Chapter 4.49
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 liabil-

ity 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 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