An Holistic View of Information Security: A Proposed Framework

Kay Fielden
Unitec Institute of Technology, New Zealand

Abstract

This discussion paper focuses on an holistic framework proposed that includes the following clusters of ideas: purpose and role of information security, societal trends, human elements, changing technologies, information security management, and complexity and interactions. These multiple views of information security provide a more complete framework in which to embed much of the global research in information security. Future directions and possible research projects are considered that would apply this holistic framework to what is considered to be a 'difficult' problem to solve.

1. Introduction

A broad, non-technical view is adopted in which an information security framework is proposed. Cyber security is a complex, ever-evolving problem space, and a broad, holistic overview is one way to provide a framework in which to situate research in this domain. Present security dilemmas include: the porous nature of information security as propriety software is continually upgraded; the proliferation in malware and the sophistication of malware production and management; walled internet communities and mistrust between and among such communities; and the reactive nature of cyber security protection.

The original designer of the internet [1] describes current internet problems as 'tussle'. Tussle is used to describe the ongoing contention among parties with conflicting interests and Clark believes that the Internet is shaped by controlled tussle in which there are no final outcomes of tussle interactions, no stable point, and no acquiescence to a static architectural model. Clark suggests that redesigning the internet needs to be designed to allow for variations in outcome that will flex and survive under pressure (because rigid designs will be broken). He also suggests that design should be modularised along tussle boundaries, so that one tussle does not spill over and distort unrelated issues. Clark states that for future applications improving end-user trust can be improved explicitly by employing third party agents to mediate an interaction.

The structure of this paper is as follows: the proposed information security framework based on findings from relevant information security literature is defined; possible research projects are considered that can be situated within this framework; and implications for future research are discussed.

2. Literature Review

In order to create this holistic information security framework to accommodate the changing nature of the internet, a diverse, multidisciplinary literature base has been consulted. Only partial framework elements at a non-technical level have been identified such as governance [2], security standards [3], security architecture [4], legal requirements [5], user issues [6], and information security management [7]. The framework presented in this paper addresses this gap in the literature.

A selection of partial non-technical information security frameworks is considered below. A socio-technical view of information security management is proposed by [2] in which information security is classified as 'an entangled research challenge'. Another theoretical approach is that a set of metrics be developed to measure an organization's security policy [3]. External and internal influences on information security are considered by [4] whilst [5] adopt the view that for information security to be successful, end-user behavior needs to be studied (at the individual as well as the organizational level).

3. Analysis of Findings

The factors that determine the information security framework within this paper are classified under six clusters: purpose and role of information security, societal trends, human elements, interaction and complexity, information security management and changing technologies.

3.1. Purpose and Role of Information security

As the internet has outgrown its original purpose and role so has the purpose and role of information security.

3.1.1. Economic Protection

Economic protection is required globally, nationally, governmentally, across and between nation boundaries, commercially, educationally and individually. Economic protection is often viewed differently from one country to the next and Clark's 'tussle space' has a wider variety of economic considerations that for most researchers have been viewed as 'hard problems' [1]. For all stakeholders in consumer-driven economies, information security is paramount in maintaining economic viability.

Economic protection is also required for privacy reasons. A secure internet provides opportunities for wealth based on secure information. With the current state of cyber security [6] (Pfleeger and Rue) suggest that information security requirements need to compete with other software development costs. These authors believe that software-development project managers need to know what the likelihood of an attack is and what the likely consequences are. The OECD [7] state that protecting the internet is a public policy priority fundamental to the global economy.

