

Faculty of Informatics

Faculty of Informatics - Papers

University of Wollongong

Year 2008

Social and Organizational Aspects of Information Security Management

K. Michael

University of Wollongong, katina@uow.edu.au

This conference paper was originally published as Michael, K, Social and Organizational Aspects of Information Security Management, IADIS e-Society 2008, 9-12 April 2008, Algarve, Portugal.

This paper is posted at Research Online.

<http://ro.uow.edu.au/infopapers/590>

SOCIAL AND ORGANIZATIONAL ASPECTS OF INFORMATION SECURITY MANAGEMENT

Katina Michael

*School of Information Systems and Technology, Faculty of Informatics, University of Wollongong
University of Wollongong, NSW, 2522, Australia*

ABSTRACT

This paper aims to explore social and organizational aspects of information security management. The changing nature of security is revealed against the backdrop of globalization. It provides a thorough review of literature on the topics of cyberethics as related to information security and transnational law. The objective of the paper is to cover broadly socio-organizational themes providing for the purpose of definition and a basis for further research. It thus raises a number of pressing issues facing organizations today, and offers an overview discussion on potential solutions. The main outcome of the paper is in showing that successful security strategies rely on well-thought out and executed organizational processes (i.e. human resources, legal), not just information technology hardware and software products.

KEYWORDS

Information security, cyberethics, security policy, risk management, human factors, transnational law

1. INTRODUCTION

1.1 Cyberethics

According to Quinn (2006, p. 55) “[e]thics is the philosophical study of morality, a rational examination into people’s moral beliefs and behavior... The study of ethics is particularly important right now. Our society is changing rapidly as it incorporates the latest advances in information technology ... some people selfishly exploit new technologies for personal gain...” The notion of cyberethics was born when the prefix *cyber* was introduced by novelist William Gibson in his book *Neuromancer*. The “cyber” refers to the world of networked computers; it therefore follows that cyberethics is the examination into people’s moral beliefs and behaviors in an online environment. Tavani (2007, ch. 3) proposes seven different ways of evaluating cyberethics issues. He also poses the question whether cyberethics issues are unique ethical issues. I.e., whether cybertechnology has had “a significant impact on our moral, legal, and social systems.” Other key sources on the topic include: Halbert (2005), Tavani (2004), Spinello (2003), Reynolds (2003), Kizza (2002), Spinello and Tavani (2001) and Fodor (1994).

1.2 Globalization

Globalization refers to “the process of creating a worldwide network of businesses and markets. Globalization results in a greater mobility of goods, services and capital around the world. Investments are made across national boundaries” (Quinn, 2006, p. 385). Globalization is at the heart of cyberethics in terms of its reach to a global society that has access to communications infrastructure. Quinn (2006, p. 54) defines a society as “an association of people organized under a system of rules designed to advance the good of its members over time.” Yet there are no distinct global rules that govern cyberethics, beyond guidelines, and this is where the challenges for international law begin. Even when treaties are ratified that pertain to computer-related issues, they are not truly global in the sense that all countries have agreed, but they are usually driven by a select group of countries (Johnson and Goetz, 2007, p. 17).

1.3 Policies, Procedures and Practice

Policies and procedures can be considered as formal rules that help resolve ambiguities in the organization (SANS Institute, 2007c). It is essential that organizations have clearly written policies on information and computer security issues. Easttom (2006, p. 144) writes that policies should cover acceptable use of organizational computers, the Internet, email, and other aspects of the system; they should prohibit the installation of any software on the systems; they should also “clearly delineate who has access to what data, how backups are performed, and what to do to recover data in the case of a disaster...” Policies differ from procedures. Procedures are defined as a set of instructions; they set out how things should be done. Policies are rigid while procedures are more flexible. Procedures are often described as a course of action developed to implement policy. For example, the anti-virus procedure in an organization typically defines guidelines for effectively reducing the threat of computer viruses on the organization’s network. A policy is defined as an organized and established system. They are a commitment by which an organization is held accountable. Policies should be written down, approved by management, and checked by lawyers (Bakry, 2003, p. 13).

