A RISK MANAGEMENT APPROACH TO INFORMATION SOCIETY

Chatzipoulidis Aristeidis, Belidis Athanasios, and
Kargidis Theodoros
Alexander Technological Educational Institute of Thessaloniki
Greece

Abstract

The most obvious features of information society are the emergence of social networks and the ever-increasing influence of Internet. While few can doubt the usefulness of this channel, such as e-commerce, there has been severe criticism about fears and beliefs that abound in illegal contents, such as pornographic and paedophile material, that stir up violence and provoke addiction. This paper conceives information society as an information security management system (ISMS) under a risk management prism. Aim is to increase the safety of individuals in respect to communication privacy, improve public administration and regulate unethical situations.

Introduction

Recently there has been a greater focus on the term “information society” due to the increasing reliance and transmittance of information in every sphere and sub-system of the society including among others culture, education, healthcare, and governance (Pinter, 2008). Challenges such as the increasing cyber crime, the function of culture in the cyberspace, the role of electronic government, and the effectiveness of information society law justify the arguments this paper presents. First we briefly introduce the synthesis of this paper. In the next section we focus on the origins of information society with special regards to the Internet. Then we present first information society as an information security management system (ISMS) to describe the as is environment and then we propose a to be environment with distinct risk management phases. The section following describes the risk identification phase by providing a short review about the impact of technology on society. Then the paper describes the risk analysis phase; the risk evaluation phase distinguishing between ethics, codes of conduct and morality; the security requirements based on Security Content Automation Protocol (SCAP); and the risk treatment phase referring to the concept of information society law. Finally, we conclude by summarizing the findings of this paper and proposing future work.

Origins of the Information Society

In this paper we define "information society" as a concept term which indicates a certain quality attribute of a society in its reliance on information transmittance (Pinter, 2008). In order to make this concept less ambiguous we describe each term separately. In particular, "information" indicates a certain aspect in which society communicates, exists and expresses itself. The transformation of raw data, personal experience and learning into information necessitates the element of knowledge and presents new set of challenges for humans (Yani-de-Soriano & Slater, 2009). Buckland (1991) categorizes the inter-related nature of information into entity oriented such as information-as-knowledge (subjective know-how) and information-as-thing (recorded knowledge), as well as into process oriented such as information-as-process (becoming informed) and information-processing (data and document processing).

The complementary term "society," according to the *Collins Dictionary of Sociology*, is defined as either the totality of human relationships or any other human group that holds its own institutions and culture. Therefore the combined meaning of terms concludes that without information flow there is no society and assuming that social interaction makes up for information flow, the terms are highly interrelated. Information society has a close relationship with the term network society (Castells, 2004). The latter is a "society whose social structure is made of networks powered by microelectronics-based information and communication technologies."

The foundations of information society lie on the influence of technology to society and thus this term is often used correspondingly with the term network society (Christakis & Fowler, 2009). This kind of society has resulted in significant changes in culture, governance, economy and personal life, determined by the concept of Information Technology (IT). A first-class technological instrument this society uses to exist and communicate through networks is without doubt the Internet. On one hand, this channel improves communication, enables instant exchange of vast amounts of information and offers services and products at low cost (e.g., e-commerce). On the other hand, this medium, as with any other technological innovation, has a number of considerations. Such include the potential theft of personal information, the potential to upload or download illegal material which can alter normal behavior while other misconceptions include the question of reliability, authenticity, data smog and the appearance of extremes (such as unnatural inclinations, e.g., drug abuse).

Information Society as an ISMS

The "as is" Environment

The concept of the information society has caused heated debate because to some it occurs as the development of a caring and professional society and to some others as a restrictive citizenship and misleading propaganda (Pinter, 2008). Nonetheless, it is a highly interactive environment where cross-cultural variability interacts instantly which in turn requires formal documentation and policies. In this section we describe information society as an information security management system (ISMS).