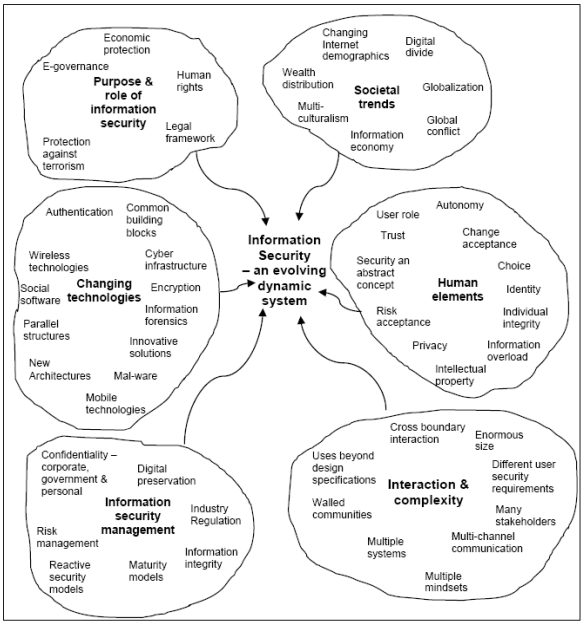

Figure 1. Information Security Framework

3.1.2. E-governance

Information security and privacy are major issues for e-government technologies [8, 9]. Cyber-security is now an international security problem. When a nation: (i) has been sensitized to security and terrorism problems; and (ii) has individual privacy and civil liberty enshrined in its culture, there is a strongly felt need for a comprehensive national cyber-security strategy that embraces both intelligence and law enforcement.

The term "techno-politics" has been coined by Rasmussen to suggest that it is not possible to make clear distinctions between technology and politics particularly with respect to information security [10].

3.1.3. Human Rights

One of the views proposed is that humanity needs the internet to keep operating for the common good [10]. It has also been suggested that the internet has irrevocably changed the global distribution of information [10].

Human rights issues have changed as the internet amplifies opinions and interests, accelerates and frees dissemination of information and enables faster delivery of services. This in turn means that information accuracy and integrity is even more important.

3.1.4. Legal Framework

Internet regulation takes a number of forms and the law is one regulatory element [11]. Management of electronic espionage and technological crime is seen as an urgent problem to solve [8].

3.1.5. Protection against terrorism

Terrorists of the 21st century target store strategic information, exploiting vulnerabilities in existing cyber infrastructure. "Financial terrorism" and "information terrorism" are a reality with a weakly protected global cyber infrastructure. Current international bodies (APEC, OECD, Group of 8, Council of Europe, the United Nations) struggle with the sheer size and complexity of a global cyber-security framework. Many layers of information security are required (legal, technical, political, societal) to protect national and international information infrastructure. A global dilemma is the myriad of ways in which nations protect information [11].

3.2. Societal trends

Societal trends considered in this framework (Figure 1) include: changing internet demographics, digital divide, globalization, global conflict, information economy, multiculturalism and wealth distribution.

3.2.1. Changed internet demographics

Internet usage patterns have changed dramatically with the advent of Web 2.0. It is estimated that in 2011, there will be 750 million Facebook users, 76 billion Google searches a month, the number of text messages every day will exceed the population of planet, new technical information is doubling every two years, approximately 1.5 exabytes (1.5×10^{18}) of new information was generated in 2008, and that more information was generated this century than in

the previous 5,000 years [12]. With the uptake of social networking sites, there is a much greater need for socio-technical analysis of information security and privacy issues in online communities.

3.2.2. Digital Divide

Economic issues for users in the push to e-government in the United Kingdom were explored by Cushman and Mclean (2008) who found that digital engagement brings both a cost and a responsibility shift to citizens [13].

3.2.3. Globalization

According to Leiner et al, the internet is playing a crucial role in globalization socially and economically not just technically [14]. With the rapid expansion of social networking sites, new global phenomena are emerging frequently. If the internet is viewed as a cultural creation then the demographics of a changing internet and the accompanying information security issues pose major problems.

3.2.4. Global Conflict

There were three major information security findings for the U.S [8]: (i) cyber-security is a national security problem; (ii) they believe that there is a need to protect and respect privacy and civil liberties; and (iii) only a comprehensive national strategy that embraces both the US and international aspects of cyber-security will make US more secure. A weak cyber security dilutes investment in innovation because it subsidises R&D of competitors (risk to the economy) [8]. This is part of the financial terrorism strategy of modern terrorists, who exploit vulnerabilities in a cyber infrastructure. There is a need to rethink how deterrence works in cyberspace to ensure resilience and continuity of service. Conflict symmetry is not present in cyberspace - some nations are far more reliant on the internet than other nations.

3.2.5. Information Economy

Both cost of maintaining information security and industry losses because of security breaches have soared. In 2008 it was estimated that industry losses were as high as $1 trillion [14]. In the current economic climate it has been suggested that the costs associated with cyber security need to compete with other project costs [6].

3.2.6. Multi-culturalism

Whilst most authors writing on cyber security focus on technical issues [15], there are also diverse cultural issues in the management of information security and privacy. Security issues identified include; access to information systems, secure communication, security management and development of secure information systems.

