https://doi.org/10.48009/1_iis_2010_35-40

THE EVOLUTION AND IMPLEMENTATION OF GLOBAL ASSURANCE

Garry L. White, Texas State University – San Marcos, gw06@txstate.edu

ABSTRACT

Because of the Internet, a global economy has developed. No longer is information restricted to a central computer, in a physically locked room, and accessed only by computer professionals. Today, information is distributed outside the physical locked room and accessed by anyone, anywhere, anytime. In turn, security of the information has changed from local to global. This paper examines the development of global assurance from local computer security. The implications, such as no perimeter to protect, are then discussed. A definition of global assurance is provided. The purpose of this paper is to lay the foundation for further research in the development of global assurance, a new concept that corporations and governments must address.

Keywords: **I**nfrastructure, Security, Assurance, Global, , Information

INTRODUCTION

The field of information security has been changing over the years. And information security has been receiving increased focus, due to the escalation of cyber crimes and vulnerabilities [13, 26]. Changes in technologies have moved the business world to a global scope [19]. There has been a move from a "central" computer in a physically locked room with only computer professionals working regular business hours to "global" networking systems allowing anywhere, anytime, anyone usage. This move has resulted in many changes as to how businesses function. Today, multinational companies have developed a global information integration infrastructure that crosses national borders and time zones [29, 33]. Security is going global.

Even the term "security" is being replaced with "assurance." What are the differences between security and assurance? And what led to the development of assurance?

Security -- Protection through technology:

"Security is a system property"[34]. A system of people, processes, and technology controls are essential elements of information technology security. This includes operations security, applications development security, physical security, cryptography, hardware, communication, personnel, and software [9, 22]. Security is primarily technically oriented. The focus is the protection of the information and systems and services from accidental and deliberate threats to confidentiality, integrity and availability [9].

Stoneburner [34] listed the objectives of security as:

1. **availability** of systems and data for intended use only,
2. **integrity** of system and data,
3. **confidentiality** of data and system information
4. **accountability** to the individual level

Assurance – operational confidence of management:

Stoneburner [34] explained assurance as the confidence in the technology and system operation to adequately meet the above four security objectives. Confidence is based on analysis, validation, and verification of the technology and system. Assurance includes the

Assurance is more people focused and preparedness. There is confidence and reasons to expect quality and dependability [34]. Managers are assured that functions are working correctly. Reliable decisions can be made from the outcomes.

Along with the technology of security, assurance includes:

1. **Authentication** of users
2. **Non-repudiation** of users
3. **Confidence** in system by users
4. **Functionality** performs correctly
5. **Protect** from unintentional errors by users
6. **Resistance** to intentional by-pass

EVOLUTION

Computer Security

Computer security began with the first mainframes after World War II [39]. During these early years, the focus was on physical security and simple document classification [39]. Physical access was to a single computer mainframe in a locked room and only by selected employees [2, 22]. The data was on a single

stand-alone computer with no remote access. This insured physical integrity, confidentiality, and availability of the data, as well as individual accountability.

The focus of security was securing of the physical perimeter. Only computer professionals had physical access along with needed passwords. Only one corporate department was involved with all the information processing and storage and access. This can be summed up as one local physical perimeter of a locked room.

Information Security

With the development of networks and the Internet, information became decentralized and easily accessible. All employees, including non-computer professionals, are now able to easily access, modify, and share data/information. Other corporate departments became involved and concerned about the data/information used. Access to outsiders as well with other employees developed. Information security standards had to be developed to protect a network [20]. These standards dealt with encryption, security policies, and Internet/network restrictions. Permissions of data for users had to be implemented. Security controls of prevent, detect, and response [22] were developed to deal with these new risks and threats originating from a decentralization of data; networks and the Internet.

Along with hardware and software components, the human component now comes into play since users/employees (non-computer professionals) have access to information from computer systems. There is now a greater risk to the information due to new vulnerabilities and external, as well as internal, threats. Security policies for all employees become necessary. Security now deals with risk management and security policies [4, 38]. Information security developed into a wider range of disciplines such as statistics, legal, social, ethics, and psychology [15, 22, 28].

The perimeter to protect the confidentiality, integrity, and availability of the data moved from a local physical perimeter to a logical perimeter of a corporate information network, a tactical issue.

Information Assurance (IA)

"Unfortunately, there is no universally accepted definition of what constitutes information assurance" [10]. However, the Information Assurance Advisory Council [17] defines information assurance (IA) as: "…the certainty that the information within an organization is reliable, secure, and private. IA encompasses both the accuracy of the information and its protection, and includes disciplines such as security management, risk management and business continuity management." Another definition is the "measures that protect and defined information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation" [7].

