

## **Ethical and Legal Issues for the Information Systems Professional**

**Thomas A Pollack**  
**Association Dean / Director of Undergraduate Studies**  
**Kathleen S. Hartzel**  
**Division Chair of Information Systems Management**  
**Duquesne University**  
**School of Business Administration**  
**600 Forbes Avenue**  
**Pittsburgh, PA 15282**  
**412-396-1639**  
[pollack@duq.edu](mailto:pollack@duq.edu)

### **Abstract**

We are living in an era in which we routinely deal with issues such as privacy, digital security, identity theft, spyware, phishing, Internet pornography and spam. These costly and time consuming concerns were completely foreign to the American public only a few years ago. State and federal privacy and security legislation is evolving with the intention of protecting the general citizenry from harm and organizations from financial loss and civil or criminal lawsuits. Organizations, particularly information systems professionals within organizations, are being called upon to deal with these issues and institute controls to minimize risk.

This paper will examine the growing issue of malicious digital risks from both a legal and ethical perspective. The relationship of these risks to the core values and ethical conduct of the information systems professionals in our organizations will be explored. A cost-benefit perspective will be used to discuss the effect of legislation on organizations and society at large. Finally, the content of university level curricula designed to address these issues will be suggested

### **Introduction**

There is a frequently used expression that emphasizes that information has no ethics. The ethical aspect of organizations and the manner in which information is managed resides with the values that are inherent in the people that comprise the organization. The manner in which information is used is dependent on the ethics and beliefs of the people that make up the organization, especially the organization's leadership. It has become increasingly clear that information is a valuable organizational resource that must be carefully safeguarded and effectively managed just as other organizational resources are managed. Information cannot secure itself or protect itself from phishers, spyware, or identity thieves.

In general, people have become much more technologically savvy. Largely due to the dramatically increased scope of information available via the Internet, the ease of access to information, and the broadened scope of computer literacy, the security of information and the privacy of individuals have become areas of significant concern. Concerns about security and privacy as well as ethical dilemmas dominate our daily lives. As a result of personal concerns and fears, and the rapid increase of theft of personal information, organizations have developed and / or revised codes of ethical conduct. Simultaneously, our government agencies have enacted laws and legis-

lation that are specifically related to ensuring the privacy and security of information and individuals.

## **Ethics**

As individuals, our civility toward each other is an indicator of our ethical values. Likewise, the value set of individuals is the sole determinant of the use of information. Because ethical issues cover a very wide spectrum, many organizations attempt to develop a broad framework that managers can apply to issues as they occur. One such general framework is derived from an article written by Richard Mason (1986). Mason identified four areas of critical concern for managers. They include privacy, accuracy, property, and accessibility and are frequently referred to by the acronym PAPA. Mason's article, which continues to be referenced as providing an ethical framework, contends that control of information as it pertains to those four areas is critical.

Another type of framework that has emerged as a standard in many organizations is a code of ethical conduct. Codes of ethical conduct are typically published by professional organizations, however, many organizations have published organizational codes of conduct. For information systems professionals, the most popular professional code of conduct is that published by the Association for Computing Machinery (ACM). The complete ACM Code of Ethical Conduct is available online at <http://www.acm.org/constitution/code.html> (Gray, 2006).

As we prepare future professionals for employment in technology fields, it is imperative that we develop a sense of awareness of the potential types of ethical issues that are common to information systems organizations. Included in a long list of issues that are covered by policies in most organizations are policies for ethical computer use, information privacy, acceptable use, email, Internet use, and an anti-spam policy (Haag, 2006).

Pearlson (2006) points out that managers must be involved in monitoring outward activities of the business because customers and their privacy are affected when there are outward breaches. Equally important are inside issues such as internal surveillance and monitoring activities, because these affect employees. Because Internet usage, instant messaging and email are so prevalent in today's organizations, a number of software surveillance products have been developed and are being implemented. Monitoring and surveillance have increased as the need to protect privacy, insure security and control the privacy of information has increased (Pearlson). However, the use of these products and practices in themselves frequently create ethical dilemmas and must be properly communicated to employees and implemented properly.

