READINGS AND CASES IN INFORMATION SECURITY: LAW AND ETHICS

Readings and Cases in Information Security: Law and Ethics provides a wealth of content presented with an engaging, analytical viewpoint. Designed for use with any Cengage Learning security text or as a standalone professional reference, this book offers a real-life view of information security management, including the ethical and legal issues associated with various on-the-job experiences. Included are a wide selection of foundational readings and scenarios from a variety of experts to give the reader the most realistic perspective of a career in information security.

Features:
• Contains a variety of case studies designed to stimulate in-class and written discussion.
• Prepares the reader for situations in the information security industry with best practices, articles, and cases relating to the most up-to-date security issues.
• Discussion questions at the end of various readings or case studies inspire the reader to further their understanding of each case and gain better perspective on material covered.
• Coverage of current ethical and legal issues provides a modern look at one of today's fastest growing fields.
• Running case studies uses realistic scenarios to prompt classroom discussion and expand worldview on legal and ethical matters in the information security field.

About the Authors:
Michael E. Whitman, Ph.D., CISM, CISSP, is a professor of Information Systems in the Computer Science and Information Systems department at Kennesaw State University, Kennesaw, Georgia. Dr. Whitman is an active researcher in Information Security, Fair and Responsible Use Policies, and Ethical Computing and Information Systems Research Methods. He has published Information Systems Research articles, the Communications of the ACM, Information and Management, the Journal of International Business Studies, and the Journal of Computer Information Systems. He is an active member of the Computer Security Institute, the Information Systems Security Association, Georgia Electronic Commerce Association’s Information Security Working Group, the Association for Computing Machinery, and the Association for Information Systems.

Herbert J. Mattord, M.B.A., CISM, CISSP, recently completed 24 years of IT industry experience as an application developer, database administrator, project manager, and information security practitioner before joining the faculty at Kennesaw State University. During his career as an IT practitioner, he has been an adjunct professor at Kennesaw State University, Southern Polytechnic State University, Austin Community College, and Southwest Texas State University. He currently teaches courses in Information Security, Data Communications, Local Area Networks, Database Technology, Project Management, and Systems Analysis and Design. He was formerly the Manager of Corporate Information Technology Security at Georgia-Pacific Corporation.

Also Available from Course Technology:

READINGS AND CASES IN INFORMATION SECURITY: LAW AND ETHICS
Michael E. Whitman and Herbert J. Mattord

COURSE TECHNOLOGY
CENGAGE Learning

To learn more about Course Technology, visit www.cengage.com/coursetechnology
Purchase any of our products at your local distributors or at our preferred online store www.cengagebrain.com
Readings and Cases in Information Security
Law and Ethics

Michael E. Whitman
Herbert J. Mattord
Global Information Security Regulations, Case Studies, and Cultural Issues

Guillermo A. Francia, III
Jacksonville State University

Andrew P. Ciganek
University of Wisconsin at Whitewater

Dr. Guillermo A. Francia, III, received his Ph.D. in computer science from New Mexico Tech. In 1996, Dr. Francia received one of the five national awards for Innovators in Higher Education from Microsoft Corporation. Dr. Francia served as a Fulbright scholar to Malta in 2007. His research interests include computer security, digital forensics, visualization, data mining, and performance dashboards. Currently, Dr. Francia is serving as Director of the Center for Information Security and Assurance at JSU.

Dr. Andrew P. Ciganek is an Assistant Professor of information technology and business education at the University of Wisconsin at Whitewater. He earned his Ph.D. from the University of Wisconsin—Milwaukee in 2006. His research interests include examining the managerial and strategic issues associated with the decision-making process of innovative technologies. He has had several refereed publications and has also published book chapters examining topics related to Mobile Computing Devices and Enterprise Application Integration.
Overview

The pervasiveness of the Internet has created a new challenge to legislators around the globe: the enactment of regulations that will preserve and protect the country’s information technology (IT) infrastructure and its integrity in delivering secure products and services. This paper examines the global, and yet unilateral, attempts of various countries in ratifying their own information security legislations.

Introduction

In 2005, Thomas Friedman wrote on the subject of a perceivable economic change that was brought about by globalization.¹ He suggested that the world has gone “flatter” in the sense that the competitive field between established and emerging market economies have leveled. Among the so-called “flatteners” that Friedman defined are “outsourcing” and “offshoring.” These two concepts induce the tapping of “economically viable” job markets in countries such as China and India. As a consequence, information security regulations have to reach out as well. Countries that need to stay viable need to legislate their own information security regulations that are in line with those in the country where their counterparts are located. However, one of the most difficult aspects of creating and passing a national legislation that is in conformity with international regulations is the need to accommodate differing cultures, varying structural and governmental models, and the intricacies of making it consistent with existing public policies and regulations.