3.2.7. Wealth Distribution

The internet has offered many more people, regardless of country of origin the opportunities for wealth creation [16]. Many more opportunities for wealth creation and distribution have been created as online businesses reach global markets. With this increase has come increased security risks.

3.3. Human Elements

Human elements considered include autonomy, change acceptance, choice, identity, individual integrity, information overload, intellectual property, privacy, risk acceptance, security as an abstract concept, trust, and the role of the user.

3.3.1. Autonomy

Social networking offers users autonomy in a way that is unprecedented in computing history. No longer are users dependent on computer scientists, engineers and web designers to have a presence on the internet. Social media has allowed users to create and share content on a peer-to-peer basis.

3.3.2. Change/Risk Acceptance

Social networking sites offer a prime target to cyber-criminals as many social networkers are unaware of information security implications. The internet as a technically-dependent public information domain operates in the face of constant change. Behavioural and cognitive research is required into security technology acceptance, use and the multiplicity of choices available online. A dilemma facing online users that has been well documented is knowing the identity of a user. This is a problem particularly for parents and children.

3.3.3. User Role

Experimental evidence presented suggests that individuals acquire, use, and presumably, value information differently when it is under the threat of disappearance. This causes people to overvalue information and hence integrate the pieces of information into their decision making process that they might otherwise not have acquired. This has important consequences in the real world. Users now play a much more active role in the Web 2.0 world

3.3.4. Information Overload and Choice

It has been demonstrated that having too much information results in poorer decision-making. People used more information not necessarily because of technological and social pressures, but rather because the people themselves, out of an aversion to loss, choose to acquire and use more information. The costs associated with this approach to information acquisition and use is considerable [17].

3.3.5. Intellectual Property

IP losses (both counterfeiting and breaches of confidentiality) are common in information security breaches [18]. It has been estimated that in 2009, $560US million was lost in internet fraud in the US [12].

3.3.6. Privacy

Protecting privacy has become much more difficult with the expansion of the internet, where data is transferred and stored at little cost. Vast amounts of personal and sensitive data are available in this public domain where loss or theft is one objective for cyber criminals [7].

3.3.7. Security - an Abstract Concept

Security is often seen as an abstract concept with outcomes that cannot be perceived in any concrete form [19]. When there is no visible and immediate outcome or reward for pro-security choices, people's perceptions are that therefore there is no visible threat. West maintains that people find it difficult to evaluate pro-security behavior when a cost benefit analysis is done. West also maintains that people make quick decisions (cognitive misers) about security behavior without considering all the risks and options.

3.3.8. User Behavior

The cyber security industry have long recognized non-acceptance of security tools as a major problem in establishing secure user practices. Habitual behavior on the internet also poses a security risk, as predictable behavior patterns are more exploitable. Another human characteristic is that individuals maintain an acceptable degree of risk that is self-leveling. If a user increases information security measures, this is likely to be accompanied by increased risky behavior. People also multi-task routinely which means that no one task receives full attention at any one time. To conserve mental resources quick decisions are based on learned rules and heuristics for 'good enough' decisions. The abstract nature of information security and the non-reward basis on which cyber security operates means that there is no instant gratification. Many users are also gamblers and are more likely to gamble for a loss than accept a guaranteed loss. Cyber security is also seen as a secondary task. West suggests that user incentives such as rewarding improved security compliance with lower costs may increase the need for an immediate reward [6]. He also suggests that built in interface design to improve awareness of risk messages and alerts may help. A more radical suggestion is that security violators in the corporate world be fined for security breaches (akin to running a red light). It seems that the ideal security user experience would be none at all, if an internet infrastructure was perfectly secure and reliable. Security mechanisms may be difficult for people to understand or use. An abstract risk is often harder for people to make optimal choices about. Therefore, it often follows, that users are not adequately protected.

3.3.9. Trust

People's trust in the security of their information is often misplaced. Because the concrete benefits of security prevention are not seen until after a security breach has occurred trust remains high and often investment in information security devices remains lower than it should be [19]. In organizations this misplaced trust poses a major threat [18]. Non-acceptance of security tools is recognized as a major problem facing cyber information systems. Non-acceptance of security tools is also a major user problem [19].