An ISMS is a system requiring management to deal with information security risk exposures (ISO/IEC 27001). In this regard, there must be an understanding of a) what assets are at stake, b) what resources are being used, c) who could attack these resources, and d) the mode of such attacks. Thus, the primary concern of risk management is directly related to the controls and procedures implemented to protect sensitive information, maintain the integrity, confidentiality and availability of information as well as the safety of individuals.

The "as is" environment of an information society can be described as a complete PDCA (Plan-Do-Check-Act) process, also known as a Deming cycle. In this process establishing the context, performing a risk assessment, developing risk treatment plan and defining risk acceptance criteria are part of the "plan" phase. The risk acceptance criteria may differ regarded to what is an acceptable level of risk (ISO/IEC 27001) however in case we specify such criteria in the risk identification phase. In the "do" phase, actions and controls to minimize risk to an acceptable level are identified and evaluated for efficiency according to the risk treatment plan. In the "check" phase, there is continual monitoring and reviewing of risks in the light of incidents and changes. In the "act" phase monitoring actions are performed and risk communication. The next table summarizes the information security risk management activities relevant to the four phases of the ISMS process to reflect the "as is" environment of information society.

Table 1: The "as is" Environment based on a PDCA Cycle

ISMS Process	Information Security Risk Management Process
Plan	• Scope and boundaries • Risk assessment • Risk treatment planning • Risk acceptance criteria
Do	• Implementation of risk treatment plan
Check	• Monitoring and reviewing of risks
Act	• Maintain and improve the Information Security Risk Management Process

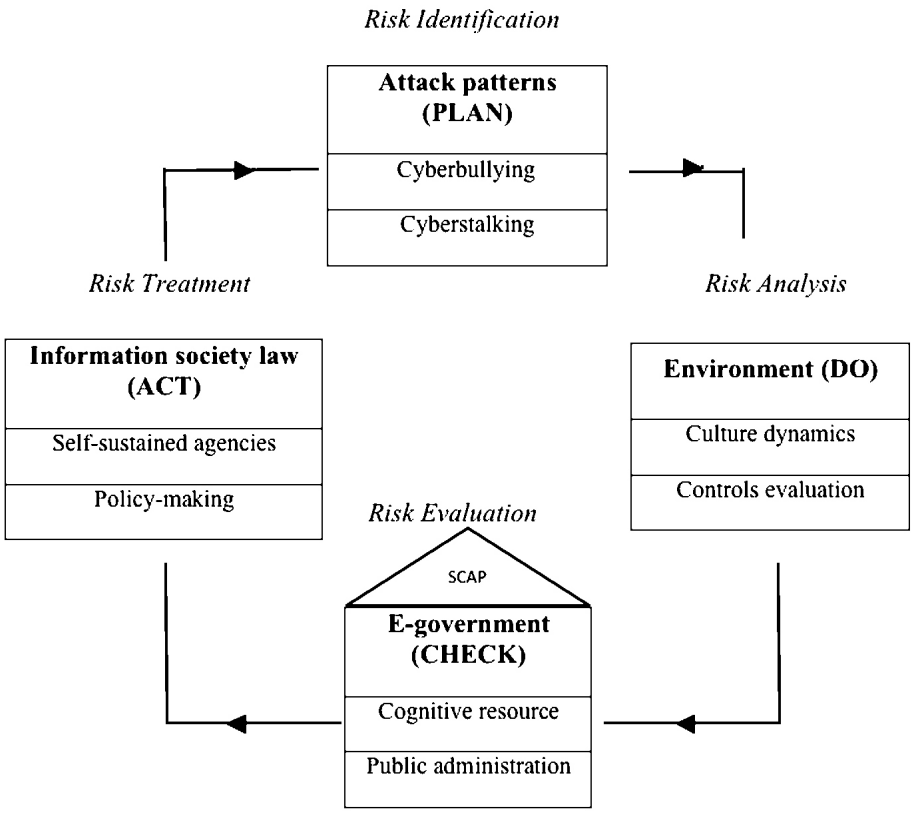
Source: ISO/IEC 27001 (2005)

Based on this process we transform the "as is" environment into a proposed "to be" environment with risk management phases under ISO/IEC 27005 standard. The purpose is to build an ideal risk management framework referring to information society security.