"Information assurance includes the products, procedures, and policies that allow the timely transfer of information in an accurate and secure way among all parties involved. While the technology, procedures, and policies used to achieve this have changed over the years, the underlying goals of timeliness, accuracy, and non-repudiation have remained consistent" [21].

IA contains all the elements of information security with a goal of information protection involving processing, storage, and transmission [31]. And, like information security, IA is an interdisciplinary business curriculum [6].

IA goes beyond anti-virus, intrusion detection, firewall technology found in security systems. IA deals with reliable management decision-making, customer trust, business continuity, and good governance in all sectors of industry and public service [10]. The new major component is people; the need for awareness, training, and education [25, 31]. Through awareness, training, and education, data defense improves; for example, keeping ahead of Internet phishers [11]. This new component has lead the way for new laws and policies for users to follow. Such new policies and practices developed to ensure precautions [28] and to deal with unpredictable threats [10].

IA policies adjusted to changing internal and external environments. These operational defensive measures focused on successful performance. A holistic view of controls and procedures replaced the protection of data. By protecting the system, the data is protected. In 2002, the Sarbanes-Oxley Act stressed internal controls of information systems issues [1]. This lead to new assurance compliance for information systems [6].

With IA, the focus of security has moved from protecting data (technical issues) for business survival to protecting the system (business issues) so as to enable business success. Security has moved from the domain of the information systems

department (technical issues) to the domain of audit and compliance committees (business issue) [10]. Not only is the focus on technology, but also with operations and people as well [31].

The goal of IA goes beyond protection. It includes the confidence that information systems function correctly so management can make decisions. Human beings need security in an emotional sense, people need to feel secure [32]. Employees' work efficiency improves and customers are confident in the business.

Like information security, the perimeter is that of the corporate network. However, IA makes security a strategic issue because of the potential impact on the rest of the business [10].. By becoming part of the corporate goals, shareholder value and competitive advantage are improved [10].

Infrastructure Assurance

On September 11, 2001, the infrastructure of the business world was attacked. This resulted in the enhancement of the Federal agency Critical Infrastructure Assurance Office (CIAO). Its job is to provide tools necessary to maintain a level of control over IT systems [14]. Another agency which formed due to this attack, was the Pacific Northwest Partnership, a regional multistate civilian-defense cooperative that provides disaster action through business and government collaboration [30]. Thus, infrastructure assurance was born to defend against possible attacks against US infrastructure information systems.

No longer are security professionals drawing a line at the firewall. Instead they are taking into account the role of developers, vendors, and customers outside the firewall. Network and system borders are porous now [16]. Corporate CEO's are more aware of external components and realize their corporate interdependences with other organizations and government agencies. Greater collaborations developed due to the 9/11 attack.

These collaborations caused businesses to move away from protecting data/ information files (information assurance), to protecting operations and processes that involve external partners (infrastructure assurance). By protecting these operations and process, corporations are protecting the data just like information assurance. Managers focus on the system rather than the assets (data).

The perimeter now has expanded to protect partners, suppliers, and customers - interdependent entities outside the corporation.

Global Assurance

E-commerce has created a global community. Today, knowledge is shared in real-time, anywhere, anytime, anyone, and any language. Small businesses are now international since customers in other countries provide sales via the Internet. The Internet has shifted businesses to a global scope [19]. There has been a shift from the importance of corporate security policies to national laws of other countries. Although managers can control corporate infrastructures, they cannot control international infrastructures. Because of global access to information, security threats become more challenging due to international issues. The perimeter to protect has expanded beyond corporate control. There is no longer a perimeter to protect. Technology has outgrown corporate security measures. Security needs to catch up to technology.

Malicious code, cyber attacks, Denial of Service attacks, and spam are originating worldwide, such as Europe, Middle East, and Africa [35, 36]. In many cases, hackers are constantly relocating their operations around the globe to avoid persecution [18, 37]. Cyber crimes often breed from the countries or regions that have weak enforcement of the law [40]. In policing the virtual world, national jurisdictions make investigation slow and tedious, and at times impossible [12]. The security infrastructure of other countries is now an issue.

Global coordination and collaboration in the field of information security is critical [27]. Such coordination and collaboration between countries are still in its early stage. Unfortunately, protection of personal data varies from nation to nation, as does the regulatory agencies governing them [8, 29]. Such adequate legislation and law enforcement measures may not yet be established [36]. Nations enact laws that are based on different political and economic interests [24]. For example, different countries may have different privacy definitions and laws [23, 41]. In some countries, privacy of their citizens is valued. Other countries are less concerned about privacy of their citizens. Demands for a certain level of security and responsibility are required before doing business in another country, and more concerned about either the power of the government or the rights of the corporations.