## **Organizational Issues**

The financial world and corporate community, in general, were rocked by the accounting scandals at ENRON, TYCO, and WorldCom. These Scandals focused attention on the lack of ethical conduct on the part of a few individuals and the magnitude of the harm and financial ruin that can result. However, the technology field has been overtaken with other types of behavior that can affect anyone who uses technology. Computer virus and hacker attacks are intended to destroy data and software and disrupt computer services. In 2002, alone, more than 7,000 computer viruses were reported (Henry, 2005). Phishing attacks frequently target a specific group of people and are intended to secure personal information, usually financially related, from innocent and unsuspecting responders (Gonsalves, 2004).

Criminals are especially interested in acquiring social security numbers, bank account information, credit card numbers and other financially-related data that can help them to steal identities or money from unsuspecting customers (Bradford, 2005). Bradford also reported that external hackers are the most significant risk to companies, but that a great amount of damage and threats to cyber security originates with insiders, especially disgruntled insiders. On the other hand, others contend that the most serious threats to computer security comes from individuals thought to be trusted insiders. Particular vulnerability comes from disgruntled and terminated employees. Although the two week notice for resignation or termination remains popular, terminating all network access upon notice of termination of employment is most effective (Henry, 2005).

Paul Roberts in an eWeek article (2005) reports that, programs commonly referred to as “spyware” or “adware” have become very widespread. These programs monitor users’ online behavior, threaten compliance efforts and intellectual property, and create problems for computer users and IT administrators, alike. It is reported by Webroot Software, Inc. that spyware is a \$2 billion per year industry (Roberts). It is also reported that a clean-up of spyware or adware will be an expensive challenge. Distribution of spyware is usually in bundles with such things as freeware and computer games.

Some of the problems that prevail as a result of spyware include slow computer processing speeds and pop-ups taking over. Research attributed to Harvard Law School student, Ben Edelman indicates that adware and spyware bundling deals are lucrative, even for companies not in favor of inclusion. Some spyware companies will pay up to one dollar per install. Microsoft reports that approximately 33 percent of application crashes are caused by spyware. Remedies for spyware include installation of anti-spyware software and switching from the more vulnerable Microsoft programs (Roberts, 2005).

Identity theft is the appropriation of someone else’s identity to commit fraud or theft (Sovern, 2004). One of the possibilities to help prevent identity theft in the future involves biometric technology such as fingerprints or voice scans used to verify the identity of credit applicants. The general sense at this time is that this may be a cure that is more costly than the problem to be solved (Sovern). However, the consequences of identity theft are significant, and the financial impacts exceed billions of dollars each year (Lacey, 2004). The victim is subject to loss of funds or other property, a tarnished credit history, a possible criminal record, difficulty in securing employment, and an inability to obtain goods and services (Lacey, 2004). Identity theft is a problem that affects both individuals and organizations, and remedies must be developed.

It became apparent after Y2K that security and privacy issues required attention. Viruses were very prevalent, operating system and application vulnerabilities were increasing and computer security breaches were increasing at an alarming rate. The organization’s first line of defense, the firewall, was most likely installed because it was easy to install and maintain and didn’t disrupt regular business applications. However, security from these early firewalls was absent. The cost of repairing damage from Internet attacks was staggering (Henry, 2005).

By 2003, there was a shift in attitudes toward security from perception as an expense side of the balance sheet to perception as an asset. In selecting firewalls, there was a notable increase in the evaluation of firewalls based on their ability to provide security. It remains imperative that firewalls, while being effective, must also be easy to manage (Henry, 2005).

From the short list of scenarios above, one can easily understand that organizations were forced to radically alter their processes with regard to privacy and security. In addition to the many measures taken by organizations to safeguard privacy and security, new laws and legislation have been introduced to help decrease the number and magnitude of privacy and security breaches.

### Legislation and Compliance Requirements

Internally, organizations realized that they were not meeting expectations and privacy concerns in the late 1990's and early 2000's. Government agencies also realized that we are facing a new and monumental problem. This brought about new legislation and laws to help ensure that personal privacy and security of information would be protected.

Haag (2006) does a wonderful job of summarizing legislation that has been enacted to help ensure the privacy of individuals and the security of information. A table summarizing some of the key legislation appears below.