1.4 Information Security Benchmarking

Security benchmarking is evaluating a company’s information technology security against another organization or set of security principles. The measures of evaluation are both qualitative and quantitative. Symantec sets out its best practice strategies for government and enterprises, indicating the following: security policies; risk assessments; standards, procedures and metrics; security roadmaps; selection and implementation of solutions; training of security professionals and employees; security management; and incident response and recovery (Australian Crime Commission, 2004, p. 56).

2. ORGANIZATIONAL SIZE AND SECTOR

2.1 Information Security Challenges in Small, Medium and Large Enterprise

In a small organization budgets are often limited (CERT, 2007a). In these firms, information security requirements are traditionally considered in terms of hardware and software, and as such treated as overheads. However, this trend is changing as small players find themselves engaged in electronic commerce with big business through global supply chains. Medium size organizations are more likely to place a greater emphasis on information security and data protection, especially given the requirement to do business online but they usually lack the security stealth of large organizations that span numerous countries. These transnational corporations are increasingly facing the pressures of globalization. How to protect their intellectual property, how to comply with laws and standards across jurisdictions (e.g. fair trade acts) etc.

2.2 Defining the Perimeters of a Global Organization

Among the hardest objectives to satisfy is managing security beyond the organization. It is often difficult to define where perimeters stop and start and what should be considered internal and external to the organization. For instance, consider an employee who forwards their work mail to a personal account on Google. Perimeter approaches to security are usually adopted by small organizations that have small budgets. Larger organizations tend to adopt hybrid security methods, where perimeters are secured but there is also a layered security approach analyzing individual systems within a network (Easttom, 2006, p. 14).

2.3 New Technologies Facilitating New Business Relationships

In global business today, relationships between companies in the form of alliances, partnerships and business-to-business (B2B) exchanges are playing a crucial role in time-to-market (TTM). Information flow

in the form of documents and transactions between firms is growing exponentially. Electronic transactions, just like paper-based transactions, are subject to regulations. The diverse range of end-user devices in the form of laptops, PDAs, and wearables that are powered by wireless networks are creating new challenges for personnel, as organizations demand real-time information. The software used on these hardware devices also carries with it security risks. Consider software errors that lead to system malfunctions and outright system failures. Major problems with electronic business for instance, may arise when one organization is engaged in best-in-class security practices, and the partner organization may not even be certified. Cultural differences also abound as organizations attempt to expand their boundaries. Strategic decisions to outsource are made by executives in positions of power who are often unaware of the implications. A typical scenario can be found in the government department who opts to outsource government-to-citizen (G2C) transactions to an offshore enterprise, only to later realize that private information has somehow found itself in the wrong hands. "While governments set their own standards ... the extent of standards use within the private sector is very patchy between different organizations" (Australian Crime Commission, 2004, p. 57).

3. ORGANIZATIONAL SECURITY POLICIES AND PRACTICES

3.1 Security Policies Across Office Locations

Instilling a culture of security to an employee base across jurisdictions and across enterprises is extremely difficult. Many remote office locations within multinational organizations deem themselves as having their own special requirements and therefore enact their own set of security policies and procedures. Even if policies look relatively similar between locations, their descriptions and how they are implemented may differ significantly. Penalties, for instance, for breaches of the ethics policy may be dealt with differently in two neighboring countries (SANS Institute, 2007a). More and more consulting companies are moving towards forming service level agreements (SLAs) and contracts with their multinational clients (Purser, 2004, p. 206). Added to this is 'how' things are done by people based on professional codes of conduct. Contrast the idea of an organizational ethics policy with that of "professional ethics" and codes of conduct.

