Chapter 13
Do We Need Security Management Systems for Data Privacy?

Wolfgang Boehmer
Technische Universität Darmstadt, Germany

ABSTRACT

The importance of personal data and managing them is increasing worldwide. However first, one must be able to distinguish between data, information, and knowledge, before one turns to protecting them. Furthermore, it must be considered that, in open systems, security is a relative term and can be characterized only with the term risk. This suggests that security is not a state in open and dynamic systems but can only be maintained on a pre-defined level (conservation status) with a security management system. Data privacy therefore requires security management systems to ensure sustainable protection at a previously defined level. Pure guidelines and policies are just not sufficient for the protection of data in open systems, as is typical in companies.

INTRODUCTION: THINKING IN SYSTEMS

This contribution can be classified thematically to the field of Security Engineering. This assignment is based on both computer science and engineering alike. For this assignment, Ross Anderson provided an apt definition in his eponymous book.

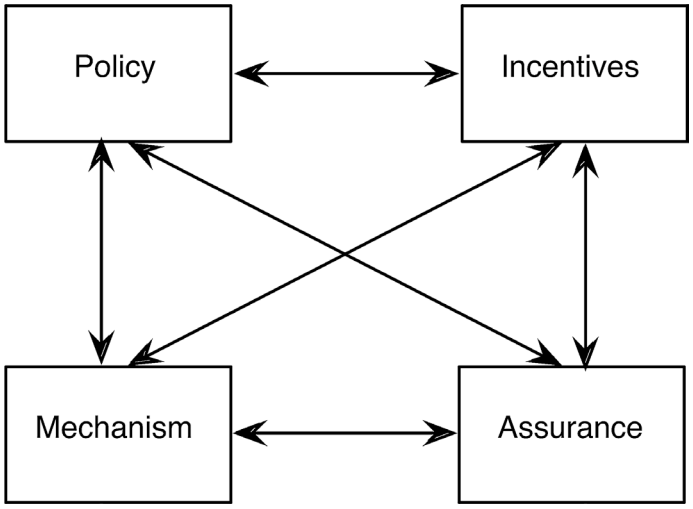
Security Engineering is about building systems to remain dependable in the face of malice, error, or mischance. As a discipline, it focuses on the tools, processes, and method needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves (Anderson, 2008).

From the view of R. Anderson (2008), four interacting components are addressed, which are illustrated in Figure 1. Firstly, a policy is postulated that describes what can be achieved. On the other hand, so-called mechanisms are required in response to this that is necessary to enforce the policy. This could, for example, be cryptographic protocols, access configuration and access arrangements, tamper-resistant hardware, etc.

DOI: 10.4018/978-1-4666-7381-6.ch013

Copyright © 2015, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Figure 1. Security engineering framework based on policies (Anderson, 2006).



The third component is the assurance in these mechanisms, according to Anderson (2008), or the security, which is provided, by these mechanisms and the last component is addressed by the incentives. He considers the incentives from two perspectives. Firstly, from the perspective of the persons who want to protect themselves and secondly the group of people who try to circumvent these mechanisms in an unauthorized manner.

It is an interactive system, as illustrated by the cross-references (arrows) between the components.

A significant disadvantage of policies becomes apparent if they alone are used to secure the value chain of a company. This disadvantage is that the policies do not provide feedback about their effects. Especially in an open system such as a company, this lack of response has proved to be a disadvantage.

To assess the overall security of a company, it is invaluable to obtain feedback on security status, for only then can an adequate response be generated if necessary. As a suitable method for complete protection of a company, standardized management systems based on systems theory have become the established practice. Based on the desire for complete security, for example in terms of the value chain, a universal framework for a risk-oriented management system can be outlined.

The framework is illustrated in Figure 2 based on the concept of systems theory. It is dominated by adjustments in response to perturbations (deviations) and shows policies and procedures as the dependent variables of the control loop. A disturbance will, in most cases, affect the value chain of the company. This point of view is aligned with overall enterprise security rather than with individual components.

Security is seen to be one facet of Quality of Service (QoS) and to include classical security goals such as confidentiality, availability, and integrity. All components of the framework are in constant interaction with each other. The aim of the management system as implemented is to adjust for deviations proactively; this is a typical case for an Information Security Management System (ISMS). However, if the risk decision for a specific deviation is to act reactively after the occurrence of the deviation, this is a typical task for a Business Continuity Management System (BCMS) argued Boehmer (2009b).

35 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/do-we-need-security-management-systems-for-data-privacy/123537

Related Content

An Overview of Recent Development in Privacy Regulations and Future Research Opportunities
Tawei Wangand Yen-Yao Wang (2021). *Research Anthology on Privatizing and Securing Data (pp. 1-14).*
www.irma-international.org/chapter/an-overview-of-recent-development-in-privacy-regulations-and-future-research-opportunities/280167

KYC Fraud: A New Means to Conduct Financial Fraud – How to Tackle It?
Vijaya Geeta Dharmavaramand Oly Mishra (2023). *Cybersecurity Issues, Challenges, and Solutions in the Business World (pp. 81-94).*
www.irma-international.org/chapter/kyc-fraud/313860

The Social Organization of a Criminal Hacker Network: A Case Study
Yong Lu (2009). *International Journal of Information Security and Privacy (pp. 90-104).*
www.irma-international.org/article/social-organization-criminal-hacker-network/34061

Establishment of Enterprise Secured Information Architecture
Shyh-Chang Liuand Tsang- Hung Wu (2012). *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions (pp. 316-325).*
www.irma-international.org/chapter/establishment-enterprise-secured-information-architecture/63097

Hybrid Intrusion Detection Framework for Ad hoc networks
Abdelaziz Amara Korba, Mehdi Nafaaand Salim Ghanemi (2016). *International Journal of Information Security and Privacy (pp. 1-32).*
www.irma-international.org/article/hybrid-intrusion-detection-framework-for-ad-hoc-networks/165104