The "to be" Environment

The proposed "to be" environment aims to identify system vulnerabilities, analyze system environment, evaluate and prioritize most critical risks, and treat unethical situations.

Figure 1: The Proposed "to be" Environment



Source: ISO 27005:2008

More specifically, we identify and summarize potential risk elements (vulnerabilities, exposures) under two main specific attack patterns, i.e., cyber bullying and cyber stalking. These two broad terms contain most of the illegal activities involved in the cyberspace that deliberately harm minors and others respectively. To combat such attack patterns we analyze on the nature of cyber-culture and on existing controls, settings and policies. This analysis will provide input for the risk evaluation phase where identified relevant incident scenarios, including threats, exploited vulnerabilities and exposures will be assessed. Central to this phase is the role of e-government. E-government is both an under

developed and under managed area with the potential not only to act as medium for public e-services but also to act as valuable cognitive resource and tool of accountability for the policymakers (Sorrentino et al., 2009).

Finally, in the risk treatment phase, we describe how the information society law can be enforced more efficiently. This framework can provide community involvement and continuous feedback when new attack patterns arise under the premise of the Security Content Automation Protocol (NIST, 2009). This protocol is a synthesis of interoperable standards with a threefold aim: automated vulnerability management, standardized reporting and policy compliance evaluation with NIST regulatory activities such as FISMA (Federal Information Security Management Act). This protocol constitutes the principles and security requirements of the proposed "to be" environment.

Risk Identification

Input: All information relevant to the context of the system.

Guidance: The context involves specification of risk acceptance criteria necessary for information security risk management and establishment of security requirements for the system. In this phase, we find, list and characterize elements of risk such as threats, vulnerabilities and exposures. Risk acceptance criteria correspond to "criteria accepting risks and identify the acceptable level of risk" (ISO/IEC 27001). While general descriptions exist such as business criteria, legal and regulatory aspects, operations, technology, finance, and social and humanitarian aspects we set up specific risk acceptance criteria that can satisfy Policy compliance with NIST SP 800-53 Rev.1 controls, freedom of speech, and safety of individuals.

For simplicity, we summarize critical threats which involve illegal contents, such as pornographic and paedophile material and other threats (e.g., drug abuse) into two main attack patterns namely cyber bullying and cyber stalking. These terms refer to certain types of attacks with a high intention to abuse and exploit human weaknesses. The term cyber bullying refers to assaulting behavior against minor Internet users (Bauman, 2007) and can be divided as follows: sycophantic defamation, assaulting and abusive messages, menace against life, and social exclusion from online communication networks. Another definition of cyber bullying is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones (O'Connell, 2003). In general, two kinds of cyber bullying exist namely: direct attacks (e.g., messages sent to minors directly) and cyber bullying by proxy which is considered more dangerous (e.g., using others to help cyber bully the victim, either with or without the accomplice's knowledge).

Once adults become involved this is called cyber stalking. Cyber stalking is another word for cyber harassment and is when adults are attempting to lure other adults or children into offline meetings, possible for sexual exploitation. Usually, users take advantage of the anonymity that Internet-based communication provides and reveal assaulting defamation against other users. Especially minor victims of this kind of malicious actions do not possess the maturity or experience to bypass consequent effects like depression or self-exclusion from social activities (O'Connell, 2003). Indeed, there is a strong connection between cyber bullying and cyber stalking attacks. Cyber bullying is often accused for exceeding authority guidelines and violating the child's right to express.

Output: A list of risk elements.

Risk Analysis

Input: Risk identification output.