3.2 Risk Assessment and Proactive Approaches to Information Security

Managing threats and vulnerabilities through risk management practices is increasingly being seen as the number one way to overcome business security challenges. Organizations conduct risk assessment and measurement in a number of different ways- (i) using risk assessment software often based on checklists, (ii) conducting risk analysis which at the simplest level identifies individual risks and then estimates the probability of loss and the likelihood of the event occurring in a given period, (iii) using compliance metrics which usually rely on automated audit software to check information system(s). Risk measurement is about measuring immunity and resiliency. If the gaps can be plugged then the chances of a breach in information security occurring is minimized (Kesar & Rogerson, 2001, p. 221). With each new breach new gaps are plugged as they are fed back to the appropriate personnel and systems (Ghosh, 2004). However, it must be stated, that a proactive approach to security management is required. Proactive approaches to security are when security tools and techniques are used to circumvent attacks before they occur. See especially Bakry (2003, p. 203) who describes going from the *current state* of security to a *target state* and emphasizes the importance of following a sound security development process. Whitman and Mattord (2005, p. 23) support this idea describing the Security Systems Development Life Cycle (SSDLC). In the past, organizations have waited for incidences that have crippled their organization's productivity before making decisions to institute a widespread, and often expensive, reflexive security measure.

3.3 Benchmarking an Organization's Security Portfolio

There are a number of ways to improve security- fundamentally it has to do with benchmarking oneself against other organizations. Even the best security solution after all, can never be foolproof, it can only

minimize breaches. One of the issues is that companies never quite know how much to spend on security, though it seems logical that the more they expend, the safer their enterprise will be. However, herein lies the anomaly, overspending on security, and becoming too security conscious, may impinge on employee welfare and productivity. How much security is too much security is a complex question even for consultants to answer. Basic information and computer security tools include: malware software, passwords, public key cryptography (asymmetric encryption), firewalls, intrusion detection systems, honeypots and audit software. These counter the potential for breaches in security including: viruses and worms, spyware, masquerading, denial of service attacks, spoofing, and phishing. Social engineering, however, is still a difficult attack to defend against as one or more individuals dupe another. Still, several layers of protection mean, that even if an attacker is able to attain some secret information that given subsequent measures, beyond logins and passwords, the attacker will be prevented from achieving their overall aim.

3.4 ISO 17799 Certification and Standards Compliance

The International Standards Organization (ISO) has a number of standards that pertain to security, and some organizations have indicated their 'readiness' to conduct electronic business by highlighting the fact that they are ISO 17799 certified (Johnson and Goetz, 2007, p. 22). This standard is mainly about security management and highlights that an organization has taken security seriously, at least at a basic level of assurance. Some security experts look on standards as compliance rather than improved security capabilities for their organization. Many organizations who achieve certification abandon the idea that security is a continual act and not a one-off quality issue. Other professional organizations and institutions also offer varying levels of certification and training. For instance see SANS Institute (2007b). GIAC has certified over 18,000 security professionals. The Certified Information Systems Security Professional (CISSP) is among the most respected security-related certifications.

3.5 Models for Funding and Resourcing Security

Funding and resourcing is an issue, and how to organize and prioritize who gets funding to meet particular types of security challenges is not straightforward. Are funds distributed only to the information technology group responsible for security, to individual departments, to individual systems, for new-hires to be utilized in security-related positions, to specific projects? CERT (2007b) state that "[n]eglecting security requirements, or isolating them from other requirements, jeopardizes the success of any development project. And because security is such a fundamental and pervasive consideration, it is difficult—and expensive—to incorporate into a finished application." Funding models are closely allied to system lifecycle approaches espoused by an organization. Other considerations include whether security funding is distributed on an annual or on a needs basis? Is security a core competency of the information technology group, and what are the risks associated with getting an external company to conduct security management? As Bernstein (pp. 88-92) predicted as far back as 1996, "budgetary constraints are likely to be the largest obstacle."

4. THE HUMAN FACTOR IN SECURITY

4.1 Hiring Talent with the Right Attitude

It has been said on more than one occasion that people are at the centre of good security practice- talent with the right attitude, expertise and business acumen (Stahl, 2002). Yet one criticism of security groups is that while they are technically astute, they often lack an overall strategic vision. The best security management initiatives can fail due to the staff's inability to carry them out appropriately (Friedman and Kahn, 1997, p. 303). In addition, security-centric resources are usually spread thinly across a number of portfolios. While Kesar and Rogerson (2001) state that "[o]rganizational problems such as lack of safeguards, together with ineffective monitoring and lack of internal audits, leads to illicit acts," they also emphasize that "personal factors" pertaining to individual employees are as much to blame.