The issue of preserving “economic viability” in the global job market is not the only compelling reason for a country to strengthen its information security legislations and regulations. Other possible reasons may include the following:

- the protection of its citizens’ fundamental right to privacy;
- the security of the country’s critical infrastructures;
- the preservation of the intellectual property rights of its public and private constituents;
- the upholding of the country’s integrity and its international reputation;
- the protection of consumers, investors, financial market, and banking system; and
- the adherence to internationally recognized standards and protocols that apply to cyberspace and information handling.

Mitrakas and Portesi raise the issue of whether there is a real need to regulate network and information security and the conditions with which it can be taken up by legislators.² They suggest using the soft law approach³ in creating regulations due to sporadic instances of ineffective legislations. Soft law, self-regulation, and co-regulation are alternative regulatory instruments that can be used to shape the processes of self-regulation, to determine an alternative to legislation, and to complement existing legislations. But no matter what approach a certain country, region, group, or union decides to follow, the resulting information security regulation should be founded on the following guiding principles: respect for basic human rights, fairness and timeliness, protection of privacy rights, and sensitivity to moral and ethical issues.
The remainder of the reading includes an extensive literature review of and case studies on global information security regulations, guidelines, and directives. In addition, a discussion on the cultural issues influencing the legislations and their enforcements are presented. Specific to the subject at hand will be a case study on the state of information security regulation in Thailand. Thailand is uniquely situated on the opposite ends of every national culture dimension with the United States, and in some instances, the most extreme ends. For example, the United States is characterized as one of the most individualistic cultures (loose bonds with others), while Thailand represents one of the most collectivist cultures (everyone takes responsibility for others). Similar dichotomies exist among both cultures in each of the other national culture dimensions and have been shown to significantly influence differences in perceptions. Such differences in culture offer opportunities to reveal insights into the various activities that prevail within each country to protect data. The reading concludes with an analysis of the similarities of different information security regulations worldwide, a discussion on the need for harmonization, and descriptions of future research opportunities related to the subject matter.

The Regulations, Acts, and Directives

The following literature review on information security regulations are organized according to affected sectors: privacy protection, financial and banking services, electronic commerce, government, publicly traded entities, and general population.

Privacy Protection

Iceland  Iceland has been actively amending its Data Protection Act, which is also known as Act on the Protection of Privacy as Regards to the Processing of Personal Data. The law has been amended four times: Act No. 90/2001, Act No. 30/2002, Act No. 81/2002, and Act No. 46/2003. Its basic provision is “to promote the practice of personal data processing in accordance with fundamental principles and rules regarding data protection and privacy, and to ensure the reliability and integrity of such data and their free flow within the internal market of the European Economic Area.” The law is very comprehensive in that it includes, among others, the following sensitive and personal data:

- data on origin, skin color, race, political opinions, religious beliefs, and other life philosophies;
- data on criminal suspicion, indictment, prosecution, or conviction;
- health data;
- data on sex life and sexual behavior; and
- data on trade-union membership.

Its provisions are clearly delineated by Articles dealing with (a) risk analysis, security, and integrity of data; (b) internal audit; (c) rights of access; (d) notification of data usage; and (e) transfer of data to other countries that may or may not provide adequate data protection.

Malta  Malta’s Electronic Communications (Personal Data and Protection of Privacy) Regulations (SL 399.25) requires that if there is a significant risk of a breach of network
security or when the contents of communications have been unintentionally made known to other parties, the entity that provides the electronic communications services should inform the affected consumers of (a) that risk; (b) any remedies appropriate to afford safeguards against that risk the subscribers themselves might take; and (c) the costs involved in relation to such remedies. This regulation is a bit dated and, essentially, has not fully addressed computer data and its protection.

**Romania** Romania’s *Law no. 506/2004. Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* states that the provider of an electronic communications service must take appropriate security measures to safeguard its service. Further, the measures taken should ensure a level of security appropriate to the current risk and the state of the technology. In case of a particular risk of a breach on network security, the provider of the service must: (a) inform the subscribers of such risk and of the possible ensuing consequences; (b) inform the subscribers of any possible remedies; and (c) inform the subscribers of the likely costs involved by eliminating the risk. This law is very similar to Malta’s privacy protection law and should be amended and expanded.