### Established Information Related Laws (Haag, 2006)

Privacy Act - 1974	Restricts the government's collectable information; requires permission to disclose name-linked info; enables your access/correction of your info
Family Education Rights and Privacy Act - 1974	Regulates government & third party access to education records and ensures the student's access
Cable Communications Act - 1984	Requires viewer's consent for cable providers to release their viewing preferences
Electronic Communications Privacy Act - 1986	Employees do not have privacy rights on their firm's computers
Computer Fraud and Abuse Act - 1986	Requires authorized access to computers used for financial institutions, US government, or interstate/international trade
The Bork Bill (Video Privacy Protection Act - 1988)	A consumer's video rental info can only be used for marketing directly towards him/her
Communications Assistance for Law Enforcement Act - 1994	Requires the ability for government agents to intercept all wire and wireless communications, and caller-ID information
Freedom of Information Act - 1967, 1975, 1994, & 1998	Allows anyone to examine government records unless it's an invasion of privacy
Health Insurance Portability and Accountability Act (HIPPA) - 1996	Requires the health care industry to keep patient information confidential
Identity Theft and Assumption Deterrence Act - 1998	Made ID Theft a federal crime and established a central federal service for victims
USA Patriot Act - 2001, 2003, & 2006	Allows law enforcement access to any restricted information while investigating terrorism
Homeland Security Act - 2002	Limits Freedom of Information Act; allows government agencies to mine data on one's emails and web site visits
Sarbanes-Oxley Act 2002	Provides investors with accurate and reliable corporate disclosures

Fair and Accurate Credit Transactions Act - 2003	Consumers' right to a free credit report; full credit card number cannot be on a receipt; requires credit agencies to take proactive measures
CAN-Spam Act 2003	Penalizes businesses for sending unsolicited e-mails to consumers
Financial Modernization Act of 1999 (Gramm-Leach-Bliley Act)	Protect consumers' personal financial information held by financial institutions

Without detailing all of the charted legislation, several pertinent laws warrant special mention. For instance a new Federal Trade Commission rule went into effect on June 1, 2005 as part of a congressional crackdown on identity theft. Basically the law requires that any personal information that businesses obtain from credit bureaus and other agencies be destroyed so it cannot be stolen or misused (Kittredge).

Signed into law on December 4, 2003 the Fair Accurate Credit Transactions Act (FACTA) is intended to thwart the growth of consumer fraud and identity theft. For example, the FACTA disposal rule requires every employer with one or more employees to dispose of any electronic or paper documents or face federal fines of up to \$2,500 per violation and state fines up to \$1,000 per violation (Gurchiek). It also obliges credit bureaus to block the reporting of any information that is based on the transaction of an identity thief once the consumer provides specific information (Sovern, 2004). FACTA also addresses several specific aspects of identity theft including compulsory credit card number truncation on receipts, mandates to credit issuers to investigate address changes and new card requests, fraud alert requirements for credit reporting agencies, mandatory blocking of identity theft related information on credit reports and free annual credit reports (Linnhoff, 2004).

Another act that is intended to reduce the amount of unwanted spam is the Federal Trade Commission's Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). Although CAN-SPAM has not yet had a significant impact on email problems, a recent report indicated that spam accounted for 67% of email messages during the first eight months of 2005, and this figure represented a nine percent decrease from the same period in 2004 (Spring, 2005). The Act has also helped reduce the amount of world spam created in the US from 46% of world spam in 2004 to 26% in 2005. At the same time, however, world spam is up, with China and South Korea leading the way ("Legislating Cyberspace," 2006).

Federal legislation such as the Sarbanes-Oxley Act and Gramm-Leach-Bliley Act emphasize the importance of identity management. Managers must be aware of how information is being used, maintained, and provided and also how it can be effectively protected and updated to meet business needs while, at the same time, complying with audit and privacy regulations (Sturdevant).