4.2 Employee and Executive Accountability for Security Practices

In global organizations, there is a well-known cultural divide that can often only be bridged by top-down communications- from executives to subordinates. Post the dot.com crash a great number of executives found themselves on the unemployment queue or worse still criminally charged. Accountability, moral responsibility (Tavani, 2007, p. 95) and transparency are all issues that global organizations are grappling with and it is unfortunate that a rotten core often means that there are large portions that are negatively influenced by dubious practices. Typical questions asked include: who did this, who is in charge, what should I do in this instance, why should I do X, why did person A do action Z (Edgar, 2003, ch. 10)? Note the differences between responsibility and liability. Liability differs from responsibility in that it is a legal notion that carries with it real consequences and is often bound by law not just policy. The opposite problem also exists where control on employee practices is relaxed so much, that it is at the detriment of the security of the overall business. To work effectively, senior management need to be vocal about supporting security, staff need ongoing training, and an attitude that security is everyone's problem is required.

4.3 Data Governance by Executives and Senior Management

Data governance has meant that executives and boards are now officially responsible for an organization's adherence to federal and state laws (Pfleeger, 2007, p. 13). Case law has shown since 1996, beginning with the Caremark case (Trope, 2007, p. 32) that civil and criminal penalties apply for breaches in security. Today, executives in positions of responsibility may not only be tried on account of a conscious decision that was made in a given situation but in an "unconsidered inaction".

4.4 Cyberinsurance and the Need to Minimize Liability

In a bid for some large companies to attain some level of assurance they have taken out cyberinsurance for incidences like destruction of data and software, business interruption, data theft, denial of services and extortion (Baer and Parkinson, 2007, p. 50). All the major cyberinsurance carriers offer network security liability, content and electronic media injury, and breaches in privacy of confidentiality liability. Current offerings even address the issue of cyberterrorism based on such government acts like the *U.S. Terrorism Risk Insurance Act of 2002* (Tavani, 2007, p. 179).

5. LAWS, REGULATIONS AND LIABILITIES

5.1 The Trusted Corporation

Organizations should not adhere to security standards for the sake of compliance; they should adhere because it means that their business will remain sustainable. Tavani (2007, p. 213) however recognizes that in "America, there are strict liability laws, but there are also disclaimers and caveats issued by manufacturers to protect themselves against litigation." The idea of a trusted corporation is important here- no one wants to do business, especially consumers, with an organization that has been in the media due to financial losses as a direct result of breaches in security. Consumers especially do not wish to be liable for security breaches, such as personal data misuse. Enter the government, as an overseer of business practices with a mission to ensure personal data protection (Europa, 2007).

5.2 The Sarbanes-Oxley Act

Regulations like the *Sarbanes-Oxley Act* help drive security in organizations but there is a sort of chicken and egg problem here- is regulation driving security or security driving regulation? For instance, in section 404 of the Act, information security is not explicitly addressed but there is a requirement for internal control over

financial reporting, which in turn implies sufficient data security controls and security practices. Compare this Act with older legislative controls such as the *1990 Computer Misuse Act* in the United Kingdom, and the *1986 Computer Fraud and Abuse Act* and *1987 Computer Security Act* in the United States (Kesar and Rogerson, 2001, p. 223). It should also be noted here, that regulatory compliance requirements also imply enormous follow-up costs in IT processes and security management.