3.3.10. Individual Integrity

There is also a relationship between increased IS security measures and increased risky behavior. West suggests that humans are cognitive misers, have limited information processing ability and routinely multi-task. By acting in this way it is likely to be that no one task has the user's full attention at any given time. Users form quick decisions based on learned rules and heuristics that give 'good enough' decisions 'just in time'. This, in turn has implications for individual integrity in the face of fast decision making about security issues.

3.4. Changing Technologies

In the changing technologies cluster the following factors are considered: authentication and access, common building blocks, cyber-infrastructure, encryption, information forensics, innovative solutions, malware, mobile technologies, new architectures, parallel structures, social software and wireless technologies.

3.4.1. Authentication

Access to information systems is usually controlled by some form of technical authentication whether it be software, firmware or hardware or a combination of these [15]. Most research on authentication as an information security device has focused on technical solutions [15]. The most notable contributions to the method of authentication include passwords and token-based authentication and authentication using special-purpose devices, such as smart cards. Mathematics is the reference discipline for authentication and the principles involved include confidentiality, availability, integrity and non-repudiation.

3.4.2. Common Building Blocks

In one new technology being developed, common computing building blocks are utilized to minimize security breaches [20]. Each architecture layer is constructed with common building blocks based on set theory.

3.4.3. Cyber Infrastructure

In today's information age cyber infrastructure, which is inextricably linked to global and national infrastructure requires multiple layers of cyber infrastructure protection [11]. This is because each layer is constructed in a different manner and as such provides opportunities for security breaches.

3.4.4. Encryption

Known encryption algorithms are regarded as a challenge to be circumvented by cyber criminals, thus perpetuating the need for ongoing technical development [15]. Information forensic activities include: incident response and analysis, network traffic tracing, event reconstruction, file system, memory and application analysis, data mining, digital evidence storage and preservation, data hiding and recovery and file extraction, digital law.

3.4.5. Information Forensics

Information forensics is also about compliance with information security and privacy policies, procedures and regulations [21]. The current internet has been described as a patchwork problem that has escalated in size and complexity [8], and therefore provides a difficult space to protect.

3.4.4. Innovative Solutions

The founder of the internet [1] suggests that because the internet's basic flaws are an economic drain on organizations, innovation is impeded and national and international information security is threatened. Clark suggests that it is time for clean slate solutions. The NSF has also invested in research to develop clean slate solutions. However, major players in global hardware and software organizations see such a change as a major threat to business therefore smaller innovators find it difficult to gain acceptance for their clean slate solutions.

3.4.5. Malware

It has been reported that mal-ware invasion is more likely to be from an organized cyber underworld malware as an industry [22] than the provenance of smart students. This is a notable change in the nature of cyber threats.

3.4.6. Mobile Technologies

Mobile technologies allow people to be connected anywhere/anytime. This then poses a threat as place and time data can be interconnected with internet-stored knowledge [23]. As mobile technologies expand so security needs increase.

3.4.7. New Architectures

In any new clean slate solution [24] suggests that security should be addressed at design stage, rather than as post-event activities.

3.4.8. Parallel Structures

Whilst is convenient to think about the internet as one structure, the backbone of cyber information, other possibilities exist in which parallel structures exist. With multiple stakeholders with different security requirements, this becomes a distinct possibility in which innovation could occur.

3.4.9. Social Software

The explosion in social networks has opened up yet another domain in which information security is required. Users with little technical knowledge generate their own sites without completely comprehending the implications of information security in a public domain.

3.4.10. Wireless Technologies

The 'Internet of things' has become possible, as wireless technologies allow connectivity to the internet anywhere and at anytime [23].

3.5. Information Security Management

The information security management cluster of factors in this framework (Figure 1) includes: confidentiality, digital preservation, industry,

regulation, information integrity, maturity models, reactive security models and risk management.

3.5.1. Maturity Models

A common approach to information security is to codify levels of maturity [25]. Organisations can then be measured, registered and rewarded for whatever level of maturity that is achieved. Layers of security management to protect confidentiality can be layered at corporate, government and personal levels.

3.5.2. Password Protection

Business success is predicated on customer loyalty for which information security is required [18]. The most common mechanism for protection of organizational proprietary information is by password protection.

3.5.3. Industry Regulation

Major computer industry organizations drive the direction that information security takes. Regulation has become even more imperative with the global reach of the internet [8], [7]. Whilst regulation is seen by both government and organizations alike to be essential for information security, regulation can also viewed as revenue collection.