**Singapore** Singapore has no dedicated or overarching legislation for privacy protection. However, personal information is protected under sector-specific laws such as the *Banking Act*, the *Statistics Act*, the *Official Secrets Act*, and the *Statutory Bodies and Government Companies (Protection of Secrecy) Act*.

**USA** Among the provisions of the *Health Insurance Portability and Accountability Act* (HIPAA) of 1996 is the protection of the privacy of personal health information. This ensures that all types of collected information are secured as they are transmitted in electronic form along a network of health care providers, insurers, clearinghouses, and payment processing centers. Compliance with this law entails, among others, the installation of access control mechanisms, intrusion detection and prevention systems, encryption systems, reporting systems, and a robust and secure network infrastructure.

The United States has passed its own consumer privacy protection laws to supplement existing federal laws. A representative sample taken from a comprehensive list is shown as follows:

- **Arizona SB 1338** requires notifying the customer of any breach in the security of unencrypted computerized personal information. A thorough investigation that deems that there is no likelihood of damage exempts the company from performing the notification.
- **California Civil Code Sec. 1798.82-84** requires that any business entity in the state must disclose any breach in system security that may compromise the unencrypted personal information of its customers.
- **Massachusetts Public Law 82-2007** states that an entity that maintains, stores, or owns data that includes personal information about a resident of the commonwealth should provide notice when such entity has reason to believe that the personal information of such resident was compromised.
- The states of Ohio (*HB 104*), Oklahoma (*Okla. Stat. 74-3113.1*), Oregon (*SB 583*), Michigan (*SB209*), and Tennessee (*HB2220*) have essentially the same requirements.
Wisconsin’s Wis. Stat. 895.507 law extends the characterization of private information to include DNA and biometric data.

Financial and Banking Services

International The Revised Framework on “International Convergence of Capital Measurement and Capital Standards” (also known as the new Basel Capital Accord or Basel II) represents a significant and complex best practice agreement that requires internationally active banking institutions to adopt risk management practices for tracking and publicly reporting exposure to operational, credit, and market risks.\(^9\) Essentially, Basel II is built on three main requirements: minimum capital to cover credit risk, supervisory review, and market disclosure of capital adequacy and intrinsic banking risks.

The Council of European Union adopted in June 2006 two directives that, in essence, adopted the Basel II agreement into EU law. The two directives are the recast Directive 2000/12/EC on the business of credit institutions and Directive 93/6/EEC on the capital adequacy of investment firms and credit institutions.


In Asia, the influence of Basel II is quite noticeable. All Malaysian banks started applying the Standardized Approach for credit risk and Basic Indicator Approach for operational risk in January 2008; most of the locally incorporated authorized institutions in Hong Kong have adopted the Standardized Approach for credit risk starting in January 2007; and the Monetary Authority of Singapore (MAS) started to implement Basel II for all Singapore-incorporated banks on January 1, 2008.

USA The Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act\(^11\) (GLBA), includes provisions to safeguard customer records and information held by financial institutions. The three principal parts to the privacy requirements of GLBA are the Financial Privacy Rule, the Safeguards Rule, and the Pretexting provisions. The Financial Privacy Rule requires financial institutions to give consumers privacy notices and to offer them the right to limit the sharing of their information. The Safeguards Rule requires all financial institutions to implement reasonable safeguards to protect customer information. This includes administrative, technical, and physical safeguards. The Pretexting provisions of GLBA essentially make it illegal to use fraudulent statements or instruments to obtain customer information from a financial institution or directly from its customer.

Electronic Commerce

Malta The Electronic Commerce Act of Malta\(^12\) (Cap 428) was enacted in 2002 and last amended in 2007. The Act requires the establishment of the validity of an electronic transaction; the acceptance of the equivalency of documents in electronic and written forms; the recognition of the legality of an electronic signature; the retention of electronic documents and communications; the formation of electronic contracts; the protection of the integrity
of electronic documents and communications; and the specifications of the responsibilities of service providers. This Act is closely aligned with the United Nations Commission on International Trade Law’s (UNCITRAL) work on the use of electronic communications in international contracts.

**Philippines** The authority of the implementation and promotion of the *Electronic Commerce Act of the Philippines* (Republic Act No.8792) is assigned to the Department of Trade and Industry. Among the provisions of the Act are the following: the development of a technology-aware workforce that will sustain electronic commerce; the promotion of electronic commerce through enhanced public awareness; the assurance of network security, connectivity, and technological neutrality; the legal recognition of electronic documents and signature; the responsibilities of service providers; and the protection of users’ rights to privacy, confidentiality, and anonymity.