5.3 The European Cybercrime Treaty

To try to overcome issues with computer-related legislation across jurisdictions, in 2001 an international law enforcement treaty was drafted and signed by the United States, Canada, Japan and South Africa, led by the Council of Europe (CoE). "The articles of the treaty regulate illegal access, data or system interference, misuse of devices, computer-related forgery and fraud, child pornography, and copyright, among other items." The treaty was ratified in June, 2004 by thirty-eight countries. One of the major problems identified at the CoE 2004 International Conference on Cybercrime was that the "laws, criminal justice systems and levels of international cooperation have not kept pace with the lightning fast speed of technological development, despite the concerted efforts by the United Nations and the CoE." The problem with cyberspace is that physical boundaries are blurred, so the concept of jurisdiction also becomes difficult to enforce (Edgar, 2003, p. 190f). According to Tavani (2007, p. 213) "[n]ot only have there been problems in prosecuting Internet crimes that span state borders, but criminal enforcement has been hampered as well by a lack of international legal agreements and treaties." See also Weismann (2006, p. 243), and Smith et al., (2004, ch. 4) for cross-border issues and dealing with cybercrime. A major problem with international treaties is that countries are not bound to make changes to conflicts that might arise between the new international treaty and existing domestic laws. This introduces a number of ambiguities depending on the case.

6. GOVERNMENT POWERS AND LAW ENFORCEMENT AGENCIES

The powers of the government and respective law enforcement agencies have increased manifold since the rise of modern day communication systems. For example, there is an increasing number of Internet pedophilia cases which have seen chat-room predators convicted internationally. Among other crimes that law enforcement agencies are dealing with include: identity theft, organized crime, money laundering, cyberterrorism, fraud or embezzlement, theft of information or services, and industrial espionage (Brenner, 2007). While an organization attempts to make its private systems and networks more secure, legislation post-September 11 is making it even easier for the government to obtain information in the form of individual transaction records. Surveillance capabilities have not only increased because of advancements in technologies such as Closed Circuit Television (CCTV) but are now fully supported by legislation as well.

REFERENCES

- Australian Crime Commission (2004). *Cybercrime*, Canberra, Australia.
- Baer, W. S. and A. Parkinson (2007). "Cyberinsurance in IT Security Management." *IEEE Security and Privacy*, Vol. 5, No. 3, pp. 50-56.
- Bakry, S. H. (2003). "Development of security policies for private networks." *International Journal of Network Management*, Vol. 3, pp. 203-210.
- Bernstein, T., A. B. Bhimani, et al. (1996). *Internet Security for Business*, New York.
- Loader, B. D., Ed. (1998). *Cyberspace divide: equality, agency, and policy in the information society*. London, Routledge.
- Brenner, S. (2007). "CyberCrimes." Retrieved 11 September 2007, from <http://law.udayton.edu/cybercrimes>.
- CERT. (2007a). "Information Assurance in Small Organizations." Retrieved 10 September 2007, from <http://www.cert.org/archive/pdf/tutorial-workbook.pdf>.
- CERT. (2007b). "Welcome to CERT." Retrieved 9 September 2007, from <http://www.cert.org/>.