Guidance: In this phase we analyze in terms of cultural dynamics and also identify existing and planned controls. This analysis should help configure the IT platforms used, current security settings and policies.

According to Linton (1945, p. 21) culture is the "configuration of learned behavior and results of behavior whose component elements are shared and transmitted by the members of a particular society." On this basis, culture is not directly equated with one particular society such as an information society. It can, however, equate with the sum of activities shared by a particular group of people. Thus, individuals may share different cultures with several different groups for a particular cultural situation that is 'operational.' The term operational here describes a culture that is shared by a group of people who must communicate and cooperate on a task or an activity. This concept of operational culture finds strong application in information society since the individual can choose the culture in which to interact with. This further implies that the individual has the responsibility to share and transmit a considerable degree of standard behavior to other people (Castells, 2004).

Culture can also be seen as a "collective programming of the mind that distinguishes the members of one group from another" (Hofstede, 1991). To this extent culture is impossible to stand perfectly still except in the case of primitive societies which are located in remote places and are subject to exterior interference. In the case of information society, where culture is forgotten in the sense that we cease to be conscious of its existence as learned behavior, cultural assumptions in three major areas — time, space and the concept of self and others — shape attitudes towards action.

Therefore the concern is how we can control and educate potential victims in avoiding malicious attacks. One possible answer can be found on creating a cognitive resource (e.g., e-government) capable to set specific codes of conduct online. Another potential answer is a direct imposition of law. Both approaches are described in following sections. Another possible answer can be found on the impact of technology to society and the prevailing values which can be described generally in the technophile or technophobe approaches. Both terms are used in sociology to describe either a positive or a negative behavior respectively towards the interaction of technology to society (Pinter, 2008).

In addition, the diffusion of innovation theory (Rogers, 1995) complements the previous by supporting that information society has a great dependency on technological innovations. Innovation has a broader meaning of a new or significantly improved series of products or services, marketing or organizational method or external relations. The main characteristic an innovation possesses is that it surpasses static processes in order to reach a financial value and this may lead to opportunities as well as threats.

Output: A list of existing and planned controls, settings and policies, their configuration and usage status.

Risk Evaluation

Input: Risk analysis output.

Guidance: In this phase, we collect the identification of attack patterns, risk elements and the configuration data analysis to evaluate and prioritize most critical risks in order to propose a revised policy-making process.

For risk evaluation criteria we consider a) the strategic value of the information process; b) the criticality of the information assets involved; c) legal and regulatory requirements; d) maintain availability, confidentiality and integrity of information; and e) satisfy humanitarian factors such as safety of individuals and freedom of speech (ISO/IEC 27005; NIST, 2010).

It is common sense that any loss of control due to risks (e.g., cyber bullying) can seriously affect not only a single individual but even groups of social networks (Christakis & Fowler, 2009). A sound example includes Facebook, Twitter and other social networks. These utilities gather daily a vast amount of connected social groups where communication and other activities take place. Like in physical society, such networks build their own codes of conduct, ethics and morals. Because these terms are highly inter-related we clearly define each meaning.

Codes of conduct are collection of rules and policy statements intended to govern the conduct of a member of a given profession (Wines, 2006). In an information society, codes of conduct aim to clarify what type of behavior is accepted and what is of the best interest for the members of a society. To preserve codes of conduct, information ethics and set high standards of morals, the concept of government is tested. In the physical environment, the term government can be defined as the act or process of controlling policymaking in a political unit or agency. In Internet, the role of government is becoming even more important since it has to consider a cyber world without borders where malevolent activities can occur from an unknown identity (Christakis & Fowler, 2009). Frequently, e-government is used interchangeably with the term e-governance. While the two terms overlap in goals, e-government can be viewed as a subset of e-governance and its focus is to improve administration, service delivery and government finances. E-governance is defined as the process of enabling transactions between concerned groups and the government through multiple channels by linking all transaction points to improve the efficiency and transparency of government (Bhatnagar, 2004).