The *Electronic Commerce Act of the Philippines* is also closely aligned with UNCITRAL’s *Model Law on Electronic Commerce,* which was expanded by the United Nations Commission on International Trade Law’s work on the use of electronic communications in international contracts in 2005.

**Singapore** Singapore’s *Electronic Transactions Act* (ETA) (Cap. 88) contains provisions that pertain to the following:

- Electronic contracts;
- Electronic records and signatures;
- Secure electronic records and signatures;
- Effect of digital signatures and duties relating to such signatures;
- Duties of Certification Authorities and their subscribers;
- Regulation of Certification Authorities;
- Government use of electronic records and signatures; and
- Liability of network service providers.

Singapore’s ETA follows closely UNCITRAL’s *Model Law on Electronic Commerce.*

**United Nations** In 2005, the United Nations Commission on International Trade Law (UNCITRAL) finalized its work on a convention that was formally entitled “The Convention on the Use of Electronic Communications in International Contracts.” The convention contains provisions that facilitate international electronic commerce. These provisions enable the two principles at the core of any electronic transaction’s legislation:

- Functional equivalence—paper documents and electronic transactions are treated equally by the law; and
- Technology neutrality—the law does not discriminate between different forms of technology.

The convention was formally adopted by the UN General Assembly on November 23, 2005, and has been open for signature since January 16, 2006. Prominent provisions that are
included in the convention are the legal recognition of an electronic contract; the acceptance of electronic communication as legally equivalent to a written form; the requirements for the integrity of an electronic signature and preservation of electronic documents; and the determination of time and place of dispatch of an electronic communication.¹⁷

**USA** There is no federal regulation that is specific to electronic commerce. Rules and regulations that apply to online retailers and service providers are found in other federal laws and regulations. For instance, the protection of customers’ privacy and security is required by GLBA. Children’s online privacy is protected by the *Children’s Online Privacy Protection Act (COPPA)*, whose basic requirement is a prominently visible privacy policy that explains what types of personal information are collected, how those data are being used, and whether those data are shared and with whom.¹⁸ Additional guidelines¹⁹ on how to comply with laws and regulations related to ecommerce in the United States are published by the U.S. Small Business Administration. The set of guidelines covers the protection of customer privacy, collecting sales taxes, selling internationally and exporting, online advertising and marketing, and digital rights and copyrights.

A very important component of ecommerce is online payment through credit cards. Payment account data security is self-regulated and is covered by a standard developed by the Payment Card Industry Security Standards Council. The standard, *Payment Card Industry Data Security Standard*²⁰ (PCI DSS), facilitates the broad adoption of globally consistent data security measures.

**Government**

**USA** The *Federal Information Security Management Act (FISMA)* applies to U.S. federal government agencies and requires them to provide security for both their information systems and the information that they use to support their operations.²¹ FISMA’s provisions fall into three major categories: assessment, enforcement, and compliance. Assessment pertains to determining the adequacy of the security of federal assets and operations. Enforcement requires that key information security management processes must be integrated with agency strategic and operational planning and execution processes. The third category compliance provisions for the management of each agency’s information security program and the accountability of each agency for compliance and reporting. In addition, FISMA requires the reporting of significant deficiencies; i.e., agencies must continuously identify and track material weaknesses and report any progress.

**Canada** The Canadian counterpart of the U.S. *Federal Information Security Management Act (FISMA)* is called the *Operation Security Standard: Management of Information Technology Security (MITS)*. It defines baseline security requirements that federal departments must comply with to ensure the security of information and information technology assets under their control.²² The standard defines and describes the roles and responsibilities of IT security personnel, the required departmental IT security policy, the management controls, the need for periodic IT security assessment and audit, and the importance of regular IT security training. Further, it provides guidance on technical and operation safeguards such as an active defense strategy, preventive tools and measures, detection of incidents, and response and recovery.
Publicly Traded Entities

USA The Sarbanes-Oxley (SOX) Act of 2002 was enacted by the U.S. Congress mainly to address the crisis brought about by the WorldCom and Enron debacle to the financial markets. The law is ratified to enforce accountability for financial record keeping and reporting of publicly traded corporations. The Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) are directly responsible for the completeness and accuracy of their institution’s financial reporting and record-keeping systems. The Public Company Accounting Oversight Board (PCAOB) is a private-sector, nonprofit corporation created by the Sarbanes-Oxley Act.