- Centre for Democracy and Technology, (2007). "International Issues: Cybercrime." Retrieved 11 September 2007, from <http://www.cdt.org/international/cybercrime/>.
- Dhillon, G. (2002). *Social responsibility in the information age electronic resource: issues and controversies*. Hershey, PA, Idea Group Pub.
- Easttom, C. (2006). *Computer Security Fundamentals*, Boston, Prentice Hall.
- Edgar, S. L. (2003). *Morality and Machines: Perspectives on Computer Ethics*. Boston, Jones and Bartlett Publishers.
- Europa. (2007). "The European Data Protection Supervisor (EDPS)." Retrieved 11 September 2007, from <http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/2>.
- Fodor, J. L. (1994). *CyberEthics*. SIGCAS: ACM Special Interest Group on Computers and Society.
- Friedman, B. and J. Peter H. Kahn (1997). People are Responsible, Computers are Not. *Computers, Ethics, and Society*. M. D. Ermann, M. B. Williams and M. S. Shauf, pp. 303-312.
- Ghosh, S., M. Malek, et al. (2004). *Guarding Your Business: A Management Approach to Security*.
- Halbert, T. (2005). *Cyberethics*. Cincinnati, Ohio London, West Legal Studies in Business; Thomson Learning.
- Hester, D. M. and P. J. Ford, Eds. (2001). *Computer and Ethics in the Cyberage*. New Jersey, Prentice Hall.
- Hodges, M. P. (2001). Does Professional Ethics Include Computer Professionals? *Computers and Ethics in the Cyberage*. D. M. Hester and P. J. Ford, pp. 195-203.
- Johnson, D. G. (2001). Professional Relationships. *Computers and Ethics in the Cyberage*. D. M. Hester and P. J. Ford, pp. 204-218.
- Johnson, M. E. and E. Goetz (2007). "Embedding Information Security into the Organization." *IEEE Security and Privacy*, Vol. 5, No. 3, pp. 16-24.
- Jones, A. and D. Ashenden (2005). *Risk Management for Computer Security*.
- Kesar, S. and S. Rogerson (2001). Developing Ethical Practices to Minimize Computer Misuse. *Computers and Ethics in the Cyberage*. D. M. Hester and P. J. Ford, pp. 218-232.
- Kizza, J. M. (2002). *Ethical and social issues in the information age*. New York, Springer-Verlag.
- Loader, B. D., Ed. (1998). *Cyberspace divide: equality, agency, and policy in the information society*. London, Routledge.
- Pfleeger, S. L. et al. (2007). "Managing Organizational Security." *IEEE Security and Privacy*, Vol. 4, No. 3, pp. 13-15.
- Purser, S. (2004). *A Practical Guide to Managing Information Security*, New York.
- Quinn, M. J. (2006). *Ethics for the Information Age*. Boston, Pearson International.
- Reynolds, G. W. (2003). *Ethics in Information Technology*. Cambridge, Mass. London, Course Technology.
- SANS Institute. (2007a). "Ethics Policy." Retrieved 12 August 2007, from http://www.sans.org/resources/policies/Ethics_Policy.pdf?portal=90c7a9b30e37790abef35cf1776d0465.
- SANS Institute. (2007b). "Global Information Assurance Certification." Retrieved 11 September 2007, from <http://www.giac.org/>.
- SANS Institute. (2007c). "The SANS Security Policy Project." Retrieved 10 August 2007, from <http://www.sans.org/resources/policies/?portal=60dc42d044fcc27083a8261e08c8aacd>.
- Slay, J. and A. Koronios (2006). *Information Technology Security and Risk Management*.
- Smith, R. G., P. Grabosky, et al. (2004). *Cyber Criminals on Trial*, New York.
- Spinello, R. A. (2003). *CyberEthics: morality and law in cyberspace*. Boston, Jones and Bartlett Publishers.
- Spinello, R. A. and H. T. Tavani (2001). "The Internet, ethical values, and conceptual frameworks: an introduction to Cyberethics " *ACM SIGCAS Computers and Society*, Vol. 31, No. 2, pp. 5-7.
- Spinello, R. A. and H. T. Tavani (2004). *Readings in cyberethics*. Sudbury, Mass., Jones and Bartlett Publishers.
- Stahl, B. (2002). *Information technology, responsibility, and anthropology*. Proceedings of the 35th Annual Hawaii International Conference on System Sciences, Hawaii.
- Stahl, B. (2004). *Responsible management of information systems*. Hershey PA, Idea Group Pub.
- Tavani, H. T. (2004). *Introduction to cyberethics electronic resource: concepts, perspectives, and methodological frameworks*.
- Tavani, H. T. (2007). *Ethics and technology: ethical issues in an age of information and communication technology*. Hoboken, N.J., John Wiley.
- Trope, R. L., E. M. Power, et al. (2007). "A Coherent Strategy for Data Security through Data Governance." *IEEE Security and Privacy*, Vol. 5, No. 3, pp. 32-39.
- Weismann, M. F. M. (2006). Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime. R. D. Clifford, pp. 243-278.
- Whitman, M. E., Mattord, H.J. (2005). *Principles of Information Security*, New York, Thomson.