E-government applications have emerged rapidly due to the development of social networks and increasing demand in customer services. In general, three factors shape the effectiveness of e-government; willingness to reform, availability of information communication technology infrastructure (ICT) and the institutional capacity to absorb and manage change (Bhatnagar, 2004). E-government can act as a *cognitive resource* and a *monitoring authority* (Christakis & Fowler, 2009) in a network society. A security-based protocol (NIST, 2011) can help e-government achieve stronger authority in the network society. E-government can surpass the role of a static public administration medium and become a dynamic, reference tool for the policy-makers.

Output: A list of risks prioritized in relation to incident scenarios that lead to those risks.

Security Requirements

For security requirements we identify the exact specifications of SCAP, i.e., automated vulnerability management, standardized reporting, and conformity with the NIST Validation program. We use SCAP components because it integrates information into an automated flow within its components. In addition, SCAP components (Table 2) aim at making security more measurable and comply with NIST federal security requirements (NIST, 2011). SCAP is usually being used to enable enterprise reporting within the US Federal Government but in this case we describe how SCAP can be used as a e-government tool to generate stronger data control over a network society.

Table 2: Security Content Application Protocol Components

SCAP Components
• Vulnerabilities (CVE)
• Configurations (CCE)
• Platforms (CPE)
• Vulnerability Scoring System (CVSS)
• Checklist Language (XCCDF)
• Assessment Language (OVAL)

(Source: NIST, 2009)

More specifically,

CVE (Common Vulnerabilities and Exposures) — Risk Identification

CVE (2011) is a dictionary list of information security vulnerabilities and exposures. This standard defines "vulnerability" as a condition in a system that allows an attacker to a) execute commands as another user, b) access restricted data, c) pose as a different entity, and d) conduct a denial-of-service. For instance a vulnerability can be a) remote command execution as root, b) world-writeable password file (modification of critical data), or c) default password (remote command execution) and others. For CVE, an "exposure" is an error in software or a pattern problem that it can permit an attack to a system or a network. For example, an exposure can allow an attacker conduct information gathering and hide activities, compromise capabilities and others. Examples of exposures include improper settings for an operating system (e.g., Windows) and protocols that are usually common attack points (e.g., WAN, LAN). Every publicly known information security vulnerability or exposure has a unique identification code which includes the following characteristics:

- CVE Identifier numerical figure (e.g., CVE-1333-1234),
- status description (e.g., default password),
- short analysis (e.g., remote command execution, sexual exploitation in progress), and
- relevant references (e.g., OVAL-ID).

CCE (Common Configuration Enumeration) — Risk Identification

Similar to the CVE effort, CCE (2011) is a complementary standard with an aim to automate the management of vulnerabilities and also provide conformity with policies such as federal information technology security requirements (e.g., NIST). To succeed in this, CCE assigns a unique identifier with an associated "configuration guidance statement" and "configuration control." The first specifies required settings or policies for the computer system under testing, e.g., the required permissions for the directory System32\Setup should be assigned to

the "Administrator account" only. A configuration control describes a control unit referring to the conceptual security model of a computer system such as the access permissions for files and directories, such as System32\Setup in Win32 Libraries. Each entry contains the following five attributes:

- CCE Identifier numerical figure (e.g., CCE-5678-122),
- short status description of the configuration issue (e.g., operating system),
- theoretical parameters of the tested system (e.g., time, space, specification, and settings),
- viable technical solutions to a given configuration issue (e.g., download a security update), and
- relevant references (e.g., OVAL-ID)

CPE (Common Platform Enumeration) — Risk Analysis

A method of naming software (e.g., vendor, title, version). Aim is to foster automation towards identification of the IT platforms to which a vulnerability or element of guidance applies. CPE uniform naming specification encourages community members generate names for new IT platforms in a consistent and formal manner. A CPE Name is a unique collection of components (URI scheme name) given to a specific platform type that is made up of hardware, applications, an operating system, and other possible parts, e.g., cpe://microsoft:windows:2000

