-3:2005 - 'Securing communications between networks using security gateways'
  - ISO/IEC 18028-4:2005 - 'Securing remote access'
  - ISO/IEC 18028-5: 2006 - 'Securing communications across networks using virtual private networks'
- 2) ISO/IEC 18043:2006 - 'Selection, deployment and operations of intrusion detection systems (IDS)'
- 3) ISO/IEC 18044:2004 - 'Information security incident management'
- 4) ISO/IEC 24762 - (1st CD 2006) - 'Guidelines for information and communications technology disaster recovery services'

## 6 Other Areas for Considerations

While several new work items focusing on addressing the standards needs of Cybersecurity have been identified and initiated in ITU-T, and similar efforts are being undertaken by ISO, it remains an ongoing challenge to ensure exhaustive coverage of these developments. For example, the rapid growth of online communities through technologies such as Instant Messaging, Blogging, Podcasting, VideoCasting, Peer-to-peer File Sharing, and Voice-over-IP have not been fully examined from a security standards perspective. Although they share most of the threats that standards have been developed or are being developed to address, the specific capability of each of these technologies may justify different security standards either from the interoperability or baseline viewpoints. From a threat angle, phishing, viruses, denial of services and similar attacks should also be evaluated to determine whether and how standards may be used to minimise, if not fully address these issues.

To ensure effective and efficient standards are being developed for addressing Cybersecurity needs, new contributions from researchers and practitioners are a critical success factor. This may include but not limited to security requirements, issues or problems definitions, desired usage scenarios, technical specifications, and best practices for addressing the Cybersecurity challenges with regards to the use of these new technologies.

## 7 Conclusion

The changing risk situation requires that we take a new look at the standards needs for Cybersecurity. While there are areas requiring new standards development, a number of existing security standards available in both ISO/IEC and ITU-T remain applicable and important for addressing the fundamental needs of information security, in both enterprise IT environment, and the Cyberspace.

The challenges of Cybersecurity will not be over even if we have all the relevant standards identified and developed today. Adoption and implementations will take time, as much as creating awareness and competency in understanding and deploying those standards. By the time we have achieved those milestones, the Cyberspace landscape would also have changed and evolved further. What this means is the need for constant vigilance and more importantly, having standards that will not result in the set up of rigid structures that do not allow for future growth or change, or do not allow us to respond effectively and efficiently to the development of new risks and requirements in the Cyberspace.

## 8 References

- [1] Webopedia. *Instant messaging*. 14 May 2004 [cited 2006 July 19]; Available from: [http://www.webopedia.com/TERM/I/instant\\_messaging.html](http://www.webopedia.com/TERM/I/instant_messaging.html).
- [2] Leuf, B. and W. Cunningham. *What is Wiki?* 2002 [cited 19 July 2006]; Available from: <http://wiki.org/wiki.cgi?WhatIsWiki>.
- [3] Pilgrim, M. *What is RSS*. 18 December 2002 [cited 19 July 2006]; Available from: <http://www.xml.com/pub/a/2002/12/18/dive-into-xml.html>.



- [4] Associated Press. *Blogging goes mainstream – Success of Web journals heralds an even bigger future*. Technology 10 March 2003 [cited 19 July 2006]; Available from: <http://www.cnn.com/2003/TECH/internet/03/10/bloggers.ap/index.html>.
- [5] Sterling, B. *Blogging for Dollars*. 2006 [cited 19 July 2006]; Available from: <http://wired.com/wired/archive/14.06/posts.html?pg=7>.
- [6] Farber, D. *What's up with blogging, and why should you care?* Tech Update: Web Technology 22 February 2004 [cited 19 July 2006]; Available from: [http://techupdate.zdnet.com/techupdate/stories/main/What\\_is\\_up\\_with\\_blogging.html](http://techupdate.zdnet.com/techupdate/stories/main/What_is_up_with_blogging.html).
- [7] Erbschlof, M., *Trojans, Worms, and Spyware: A computer security professional's guide to malicious code*. 2005: Elsevier. 212.
- [8] Kang, M.-C., *Trends and Developments in Malicious Software*, in *Cybercrime Prevention and Digital Forensics: Report of the International Workshop*. 2005, Asian Development Bank Institute and Microsoft Corporation: Bangkok. p. 7-9.
- [9] McMillan, R. *Researcher posts Google-based malware – 'Malware Search' tool uses engine to find known viruses and worms*. 18 July 2006 [cited 20 July 2006]; Available from: [http://www.infoworld.com/article/06/07/18/HNgooglemalware\\_1.html](http://www.infoworld.com/article/06/07/18/HNgooglemalware_1.html).
- [10] OECD. *The OECD Anti-Spam Toolkit*. 12 June 2006 [cited 19 July 2006]; Available from: <http://www.safeinternet.org/ww/en/pub/insafe/news/articles/0606/oecd.htm>.
- [11] Roberts, P. *Companies team to reel in 'phishing'*. InfoWorld 16 June 2004 [cited 19 July 2006]; Available from: [http://www.infoworld.com/article/04/06/16/HNphishing\\_1.html](http://www.infoworld.com/article/04/06/16/HNphishing_1.html).
- [12] Mitnick, K. and W.L. Simon, *The Art of Intrusion – The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers*. 2005: Wiley Publishing, Inc. 270.
- [13] Mitnick, K., W.L. Simon, and S. Wozniak, *The Art of Deception – Controlling the Human Element of Security*. 2002: Wiley Publishing, Inc.
- [14] Delio, M. *Hactivism and How it Got Here*. Wired News 14 July 2004 [cited 19 July 2006]; Available from: <http://www.wired.com/news/infostructure/0,1377,64193,00.html>.
- [15] Ernst & Young, *Global Information Security Survey 2005: Report on the Widening Gap*. 2005, Technology and Security Risk Services, Ernst & Young LLP. p. 26.
- [16] ITU-T Study Group 17, *New WTSA-04 Resolutions 50, 51, and 52*, in *Temporary Document*. 2004, International Telecommunication Union.

- [17] ISO/TMB, *Final Report of ISO Advisory Group on Security*. 2005, ISO Technical Management Board Advisory Group on Security. p. 42.
- [18] Kang, M.-C., *Benefits, Pitfalls, and Applications of IT Security Standards*. Handbook of National IT Security Standards, 1999. 1(1): p. 72-77.