Needs: There is a need to assure that customers and businesses in a foreign country are legitimate and

legal. There is a need for confidence toward all governments to block or arrest spammers. There is a need by global corporations to assure that foreign contractors can meet standards [3]. There needs to be global coordination and collaboration for ensuring data flows across national boundaries [27].

Solution: International laws and agencies to enforce global assurance are impractical due to the differences in laws, cultural values, and infrastructure of the country. For example, the age of consent varies from country to country. How privacy is defined varies between countries. And there is the issue of freedom of speech, a value in many countries, but suppressed in others. The solution for global assurance is a private-sector compliance and enforcement infrastructure working with different governments.

GLOBAL ASSURANCE DEFINED: Global assurance is the global collaboration of governments, ISP's, search engines, and businesses to ensure the integrity and confidence in the use of the Internet.

Currently, assurance is outsourced to a global army of privately trained and authorized inspectors and certifiers, a third party assurance industry [3]. An example of a third party assurance service is the external auditor [3]. Another example is how global financial institutions created Identrus, a company that offers certificate authority services via the Internet. It is a global infrastructure system to authenticate digital signatures for end-customer applications [5]. What is driving third party assurance service is international standards and technical specifications under the auspices of the International Organization for Standardization (ISO) [3].

In the future, the author predicts the burden of global assurance will be on ISP, search engines, and telecommunication carriers. These private organizations can and will trace and block and detect malicious communications via routers, gateways, and switches used by the Internet. For example, ISP will address spam coming from its clients. Search engines will block (censor) illegal web sites as defined by the country. This is already being done in China with Google.

SUMMARY

As security moved from a centralized mainframe computer to enterprise integrated systems, assurance must move from enterprise assurance to global assurance, the confidence that business done on the Internet is secured.

For global assurance, there is no perimeter to protect and it is difficult to know where the hacker is. Focus must be on the whole global system that crosses national boundaries. New strategies, policies, regulations, and techniques need to be developed and implemented by search engines and internet service providers, as well as corporations, governments, and private multi-national organizations, to provide global assurance.

An analogy for the development of global assurance is warfare. Past traditional warfare involved protecting a perimeter and having a frontline, and knowing where the enemy was. Today's modern warfare has no perimeter and lacks a frontline. You do not know where the enemy is.

However, a corporate official suggested that the perimeter, a frontline, to protect has collapse to that of the individual devices (leaf objects) on a network. Instead of thinking of protection expanding outward, thinking inward maybe the new paradigm.

"We must do our best to anticipate and defend ourselves from attack now that it is not clear where the enemy is. We also must be strategic and attack back in the right way and at the right times" (Anna Bynum, graduate student).

The next step is to further the theory development of global assurance for corporations and governments. This will lead to a paradigm shift for decision makers. A Delphi study, using corporate and government decision makers, is warranted for future research.

REFERENCES

1. Arens, A & Elder, R. & Beasley, M. (2005). Auditing and assurance services (10th Ed.). Prentice-Hall. Upper Saddle River, NJ.
2. Bella, G. & Bistarelli, S. (2005). Information assurance for security protocols. Computers & Security, 24(4), 322.
3. Blair, M. & Williams, C. & Lin, L. (2008). The new role for assurance services in global commerce. Journal of Corporation Law, 33(2), 325-361.
4. Bodin, L. & Gordon, L. & Loeb, M. (2008). Information Security and Risk Management. Communications of the ACM, 51(4), 64.
5. Bullard, J. (2000). Certainty in an age of uncertainty. The Banker, June 2000, pg. 10.