CVSS (Common Vulnerability Scoring System) — Risk Evaluation Phase

CVSS (2007) is a universal open and standardized method for vulnerability scoring. CVSS uses multiple fields for evaluating the overall risk of an individual vulnerability. Two common uses of CVSS are prioritization of vulnerability remediation activities and in calculating the severity of vulnerabilities discovered on a system. Metrics used to score and prioritize a vulnerability are Base Score Metrics (inherent characteristics of the vulnerability); Exploitability Metrics (related exploit range, attack complexity, and level of authentication needed); Impact Metrics (confidentiality, integrity, availability and impact value weighting); Environmental Metrics (effect of a vulnerability on the system environment); and Temporal Metrics (elements about the vulnerability that change over time, e.g., availability of exploit, type of fix available and level of vulnerability verification).

XCCDF (eXtensible Configuration Checklist Description Format) — Risk Evaluation, Risk Treatment Phase

XCCDF is a selection of documents or checklists for automated policy compliance. XCCDF uses an XML specification language to provide compliance with recommendations for minimum security controls under NIST guidelines. This method describes a process for measuring system configuration to a specified document or checklist. Audience of the XCCDF specification is primary *government* and secondary industry security analysts and product developers. The

use of XCCDF is mainly technical security checklists which with high security expertise can reduce the vulnerability exposure of a system. Specifically, XCCDF goals are to a) generate documentation, b) express policy-aware configuration rules, c) support complex systems that may require complex rules, d) support compliance scoring, and e) support customization. In addition, XCCDF can perform as a vulnerability scanner and when a new vulnerability is found to distill English (or other language) text into machine-readable XML/XCCDF files. XCCDF can foster the generation of readable documents for the general public (e.g., pdf files, html pages) to communicate the results of checklists evaluation.

OVAL (Open Vulnerability and Assessment Language) — Risk Evaluation Phase

A method for performing structured tests for reporting purposes. OVAL supports, homogenizes and transfers the communication of security content across the whole system. OVAL actual use is similar to a common risk assessment process, namely: identify and collect configuration data (OVAL System Characteristics); analyze a "specified machine state" such as a vulnerability (OVAL Definition schema); and document and report the final results about the state of a system (OVAL Results schema). OVAL uses a language (in XML format) for storing system configuration information in local systems. Configuration information includes installed software settings, OS parameters, and security relevant configuration values. The purpose of OVAL is to create and update a database of system characteristics against OVAL definitions so as to evaluate a system for a specified machine state. OVAL definitions are posted under a unique identifier (OVAL-ID).

SCAP Role Summary: a) To identify the context of the system, existing and new risk elements (vulnerabilities and exposures) in automated fashion and constantly update the candidate list; b) to analyze and configure the data from the IT platforms used based on cultural dynamics and existing controls (policies and settings); c) to score and prioritize risk elements; d) facilitate community involvement via an enhanced role of e-government as a cognitive resource; and e) to insure compliance with NIST 800-53 controls. This integration of efforts can help standardize a highly complex environment and provide real-time risk management.

Risk Treatment

Input: Risk evaluation output

Guidance: In this phase we discuss the legal environment of information society giving emphasis on the law enforcement for risk exposing events naming cyber bullying and cyber stalking. We do not get into specific legal details such as directives from the European Union because this may be another type of research.

The action here is to reduce risks to an acceptable level through the selection of controls.

While there many types of controls (e.g., corrective, detective, preventive, etc.) we put emphasis on legal controls. The legal regulation of information society, also known as the information society law, can be grouped according to the system of law (Pinter, 2008). Online risks, such as cyber bullying, can be addressed under civil or criminal law (Hiller & Cohen, 2002). We acknowledge legislation already exists towards cyber bullying and cyber stalking yet effectiveness is a matter of doubt. This is because the existing approaches do not control adequately cyber bullying and cyber stalking activities because they focus on the measures after attack happening and not before. Therefore, focus is to create entities and procedures that can control such risks before actual initialization.

