Chapter 22
Trends in Information Security Regulation

Christopher A. Canning
Carnegie Mellon University, USA

Baoying Wang
Waynesburg University, USA

ABSTRACT

This chapter reviews regulations and laws that are currently affecting information assurance and security policy in both the public and private sectors. Regulations and laws in different areas and at different levels are considered. Important industry sector regulations are also included when they have a significant impact on information security, such as the Health Insurance Portability and Accountability Act (HIPAA). Analysis of these regulations including evaluation of their effectiveness, enforceability, and acceptance is presented. Since the regulations in this field are in a state of continuous fluctuation, this chapter also attempts to make proposals for statutory improvements that would make security policy development more comprehensive and consistent, resulting in more secure systems throughout the world. It is also predicted that there will be a need for international information security regulations given the nature of the worldwide internet and cross-border information systems. Such developments will improve digital crime investigations worldwide.

INTRODUCTION

Laws and regulations are used to create legal obligations and define crimes. Information security concerns have prompted legislation and regulations at different levels and in different sectors to enforce legal practices and to define digital crimes. The results of digital investigations are often used as evidences whether there are guilty acts according to information security regulations. Because the importance of information increases on a daily basis to both government and the economy, securing data is becoming increasingly necessary in various sectors. While progress has been made towards a well-defined set of

DOI: 10.4018/978-1-60566-836-9.ch022

Copyright © 2010, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

best practices for managing information security, the media frequently reports about the failures of such practices. Since legislation typically lags behind technology developments, it should come as no surprise that information security regulations are not up-to-date, but progress must continue.

This chapter reviews the history of information security legislation, analyzes current information security regulations, and proposes improvements for the future information security regulations. Because of the piecemeal nature of today's information security regulations, they are difficult to implement, enforce, and understand. A piecemeal policy is one that is developed over time by different legislative and regulatory bodies instead of being created and implemented at one time by one governmental body or organization. As a result, some professionals attempted to compose "a compliance model that incorporates all the guidelines, standards, legislations and best practices for the financial sector" (Maphakela, Pottas, & von Solms, 2005, p. 2). However, we believe that by establishing laws that are well-defined, enforceable, and wide-ranging, a national government or an international organization would help to make cybersecurity an attainable objective. With an increasing reliance on information technologies, ensuring the success of information security is undoubtedly a critical stepping stone in ensuring overall national and international security. Given the nature of the worldwide Internet and cross-border information systems, there will soon be a need for international information security regulations to assist governments in their investigations of digital crimes.

BACKGROUND

There are many laws and regulations on security information issued at different levels in different countries all over the world. In Europe, for instance, there are the Computer Misuse Act 1990, UK Data Protection Act 1998 and the European Union Data Protection Directive (EUDPD) 95/46/EC. The Computer Misuse Act 1990 is an act of the UK Parliament which made computer related crime a criminal offence. The Act has inspired several other countries to draft their own information security laws. The UK's Data Protection Act 1998 regulates the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. All European Union members are required to adopt national regulations to standardize the protection of data privacy for citizens throughout the European Union. The European Union Data Protection Directive 95/46/EC relates to the protection of individuals with regard to the processing of personal data and on the free movement of such data. This legislation has had a wide-ranging effect, both in the European Union and around the world because of its provisions allowing "transfers of personal data . . . only to non-EU countries that provide an 'adequate' level of privacy protection" (U.S. Department of Commerce, 2000). To keep information flows active between the European Union and the United States, the U.S. Department of Commerce negotiated Safe Harbor provisions to allow certain companies to transfer information if certain provisions are upheld. The nation of South Africa has felt the effects of legislation such as the "Basel Accord; Sarbanes-Oxley; FICA (Financial Intelligence Centre Act); Banks Act; ECT Act (Electronic Communication and Transaction Act); Gramm-Leach-Bliley Act; and others, have been created to help companies understand their rights and responsibilities among board members, business and IT managers." (Maphakela, Pottas, & von Solms, 2005, p. 2)

Within the United States, there are essentially four federal laws with a major impact on information security: the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley Act (SOX), and the Federal Information Security Management Act

11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/trends-information-security-regulation/39232

Related Content

Models for the Detection of Malicious Intent People in Society
Preetish Ranjan, Vrijendra Singh, Prabhat Kumarand Satya Prakash (2018). *International Journal of Digital Crime and Forensics (pp. 15-26).*
www.irma-international.org/article/models-for-the-detection-of-malicious-intent-people-in-society/205520

Consequences of Corruption on Economy, Politics, and Society: The Case of India
Asim Kumar Karmakar, Priyanthi Bagchiand Somnath Karmakar (2023). *Theory and Practice of Illegitimate Finance (pp. 54-67).*
www.irma-international.org/chapter/consequences-of-corruption-on-economy-politics-and-society/330623

Testing Digital Forensic Software Tools Used in Expert Testimony
Lynn M. Battenand Lei Pan (2010). *Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions (pp. 257-278).*
www.irma-international.org/chapter/testing-digital-forensic-software-tools/39221

Task Offloading in Cloud-Edge Environments: A Deep-Reinforcement-Learning-Based Solution
Suzhen Wang, Yongchen Dengand Zhongbo Hu (2023). *International Journal of Digital Crime and Forensics (pp. 1-23).*
www.irma-international.org/article/task-offloading-in-cloud-edge-environments/332066

Research and Application of Warship Multiattribute Threat Assessment Based on Improved TOPSIS Gray Association Analysis
Dongmei Zang, Xinlei Sheng, Liya Wang, Aimin Yang, Tao Xueand Jie Li (2022). *International Journal of Digital Crime and Forensics (pp. 1-14).*
www.irma-international.org/article/research-and-application-of-warship-multiattribute-threat-assessment-based-on-improved-topsis-gray-association-analysis/315288