The piece of legislation that warrants special consideration for IT professionals is the Sarbanes-Oxley Act of 2002 (SOX). This legislation has a far-reaching impact on publicly traded companies. Although originally aimed at the financial health and regulatory visibility and accountability of public companies, the act has also significantly impacted IT departments. Particularly Section 404 of the act requires that auditors certify the underlying controls and processes used to compile financial results. Officers are held personally responsible for financial information reported, and penalties range from fines to a five to 30 year jail term (Pearlson 2006).

SOX Section 404 requires public companies to attest to the effectiveness of internal controls at year end. SOX stresses that upper management has ultimate responsibility for ensuring that adequate controls are in place throughout the organization (Summary of Sarbanes-Oxley, 2002). Although SOX was originally targeted at accounting, it became obvious very quickly that IT plays a vital role in ensuring the accuracy of accounting data. It is imperative for IT professionals to become “well-versed in internal control theory and practice to meet the requirements of the act” (Sarbanes-Oxley, FAQ, 2006).

Although the focus of SOX is on financial controls, many auditors required IT managers to extend their attention to organizational controls and risks in business processes (Pearlson, 2006). Some companies have created new IT positions to deal with compliance challenges (Bednarz, 2006).

### **Compliance is Costly**

The implementation of adequate system controls and attention to compliance and corporate governance requirements are expected to increase corporate budgets. For example, process manufacturers are expected to increase their IT investments in 2006 from 3.5% to 3.7% of total revenues as reported by AMR Research of Boston (Seewald, 2006). The report goes on to state that the primary impact on increased costs is regulatory compliance. The Gartner Group of Stamford, CT reports that a 2005 survey of 190 firms revealed that compliance and corporate governance requirements including Sarbanes-Oxley (SOX) regulatory mandates will account for 10-15% of IT budgets up from less than 5% in 2004 (Seewald). The Gartner Group also indicates that although there is no single SOX compliance software, two new software markets have emerged in response to compliance regulations. They are financial compliance process management software (records retention, archiving and access, management oversight, substantiation of due diligence) and application and access control software (segregation of duties, adherence to change management procedures) (Seewald).

A study of 450 companies conducted by Foley and Lardner and KRC Research indicated that in large organizations with a capitalization around \$1 billion, audit fees increased about 35% in 2002 due largely to SOX implementation. AMR Research reported that SOX compliance is like “Y2K” and will cost as much as \$2.5 billion. The rule of thumb has been an average of \$1 million in SOX expenses for every \$1 billion in revenue (Bednarz, 2006). AMR Research also reports that collective spending on SOX compliance has increased from \$2.5 billion in 2003 to \$5.5 billion in 2004 to \$6.1 billion in 2005 and will exceed \$6 billion in 2006. The typical allocation of costs breakdown as 39% for internal labor, 32% for technology and 29% for external consulting. As companies gain SOX experience, these costs are expected to decrease (Bednarz).

### **Conclusions and Recommendations**

One can readily conclude that the inter-related issues of personal and organizational ethics, privacy, information security, and protective legislation have formed a rather complex web that must be understood by technology managers. Spyware, adware, and phishing attempts have grown in sophistication and prominence. Identity theft is a threat that must be taken seriously by all members of our society. Organizations have taken preventative actions through enactment of codes of ethics and codes of conduct. Government agencies have responded with legislation intended to protect the integrity of data and the privacy of individuals.

Educators are aware of the growing complexity of information security and the ethical issues that revolve around the multitude of possible breaches. Some may contend that it is difficult to teach ethics and values, but, as educators, we have a responsibility to develop a sense of awareness of the issues. More and more colleges and universities are offering, or in some cases, requiring ethics courses. If you are concerned about some of the issues raised in this paper, a required ethics course may be worthy of your consideration.

As we assess our technology curricula, the following considerations may warrant your consideration for possible inclusion in revised curricula:

- A course in information ethics that examines the types of ethical dilemmas likely to be encountered by technology professionals.
- Inclusion of professional codes of conduct such as the Association for Computing Machinery Code of Ethical Conduct.
- Detailed coverage of the range of issues related to identity theft.
- Emphasis on system security controls.
- Comprehensive coverage of laws and legislation to develop a sense of awareness of compliance requirements that affect technology professionals.
- Specific discussion and familiarization with Section 404 of the Sarbanes-Oxley Act.
- A strongly recommended or required field employment or internship experience.