3.5.4. Confidentiality – Corporate, Government, Individual

Not only is confidentiality important, corporate and government knowledge bases need to maintain information integrity. Infiltration of sensitive data sources to invalidate stored data is a major information security dilemma. A common approach to information security is to codify levels of maturity [25]. Organisations can then be measured registered and rewarded for whatever level of maturity that is achieved.

3.5.7. Reactive Security Models

Better measurement devices are required to assess internet security and stability [7]. Current information security software can, in general be classified as reactive. Patches are issues continuously by security software organizations to combat ever-changing malware.

3.5.8. Risk Management

Multi-layered risk management is required for all stakeholders [18] that analyses and predicts system vulnerabilities [26]. A major risk to organisations is insider threat [18].

3.6. Interaction and Complexity

In the interaction and complexity cluster of factors (Figure 1) factors considered are cross boundary interaction, size, different user security requirements, many stakeholders, multi-channel communication, multiple mindsets, multiple systems, walled communities, and uses beyond design specifications.

3.6.1. Cross Boundary Interaction

In describing the history of internet development Leiner et al suggest that the messiness of the internet is the result of a complex set of interactions between many people mediated by technology [3]. Complexity also arises because cyber communities are neither planned nor are they ‘plannable’. Not only is internet interactions complex, the many different levels of network infrastructure architecture, give rise to a large and complex cyber security problem space. Critical events [18] are also dependent on accurate and secure information. Information security conflicts across internet boundaries are inevitable and, according to Clark, is a vital and necessary part of on internet-based economy regardless of differing security requirements [1]. The OECD [7] recommend that more work be done to combat threats to security and stability at internet boundary intersections.

3.6.2. Enormous Size

Information security is also complex because of the sheer size of the internet [12]. For instance, in 2011 it has been estimated that there will be 750 million facebook users, 76 billion Google searches a month, more text messages each day than the population of planet, a doubling of new technical information every 2 years, approximately 1.5 exabytes (1.5 x 1018) (approximately) of new information generated, and more information generated than the previous 5,000 years [6].

3.6.3. Different User Security Requirements

It is also recognized that there is ‘no one security requirement for all [18]. People are both biggest asset within an organization or community and the largest contributing factor to information security risks. A more holistic approach is advocated to understand different user requirements.

3.6.4. Many Stakeholders

Internet-related policies require input and collaboration from multiple stakeholders including business, governments, civil society and technical experts [11]. An all-inclusive multi-stakeholder

approach is required to shape information security to protect the global economy [7].

3.6.5. Multi-channel Communication

Today's internet offers multi-channel communication through the 'Internet of Things". While this is regarded as an advantage in the range of connectivity provided, further information security threats are posed as it is now possible to interconnect location and time data on the internet.

3.6.6. Multiple Mindsets

It has been noted that a holistic approach to information security is required that allows for multiple mindsets, innovative design and changing uses of cyberspace [1, 9, 27].

3.6.7. Multiple Systems

It has been suggested that one way to view information security is as a "system of systems" and that employing multiple layers of appropriate defenses possible solutions can be found [28]. One three layered security architecture is proposed by [29].

3.6.8. Walled Communities

Different views have been preserved by national governments (in particular China and Iran) imposing restrictions on access to the internet for their citizens. This has been described as 'balkanizing' by [11].

3.6.9. Uses beyond Design Specifications

In exploring the history of the internet, where the internet was conceived originally as a solution to a narrowly-defined problem of time-sharing with scarce computer resources, Leiner et al believes that the internet is being used beyond its current design specification [27]. For instance, social networking has meant that users with little technical knowledge dynamically change their own sites. This in turn provides more opportunities for information security breaches.

4. Research Contribution

The holistic information security framework discussed in this paper contributes to the ongoing debate about information security and suggests that inclusion of multidisciplinary partners take place, particularly with the call by a number of authors to include various socio-technical perspectives in developing information security theories and frameworks.

5. Conclusion

Further research is required in many areas of information security. Innovative 'clean slate' technical solutions are required. While large organizations dominate information security provision there is less likelihood of smaller businesses providing the innovation required. Cross border interaction is also another area that requires global problem solving to suit the needs of multiple stakeholders. It would appear that the current complex cyber security situation requires research from many points of view. In the short history of the internet, information security has progressed from the domain of computer scientists to include politics, economics, civil society and the individual [30]. In this short paper an information security framework is proposed based on six clusters. Information security has been described as one of the hard problems facing the world. By considering multiple clusters of factors a more holistic approach has been taken that provides fertile ground for further research.