The main concern of regulation is how to maintain stability and provide an adequate level of protection using rules or restrictions. In this regard, there are two viable methods of regulation: *ex-ante* and the *ex-post* regulation (Pinter, 2008). The ex-ante regulation refers to an 'advance' regulation where the precaution measures are most important whereas, on the other hand, the ex-post regulation provides regulation metrics after the completion of related processes. Having in mind that precaution measures are more important than the 'cure' itself (the treatment of any disease) we encourage the development of self-sustained and self-regulated agencies at a local level. By self-regulated we mean the series of rules or laws a society possess and impose to its participants, in an attempt to regulate itself before legislators enforce their demands (Vohs & Baumeister, 2010). This notion is characterized with flexible, non-bureaucratic rules in the dynamic transnational electronic environment. An example could be self-sustained, private agencies in social network utilities (e.g., Facebook). Such agencies can be created by certain criteria (e.g., business status, birth, etc.) in order to communicate and give feedback to e-government.

Output: Revised policy-making plus ongoing monitoring and reviewing of the information security risk management process.

Conclusions

This paper describes the concept of information society as a highly interactive Information Security Management System (ISMS). In this regard, we developed a concept risk management approach based on an existing "as is" environment and we proposed a "to be" environment as an 'ideal' framework to manage information society. To define the security requirements we used the exact specifications from the Security Content Automated Protocol (SCAP). SCAP purposes include standardizing reporting of system security management by supporting the use of standard expressions of security content.

The proposed "to be" environment identified critical risks involved in illegal contents into two main categories namely cyber bullying and cyber stalking. It further analyzed the impact of technology to society to configure existing settings, policies, IT platforms referring to the cross-cultural environment of information society. This analysis should provide inputs for evaluation for e-government in order to generate stronger data security. In this regard, the e-government concept can operate not only as a medium to public administration but also as a cognitive resource for policy makers. Finally as the importance of information and personal privacy is continually on the increase we recommend the creation of private, self-regulated and self-sustained agencies which can act as pre-regulation authorities in a network information society system. This process encourages community participation and personal contribution towards a safer information society. Future work will focus on system interdependencies in order to calculate the impact of attack holistically.

References

Bakopoulos, B., & Walker, R. (2005). Conversations in the dark: How young people manage chatroom relationships. *First Monday, 10*(4). Retrieved March 30, 2011, from http://firstmonday.org/issues/issue10_4/walker/index.html/

Bauman, S. (2007). *Cyber bullying: A virtual menace.* National Coalition Against Bullying. Retrieved March 30, 2011, from www.ncab.org.au/Assets/Files/Bauman,%20S.%20Cyberbullying.pdf/

Bhatnagar, S. (2004). *E-government: From vision to implementation.* Sage Publications, pp. 17–56.

Buckland, M. (1991). Information as thing. *Journal of the American Society for Information Science, 42*(5), 351–360.

Buttner, A. (2009). *Common Platform Enumeration (CPE) — Specification Version 2.2, National Security Agency.* Retrieved March 30, 2011, from http://cpe.mitre.org/files/cpe-specification_2.2.pdf/

Castells, M. (2004). *Informationalism, networks, and the network society: A theoretical blueprinting.* Retrieved March 30, 2011, from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.114.1795./

CCE. (2011). *Common configuration enumeration.* Retrieved March 30, 2011, from http://cce.mitre.org/about/index.html/

Christakis, N. A., & Fowler, J. H. (2009). *Connected: The surprising power of our social networks and how they shape our lives.* Little, Brown and Company.