## References

- Bednarz, Ann. "The SOX Tax." Network World. Framingham: Apr 10, 2006. Vol. 23, Iss. 14; pg. 45, 3 pgs.
- Bradford, Michael. "Cyber Privacy Rules Challenge Employers." Business Insurance. Chicago: Nov 28, 2005. Vol. 39, Iss. 48; pg. 11, 3 pgs.
- Gonsalves, Antone. "Latest Trojan 'Phishes' For Personal Data." Internet Week. <http://internetweek.cmp.com/showArticle.jhtml?articleID=17301949>. January 14, 2004.
- Gray, Paul. Manager's Guide to Making Decision About Information Systems. John Wiley & Sons, Inc. 2006.
- Gurchiek, Kathy. "Federal Rule on Disposal of Sensitive Data in Effect." HRMagazine. Alexandria: July 2005. Vol. 50, Iss. 7; pg. 27, 2 pgs.
- Haag, Stephen, Paige Baltzan, and Amy Phillips. Business Driven Technology. McGraw-Hill. 2006.
- Henry, Paul A. "Firewall Consideration for the IT Manager." Information Systems Security. New York: Nov/Dec 2005. Vol. 14, Iss. 5; pg. 29. 23 pgs.
- Kittredge, Clare. "ID Theft Rule Casts Wide Net." New Hampshire Business Review. Concord: July 8, 2005. Vol 27, Iss. 14; pg. 1.

- Lacey, David and Suresh Cuganesan. "The Role of Organizations in Identity Theft Response: The Organization –Individual Victim Dynamic." The Journal of Consumer Affairs. Madison: Winter 2004. Vol. 38, Iss. 2; pg. 244, 18 pgs.
- "Legislating Cyberspace." eWeek. New York: Jan 9, 2006. Vol. 23, Iss. 2; pg. 32.
- Linnhoff, Stefan and Jeff Langernderfer. "Identity Theft Legislation: The Fair and Accurate Credit Transactions of 2003 and the Road Not Taken." The Journal of Consumer Affairs. Madison: Winter 2004. Vol. 38, Iss. 2; pg. 204, 13 pgs.
- Mason, Richard O. "Four Ethical Issues of the Information Age." MIS Quarterly. March 1986, Vol. 10, Iss. 1.
- Milne, George R. "How Well Do Consumers Protect Themselves From Identity Theft?" The Journal of Consumer Affairs. Madison: Winter 2003. Vol. 37, Iss. 2; p. 388.
- Pearlson, Keri E. and Carol S. Saunders. Managing & Using Information Systems: A Strategic Approach. John Wiley & Sons, Inc. 3<sup>rd</sup> Edition. 2006.
- Roberts, Paul F. "The Many Faces of Spyware." eWeek. New York: June 20, 2005. Vol. 22, Iss. 25; pg. 24.
- "Sarbanes-Oxley Frequently Asked Questions." Accessed at [www.isaca.org](http://www.isaca.org), 2005.
- Seewald, Nancy. "Budgets Rise as Firms Seek Software to Improve Business." Chemical Week. New York: Mar 22, 2006. Vol. 168, Iss. 10; pg. 39, 1 pgs.
- Sovern, Jeff. "Stopping Identity Theft." The Journal of Consumer Affairs. Madison: Winter 2004. Vol. 38, Iss. 2; pg. 233, 11 pgs.
- Spring, Tom. "Spam Slayer: FTC's CAN-SPAM Report Card." PC World.Com. San Francisco: Dec 20, 2005. pg. 1.
- Sturdevant, Cameron. "Stronger Sense of Identity." eWeek. New York: Dec 19, 2005. Vol. 22, Iss. 50; pg. 73.
- "Summary of Sarbanes-Oxley Act of 2002." Accessed at [www.aicpa.org/info/sarbanes\\_oxley\\_summary.htm](http://www.aicpa.org/info/sarbanes_oxley_summary.htm)
- Swartz, Nikki. "The Cost of Sarbanes-Oxley." Information Management Journal. Lemexa: Sep/Oct 2003. Vol. 37, Iss. 5; pg. 8.