6. References

[1] Clark, D.D., et al., Tussle in cyberspace: defining tomorrow's internet. IEEE/ACM Transactions on Networking, 2005. 13(3): p. 462-475.

[2] Coles-Kemp, L., Information security management: An entangled research challenge. Information Security Technical Report, 2009. 14(4): p. 181-185.

[3] Goel, S. and I.N. Chengalur-Smith, Metrics for characterizing the form of security policies. The Journal of Strategic Information Systems, 2010. 19(4): p. 281-295.

[4] Hu, Q., P. Hart, and D. Cooke, The role of external and internal influences on information systems security - a neo-institutional perspective. The Journal of Strategic Information Systems, 2007. 16(2): p. 153-172.

[5] Rhee, H.-S., C. Kim, and Y.U. Ryu, Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 2009. 28(8): p. 816-826.

[6] Pfleeger, S. and R. Rue, Cybersecurity Economic Issues: Clearing the Path to Good Practice. IEEE Software, 2008. 25(1): p. 35-42.

[7] OECD, The future of the Internet economy. 2008.

[8] Langevin, J.R., et al., Securing cyberspace for the 44th presidency, in A Report on the CSIS Commission on Cybersecurity for the 44th

Presidency. 2008, Center for Strategic and International Studies: Washington DC.

[9] Rasmussen, T., Techno-politics, internet governance and some challenges facing the Internet, in Research Report 15. 2007, Oxfiord Internet Institute: Oxford.

[10] Wescott, N., Digital diplomacy: The impact of the Internet on International relations, in Research report 16. 2008, Oxford Internet Institute: Oxford.

[11] Zittrain, J.L. and J.G. Palfrey, Access Denied: The practice and policy of global internet filtering, in Research Report 14. 2007, Oxford Internet Institute: Oxford.

[12] Rittenhouse, G. Shaping the Future Internet: opportunities and risks. Alcatel-Lucent 2009 [cited 2009 June 10]; Available from: http://www.fi-prague.eu/program/p/rittenhouse.pdf.

[13] Cushman, M. and R. McLean, Exclusion, inclusion and the changing face of information systems research. Information Technology & People, 2008.

[14] Mcafee (2008) Security breaches.

[15] Siponen, M.T. and H. Oinas-Kukkonen, A review of information security issues and respective research contributions. The Data Base of Advances in Information Systems, 2007. 38(1): p. 60-80.

[16] Franklin, J., et al. An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants. in CCS'07. 2007.

[17] Davis, J.D. and S. Ganeshan. Aversion to loss and information overload: An experimental investigation in ICIS09. 2009. Phoenix, Arizona.

[18] Townley, A., The philsophy of enterprise information security. Information Security Bulletin, 2005. 10: p. 163-170.

[19] West, R., Thepsychology of security. Communicati ons of the ACM, 2008. 31(4): p. 34-40.

[20] An Interoperable information infrastructure (III) model in 12th Collecter Workshop on eCommerce, P. Swatman, Editor. 2004: Adelaide.

[21] Cohen, F.B. (2007) Fundamentals of digital forensic evidence.

[22] Poulsen, K., Wired reports: hacking used to be a casual affair, the province of smart college kids mostly fooling around. No More. Today's hackers mean business, in Wired. 2009.

[23] Floridi, L., A look into the future impact of ICT on our lives. The Information Society, 2007. 23: p. 59-64.

[24] Updegrove, A., Security standards and the internet: keeping the cyber barbarians behind the gates. Standards Today, 2009: p. 1-33.

[25] McElwee, S. (2009) Security process maturity: Implementing security as a set of measurable processes.

[26] Wing, J.M., Cybersecurity Research Challenges, in Cybersecurity Summit 2008: Crystal City, VA

[27] Leiner, B.M., et al (2009) State of the art report: Internet development across the decades. find details.

[28] Conklin, W.A. and G. Dietrich. Systems theory model for information security. in 41st Hawaii International Conference on Systems Sciences. 2008. Hawai.

[29] Blackwell, C. A security architecture to protect against insider threat from damage, fraud and theft. in CSIIRW'09. 2009. Oakridge, Tennessee.

[30] Zittrain, J., Law and technology; The end of the generative internet. Commnications of hte ACM, 2009. 52(1): p. 18-20.

