Chapter VIII

Implementing IT Security for Small and Medium Enterprises

Edgar R. Weippl, Vienna University of Technology, Austria
Markus Klemen, Vienna University of Technology, Austria

Abstract

Small and medium enterprises (SMEs) increasingly depend on their information technology (IT) infrastructure but lack the means to secure it appropriately due to financial restrictions, limited resources, and adequate know-how. For many managers in SMEs, IT security in their company is basically equivalent to having a firewall and updating the antivirus software regularly. Strategic policies, information theft, business continuity, access controls, and many other aspects are only dealt with in case of security incidents. To improve security in a company holistically, four levels (organizational level, workflow level, information level, and technical level) need to be addressed. Parts of existing standards are useful to address issues on the organizational level; Pipkin’s approach is especially useful for SMEs. Modeling of business processes and taking security/dependability into account can improve reliability and robustness of the workflow level. On the information level, role-based access control is state-of the art. On the technical level, basic security measures (antivirus software, firewalls, etc.) need to be addressed and aligned with a corporate security policy.
**Introduction**

In most countries, small and medium-sized enterprises employ far more people than large corporations and are an important and often underestimated economic factor. For both large companies and SMEs, business success depends increasingly on reliable IT infrastructure. That said, new e-commerce technologies offer great opportunities and chances, especially for SMEs, but they also pose novel IT-related risks that so far have not been addressed with the necessary vigilance. In this context, we define “SMEs” as companies employing not more than 400 employees.

In comparison to large corporations, SMEs typically have fewer resources and less expertise in strategic and operational IT security policies and tasks. Their IT infrastructure is either maintained by one or very few employees, usually with limited know-how regarding IT security, or by small IT service companies, most of which are not accustomed to even consider using information security standards — such as Control Objectives for Information and related Technology (COBIT) or Common Criteria — due to various reasons. We will address this problem later in this chapter.

According to Avizienis, Laprie, Randell, and Landwehr (2004), security encompasses the aspects of availability, confidentiality, and integrity. The main attributes of dependability are availability, reliability, safety, integrity, and maintainability. In this chapter, we will address security and some aspects of dependability on all four layers mentioned before. On the organizational level, security strategies are developed and a corporate security culture has to be established. The second level is the workflow level. Day-to-day core business processes need to be aligned with the company’s security strategy. In addition, IT administrators need this guidance to know which information and technical infrastructure needs to be secured. Protecting information against unauthorized access is addressed on a logical level, the information level. Security on the technical level encompasses aspects such as network security, antivirus software and hardware dependability.

---

**Figure 1. A holistic approach to security encompasses four levels within SMEs**

<table>
<thead>
<tr>
<th>Security Layer</th>
<th>Security-related Research Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Organisational Level</td>
<td>Decision-making processes under uncertainty, IT-Security strategies, Corporate Security Culture, Risk Management</td>
</tr>
<tr>
<td>2. Workflow Level</td>
<td>Security Workflows: Integration of standardized security workflow methodologies; Development of secure business processes</td>
</tr>
<tr>
<td>3. Information Level</td>
<td>Access Control, User Rights, Federal Identity (Single-Sign-on)</td>
</tr>
<tr>
<td>4. Infrastructure Level</td>
<td>Classical Security Aspects: Secure Networks, Hardware, Tempest, Sniffer, Trojans, viruses, vulnerabilities</td>
</tr>
</tbody>
</table>

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

Application of the Big Data Grey Relational Decision-Making Algorithm to the Evaluation of Resource Utilization in Higher Education

RFID Adoption: Issues and Challenges
[www.igi-global.com/article/rfid- adoption-issues-challenges/3947?camid=4v1a](www.igi-global.com/article/rfid-adoption-issues-challenges/3947?camid=4v1a)

Relational Dynamics and Outcomes in Small and Large Service Organizations
[www.igi-global.com/chapter/relational-dynamics-outcomes-small-large/74477?camid=4v1a](www.igi-global.com/chapter/relational-dynamics-outcomes-small-large/74477?camid=4v1a)
Collaborative Systems for Decision Making for Disaster Preparedness and Response,
Department of Information Systems
Deidre Hahn, Jessica Block, Mark Keith and Ajay Vinze (2010). *Always-On Enterprise
Information Systems for Business Continuance: Technologies for Reliable and Scalable Operations* (pp. 41-57).
www.igi-global.com/chapter/collaborative-systems-decision-making-
disaster/36590?camid=4v1a