Category: Concepts, Trends, and Challenges

Information Security for Legal Safety

Andreas Mitrakas
European Network and Information Security Agency (ENISA), Greece

INTRODUCTION

The growing use of information technology in sensitive daily transactions highlights the significance of information security to protect information assets. Vulnerabilities associated with public and private transactions pose challenges that government, private organizations, and individuals are compelled to respond to by adopting appropriate protection measures. Information security responds to the need of transacting parties for confidentiality, integrity, and availability of resources (Pfleeger, 2000). Information security is required in transactions carried out among, businesses, public administrations, and citizens. An organizational response to information security threats includes setting up and implementing appropriate policy frameworks that are typically endorsed by agreement. Beyond organizational objectives lies an emerging legal framework instigated by the role of information security as a means to safeguard information assets that are socially significant. Organizations are often required to implement information security measures mandated by industry regulations or legislation, such as in electronic banking transactions. The scope of these legal and regulatory requirements is to mitigate potential risk that entails liabilities for shareholders, employees, customers, trading partners, or other third parties involved in a transaction. Information security and its subsequent regulation are equally important for public services. In e-government services made available to citizens and businesses, information security ensures e-government transactions. The remainder of this article presents an overview of the prevailing legal and policy issues that are currently associated with information security.

BACKGROUND

Electronic transactions typically require a high level of assurance with respect to the content and management of the transaction, the authentication of the trade partners, threats against enterprise resources, and so forth. The following presents a brief and non-exhaustive overview of the regulatory background on information security. If not properly treated, security risks may nurture liability risks for the parties who fail to adopt security countermeasures. Liability in this regard might emanate from general legal requirements or as it has become increasingly apparent from specific legislation that addresses specific security matters. The evidential value of electronic documents, for example, can be challenged as long as the contents of the transaction and the conditions under which it was carried out cannot be ascertained (Mitrakas, 1997). Information security can also function as negative proof of actions that are under investigation in a digital forensics process.

The *U.S. National Information Systems Security Glossary* defines information security as "the protection of information systems against unauthorized access to or modification of information, whether in storage, in processing, or in transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats" (1992, p. 38). Information security threats can be distinguished in categories such as the following:

- **Natural threats**, which are described by terms such as *acts of God*, sometimes described as *force majeure*; for example, unforeseen events such as a flood or an earthquake.
- **Accidental threats** caused by the actors involved, such as, for example, missing out in a plan or a procedure.
- **Intentional threats** by actors directly or indirectly involved, such as, for example the deletion of data with the intent to transfer funds without authorization.

Although threats might carry liability or criminal consequences to the implicated parties, the basis for information security in law is the legal duty of care that transacting parties must show in their daily or business dealings (Lindup & Lindup, 2003). The duty of care is yet more significant in situations where a party acts under a certain capacity or in a trade. There are situations, however, whereby the law mandates certain information security measures in order to protect against information threats, such as, for example, in the case of processing personal data. In such cases, there is a set of duties of the implicated

Copyright © 2006, Idea Group Inc., distributing in print or electronic forms without written permission of IGI is prohibited.

personal data controller to implement security safeguards on personal data stored or processed (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of personal data and on the free movement of such data, p. 31).

Information security objectives must be associated with the acts at hand and strive to detect the implementation of the following principles with the evidence in hand:

- Confidentiality ensuring that information is accessible only to those authorized to have access, according to the International Standards Organization (ISO). Confidentiality is typically ensured through encryption.
- Integrity is the condition that exists when data are unchanged from their sources and have not been modified, altered, or destroyed at any operation according to an expectation of data quality.
- Availability of data is the degree to which a system is operable and in a committable state at the start of an assignment.
- Accountability of parties involved for acts performed being held to account, scrutinised, and required to give an account. Especially in white collar crime, accountability is often associated with governance.