Australia The Corporate Law Economic Reform Program (CLERP), also known as Audit Reform and Corporate Disclosure Act 2004 or CLERP 9, governs corporate law in Australia. CLERP 9 requires companies to have adequate measures, processes, and procedures for auditing and company financial reporting. These requirements are embodied in four regulatory policies: auditor registration, disclosure for on-sale of securities and other financial products, reporting obligation of an auditor to the Australian Securities and Investments Commission, and transaction-specific disclosure.

Canada In 2004, the Canadian Securities Administrators (CSA) introduced a series of rules called Multilateral Instruments (MI), and National Instruments (NI) to closely align with the U.S. SOX Act and, with the same effort, to address the unique nature of the Canadian financial market. MI’s are securities rules that cover all Canadian provinces and territories, while NI’s are rules in force in each Canadian province and territory that elects to adopt those instruments.

European Union (EU) Directive 2004/109/EC of the European Parliament established the transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market or operated within a Member State. Important provisions of the Directive include the effective protection of investors and the proper operation of regulated markets; the designation of a single competent authority in each Member State to oversee compliance; the removal of barriers and the effective enforcement of controls; the transparency of the securities market through the disclosure of accurate, comprehensive and timely information about security issuers; and the mandatory reports required on issuers of securities on regulated markets.

Japan In June 2006, the Japanese legislative body passed the Financial Instruments and Exchange Law, which contains provisions that are unofficially referred to as the “J-SOX” requirements. Compliance is effective for fiscal years beginning on or after April 1, 2008. While this legislation in Japan is different from the contents of the U.S. Sarbanes-Oxley Act, the specific requirements are very similar to the Sarbanes-Oxley Act Sections 302 (Management Certification) and 404 (Management Evaluation and Report on Internal Controls). Among the provisions of J-SOX are that (a) management is required to evaluate the efficacy of its internal control for financial reports and draw up a report on it and (b) the external auditor who already carries out the audit for the financial reporting must also conduct an audit to determine the appropriateness of the management’s evaluation of the effectiveness of the internal control for financial reports.
General Population (Cyber Crime)

Norway  The Odelsting, a chamber in the Norwegian Parliament, recommended in March 2005 an Act amending the Penal Code and the ratification of the Budapest Council of Europe Convention on Cybercrime. The Act was enacted in April 2005 and entered into force and the ratification of the Budapest Council of Europe Convention on Cybercrime was made in November 2005. The amendment to Penal Code 145 includes a penalty for unlawful access to data or programs that are stored electronically. Penal Code 151 has been amended to include a penalty for destroying, damaging, or putting out of action any data collection instrument. The Budapest Council of Europe Convention on Cybercrime contains the remaining provisions for fighting cyber crime in Norway.

Pakistan  Pakistan has enacted its Electronic Crimes Act in 2006. The law includes deterrence against cyber attacks such spoofing, spamming, fraud, forgery, malicious code distribution and authoring, cyber stalking, and cyber terrorism. In addition, the federal government is given the broad power to collect electronically transmitted data in real time. Some very interesting provisions of this Act include life imprisonment for anyone who willfully defiles, desecrates, or damages the Quran or the prophet Mohammed.

USA  Laws against cyber crime in the United States are part of four major regulations:

- The Prosecutor Remedies and Tools Against the Exploitation of Children Today Act (PROTECT Act)
- The Homeland Security Act of 2002
- The USA Patriot Act of 2001
- The US Code Title 18 Part I Chapter 47 Section 1030 “Fraud and Related Activity in Connection with Computers”

The Patriot Act contains the Computer Crime and Intellectual Property Section (CCIPS), which includes the authority to intercept voice communications; the facility to obtain voice mail and other stored voice data; allowing the use of a subpoena for collecting electronic evidence; utilization of pen/trap orders to intercept evidence; and deterrence and prevention of cyberterrorism.

Case Studies

Privacy Protection/Health Care Regulations

In October 2003, workers in Bangalore, who are employed by an outsourcing company in Ohio, threatened to reveal confidential medical records unless they received financial payoff. A similar threat was received by the University of California in San Francisco (UCSF) Medical Center just three weeks earlier from a Pakistani woman who was transcribing the hospital’s files.

The above incident puts a serious doubt on the safe handling of customers’ confidential information by outsourcing companies located abroad. A nonprofit public interest organization, Public Citizen, publicly exposed the inadequacy of the U.S. law regarding privacy protection