6. Cegielski, C. (2008). Toward the Development of an Interdisciplinary Information Assurance Curriculum: Knowledge Domains and Skill Sets Required of Information Assurance Professionals. Decision Sciences: Journal of Innovative Education, 6(1), 29-49.
7. Committee on National Security Systems (2005). National Information Assurance (IA) Glossary, Introduction No. 4009.
8. Connolly, P. (2000). Privacy as global policy. InfoWorld 22(37), 49-50.
9. Cryptome (1995). Technical Security Standards for Information Technology. http://cryptome.org/jya/rcmp1.htm (accessed March 3, 2010).
10. Ezingeard, J. & McFadzean, E. & Birchall, D. (2005). A Model of Information Assurance Benefits. Information Systems Management, 22(2), 20-29.
11. Ferrell, K. (2004). Cybercrime Spins Out of Control, TechWeb.com.
12. Fleming, C. (2008). Data Defense. Credit Union Magazine, 74(4), 64-65.
13. Gerber, M. and von Solms, R. (2008), Information security requirements – Interpreting the legal aspects. Computers & Security, 27(5-6), 124-135.
14. Hawkins, K.W. & Alhajjaj, S. & Kelley, S. S. (2003). Using CobiT to secure information assets. The Journal of Government Financial Management, 52(2), 22.
15. Himma, K. (2008). Legal, Social, and Ethical issues of the Internet. In Global Perspectives in Information Security: Legal, Social, and Internationsl issues, edited by Hossein Bidgoli, Wiley & Sons, New Jersey (2008).
16. Hoover, J. N. (2009). Securing the Cyber Supply Chain. InformationWeek, Nov 7, 2009. Accessed on Nov 12, 2009 at: www.informationweek.com/shared/printableArticle.jhtml; jsessionid=MDVLR2IXVQMBFQE1GHPCKH4ATMY32JVN?articleID=221600499
17. IAAC (2003). Engaging the Board: Corporate Governance and Information Assurance. Information Assurance Advisory Council, Cambridge, UK.
18. Jung, Bumsuk., Han, Ingoo., Lee, Sangjae. (2001), Security Threats to Internet: A Korean Multi-industry Investigation. Information & Management, 38(8), 487-498.
19. Karimi, J. & Konsynski, B. (1991). Globalization and information management strategies. Journal of Management Information Systems, 7(4), 7-26.
20. Lindenmayer, G. (2007). Information Security Standards: The 10 Keys to Protecting your Network. Risk Management, 54(12), 11.
21. McKnight, W. L. (2002). What Is Information Assurance? CrossTalk – Journal of Defense Software Engeinnering, July 2002 issue. http://www.stsc.hill.af.mil/crosstalk/2002/07/mcknight.html (accessed March 3, 2010).
22. Merkow, M. & Breithaupt, J. (2006). Information Security: Principles and Practices. Perason-Prentice Hall, Upper Saddle River, NJ. p. 8, 29, 31, 165.
23. Milberg, S., Smith, J. & Burke, S. (2000). Information privacy: Corporate management and national regulation. Organization Science 11(1), 35-57.
24. Oz, E. (1994). Barriers to international data transfer. Journal of Global Information Management 2(2), 22-29.
25. Phillips, T. (2007). Developing an information assurance learning programs based on academics. EDPACS, 36(2), 1-23.
26. Rasmussen, M, (2003) Analyst Report: IT Trends 2003 – Information Security Standards, Regulations and Legislation – Giga Information Group® 2003. Retrieved May 21, 2005 from CSOonline.com site: http://www.csoonline.com/analyst/report721.html.
27. Reidenberg (2000). Resolving conflicting international data privacy rules in cyberspace. Stanford Law Review, 52(5), 1315-1367.
28. Rose, L. (2004). Information security: A different balance. EDUCAUSE Review, 39(5), 5-10.

29. Rudraswamy, V. and Vance, D.A. (2001). Transborder data flows: Adoption and diffusion of protective legislation in the global electronic commerce environment. Logistics Information Management, 14(1/2): 127-136.
30. Scalingi, P. & Morrison, M. (2003). Power to the People. Security Management, 47(12), 93-97.
31. Schou, C. & Trimmer, K. (2004). Information Assurance and Security. Journal of Organizational and End User Computing, 16(3), 1-7.
32. Stahl, B. (2004). Responisbility for Information Assurance and Privacy: A Problem of Indvidual Ethics. Journal of Organizational and End User Computing, 16(3), 59-77.
33. Stephens, D. (1999). The globalization of information technology in multinational corporations. Information Management Journal 33(3), 66-71.
34. Stoneburner, G. (2001). Underlying Technical Models for Information Technology Security, NIST Speical Publication 800-33. National Institute of Standards and Technology, Gaithersburg, MD. p. 22.
35. Symantec Internet Security Threat Report (2006), Trends for July 05–December 05, Volume IX, Published March 2006, https://enterprise.symantec.com/enterprise/whitepaper.cfm
36. Symantec Internet Security Threat Report (2008a), Trends for July 07–December 07, Volume XIII, Published April 2008, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf
37. Symantec Report on the Underground Economy (2008b), July 07–June 08, Published November 2008
38. West, R. (2008). The Psychology of Security. Association for Computing Machinery. Communication of the AMC, 51(4), 34.
39. Whitman, M. & Mattord, H. (2009). Principles of Information Security, 3rd ed. Thomson-Course Technology, Bostom, MA. p. 4.
40. Williams, P. (August, 2001). Organized Crimve and Cybercrime: Synergies, Trends, and Responses, Global issues, arresting transnational crimes. An Electronic Journal of the U.S. Department of State, 6(2).
41. Zuckerman, A. (2001). Order in the courts? World Trade, 14(9), 26-29.

ACKNOWLEDGEMENT

The author wishes to acknowledge the Graduate students of his Spring 2010 Information Security graduate class for their input to this paper. Special recognition goes to Sarah Phillips, Anna Bynum, and Amy Laws.