Whereas the aforementioned principles might only be fully observed within highly organized environments that operate on the basis of audited security policies and practices (e.g., in white-collar crime investigated in a corporation) in other less organized environments odd data has to be put in context through social methods and mundane practices to pinpoint actions in the crime under investigation. To determine information security measures, it is typically required that a risk assessment is carried out by measuring two quantities of risk the magnitude of the potential loss, and the probability that the loss will occur. Prior to a risk assessment, it is advisable to carry out a vulnerability assessment by identifying and quantifying vulnerabilities in a system that seeks network and information security measures (Dunn & Wigert, 2004).

Information security is an enabler to ascertain basic rights, such as the right to confidentiality, personal data protection, trade secrets, and so forth. In information society, information security is gradually becoming a significant factor upon which basic rights depend in order to be exercised by all members of the society. Information security as such is not a right in itself; there is no such thing as a right to information security. This article argues that although information security is an instrument to exercise and enjoy other basic rights and freedoms, it should be encouraged and afforded protection in a meaningful way (Dworkin, 1977). Within the European Union, internal market rules that sometimes depend on information-society services rely on information security in order to take meaningful effect. Conditions regarding the encouragement and exercising of information security include, for example, exceptions with regard to crime investigation through digital forensics, lawful interception, and so forth. A balance, however, must be sought to ensure that legitimate users are granted sufficient access to information security resources and that they are not unnecessarily constrained in the choice of information security resources that evolved over time. The commercial use of public networks has resulted in a surge of regulation concerning an array of issues, among which information security plays a lynchpin role (Rathmell & Valeri, 2002). It is important to stress that information security regulation is twofold in the following situations:

- Addressing risks associated with an attacker carrying out an illegal act, such as hacking or spreading viruses.
- Setting out the requirements for the party that is attacked to take out appropriate measures mitigating risks or face the consequences.

LEGAL CONSIDERATIONS

Information security has emerged as a legal requirement in order to ensure, for example, the legitimate use of computer resources; protection against cyber-crime, and compliance in critical areas such as electronic signatures, personal data protection, and so forth. At an international level, the legal framework of information security includes the UNCITRAL Model Law on Electronic Signatures (United Nations, 2001), which recommends that countries adopt laws allowing the enforceability of electronic signatures, subject to a risk assessment with regard to reliability and trustworthiness. Similarly, the OECD Information Security Guidelines (2002) aim at creating a culture of security by effectively managing risk (Ward, 2003). When carrying out risk assessments, it is necessary to consider legal risks in the audit processes.

Information security is necessary to control risk in transactions. An information security approach and information security rules allow for the assessment of threats and mitigation of risk. Whereas a threat is the possibility of hindering the operation of an information system, risk is the probability that a threat might materialize. The principles of proportionality and reasonableness have been enshrined in the EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Privacy protection requires the setup of discreet

4 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/information-security-legal-safety/12603

Related Content

E-Health Security and Privacy
Yingge Wang, Qiang Chengand Jie Cheng (2006). *Encyclopedia of E-Commerce, E-Government, and Mobile Commerce (pp. 385-390).*
www.irma-international.org/chapter/health-security-privacy/12567

Challenges of Transforming a Traditional Brick-and-Mortar Store into a Bricks-and-Clicks Model: A Small Business Case Study
Irvine Clarke IIIand Theresa B. Flaherty (2004). *Journal of Electronic Commerce in Organizations (pp. 75-89).*
www.irma-international.org/article/challenges-transforming-traditional-brick-mortar/3442

Can Virtual Customer Service Agents Improve Consumers' Online Experiences?: The Role of Hedonic Dimensions
Ana Maria Soares, José Carlos M. R. Pinho, Teresa Heathand António Alves (2021). *Research Anthology on E-Commerce Adoption, Models, and Applications for Modern Business (pp. 764-780).*
www.irma-international.org/chapter/can-virtual-customer-service-agents-improve-consumers-online-experiences/281534

Reverse Auction Impact on Mining Company
Radoslav Delinaand Anton Lavrin (2006). *International Journal of Cases on Electronic Commerce (pp. 61-84).*
www.irma-international.org/article/reverse-auction-impact-mining-company/1492

The Naming of Corporate eBrands
Tobias Kollmann (2009). *Contemporary Research in E-Branding (pp. 48-60).*
www.irma-international.org/chapter/naming-corporate-ebrands/7059