CPE Specification, Version 2.2 — March 2009. Retrieved March 30, 2011, from http://cpe.mitre.org/files/cpe-specification_2.2.pdf/

CVE. (2011). *Common vulnerability and exposures.* Retrieved March 30, 2011, from http://cve.mitre.org/

CVSS. (2011). *Complete guide to the Common Vulnerability Scoring System Version 2.0, June 2007.* Retrieved March 30, 2011, from http://www.first.org/cvss/cvss-guide.pdf /

Hiller, J., & Cohen, R. (2002). *Internet law and policy.* Upper Saddle River, NJ: Prentice Hall.

Hofstede, G. (1991). *Cultures and organizations: Software of the mind.* London: McGraw-Hill.

Hughes, T. P. (1987). The evolution of large technological systems. In E. B. Wiebe, T. P. Hughes, & T. J. Pinch (Eds.), *The social construction of technical systems: New directions in the sociology and history of technology* (pp. 51–83). Cambridge, MA: MIT Press.

International Standard ISO 27001. (2005). *Information technology — Security techniques — Information security management systems — Requirements, Ref. No. ISO/IEC 27001:2005.*

International Standard ISO 27005. (2008). *Information technology — Security techniques — Information security risk management, Ref. No. ISO/IEC 27005:2008* (1st ed.).

Kabakci, I., & Odabasi, H. F. (2004). Using the technology and being a technorealist. *Anadolu University Journal of Social Sciences, 4*(1), 19–28.

Law, J. (1992). Notes on the theory of actor-network: Ordering, strategy and heterogeneity. *Systems Practice, 5,* 379–393.

Linton, R. (1945). *The cultural background of personality.* New York: Appleton-Century.

National Institute of Standards and Technology Special Publication 800-126 Rev. 1, "The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1." (2011, February). Retrieved March 30, 2011, from http://csrc.nist.gov/publications/nistpubs/800-126-rev1/SP800-126r1.pdf/

National Institute of Standards and Technology Special Publication 800-53 Rev.1 controls, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans." (2010, June). Retrieved March 30, 2011, from http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf/

National Institute of Standards and Technology Special Publication 800-117 (Draft), Guide to Adopting and Using the Security Content Automation Protocol (SCAP). (2009, May). Retrieved March 30, 2011, from http://csrc.nist.gov/publications/nistpubs/800-117/sp800-117.pdf/

O'Connell, R. (2003). *A typology of child cyber sexploitation and online grooming practices.* Cyberspace Research Unit, University of Central Lancashire (UK). Retrieved March 30, 2011, from http://image.guardian.co.uk/sys-files/Society/documents/2003/07/24/Netpaedoreport.pdf/

OVAL. (2011). *Open vulnerability and assessment language.* Retrieved March 30, 2011, from http://oval.mitre.org/

Pinter, R. (2008). *Information Society: From theory to political practice, Coursebook.*

Rogers, E. M. (1995). *Diffusion of innovations* (4th ed.). New York: Free Press. Retrieved March 30, 2011, from http://www.maurice-anemaat.nl/uni/Scriptie/ARTIKEL_ROGERS_DIFFUSIONINNOVATIONS.pdf/

Sorrentino, M., Naggi, R., & Agostini, L. P. (2009). E-government implementation evaluation: Opening the black box. *Lecture Notes in Computer Science, 5693,* 127–138.

Vohs, K. D., & Baumeister, R. F. (2010). *Handbook of self-regulation: Research, theory, and applications* (2nd ed.) (pp. 390–422). Guilford Press.

Wines, W. A. (2006). *Ethics, law and business* (pp. 5–65). Lawrence Erlbaum Associates.

XCCDF. (2006). *eXtensible Configuration Checklist Description Format, NIST Interagency Report 7275 Revision 1.* Retrieved March 30, 2011, from http://nvd.nist.gov/scap/xccdf/docs/xccdf-spec-1.1.2-20060913.pdf/

Yani-de-Soriano, M., & Slater, S. (2009). Revisiting Drucker's theory: Has consumerism led to the overuse of marketing? *Journal of Management History, 15*(4), 452–466.