IT Security Strategies for SME’s

Ji-Yeu Park¹, Rosslin John Robles¹, Chang-Hwa Hong¹, Sang-Soo Yeo², Tai-hoon Kim¹
¹School of Multimedia, Hannam University, Daejeon, Korea
²BTWorks Inc, Seoul, Korea
rosslin_john@yahoo.com, ssyeo@btworks.co.kr, taihoonn@hannam.ac.kr

Abstract

Small and medium enterprises (SMEs) is leaning more on their information technology (IT) infrastructure but they lack the means to secure it appropriately due to financial restrictions, limited resources, and adequate know-how. Many SME managers believe that 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.

Keyword : IT Security, e-Enterprise Management, SME’s Management, Secure Infrastructure

1. Introduction

Small and medium-sized enterprises employ far more people than large corporations and are an important and often underestimated economic factor in many countries. 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.
2. SME's and Large Companies

In highly competitive global markets, SMEs usually are only successful if they provide highly customized solutions for their customers. The knowledge of their customers is also emphasized by the management style of many SMEs. Many SMEs are operated as family businesses managed by their founders or their descendants. Even though the management usually knows a lot about their customers and their core business, they often lack a systematic approach of organizing their business processes. In many cases, the management of SMEs does not see their company as a likely target for hacker attacks or intruders. Therefore, they deem IT security low priority. This is a very dangerous misconception of the evolving threats to modern IT infrastructure. Another aspect, which is often underestimated, is industrial espionage. Since know-how is the most important asset of SMEs, proper safeguards have to be taken to protect this asset from intruders as well as from malicious or disgruntled employees or former employees. This fact becomes even more evident as the IT infrastructure used by many SMEs offers services similar to large companies, such as Internet access on every work desk, remote access for home workers or traveling salesmen, distributed databases, or simple ERP and CRM systems. However, as SMEs usually spend less money — both in absolute and relative figures — on IT management and information security; they are much less prepared for potential attacks from outside or inside.

<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,</td>
</tr>
<tr>
<td></td>
<td>Corporate Security Culture, Risk Management</td>
</tr>
<tr>
<td>2. Workflow Level</td>
<td>Security Workflows; Integration of standardized security workflow</td>
</tr>
<tr>
<td></td>
<td>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,</td>
</tr>
<tr>
<td></td>
<td>Tempest, Sniffer, Trojans, viruses, vulnerabilities</td>
</tr>
</tbody>
</table>

Fig. 1 An approach to security encompasses four levels within SMEs

3. Organization

While large companies often invest a large amount of resources in the organizational aspects of IT security, the management of small- and medium-sized companies usually ignores these areas. This is a serious problem, because despite the smaller hierarchy and manageable organizational structure, a missing strategy and proper documentation leaves many important questions unasked. A corporate security culture would be an important strategic guideline for the day-to-day operational security-related decisions of IT administration personnel, who otherwise have to make decisions in an ad-hoc manner and without a coherent strategy. In contrast to large companies, SMEs rarely develop strategic policies; written IT security policies and even system documentation are often nonexistent.
Therefore, a clear strategic guideline that would help administrative personnel to properly assess the role and importance of IT security as seen by senior management is missing.

3.1 IT Security Standards for SMEs

3.1.1 Established Standards Most Information Security Frameworks were originally developed either for large corporations or governmental institutions to establish or keep a certain level of service quality and security. Therefore, a more pragmatic approach is needed that covers all areas that need to be addressed, but which is still feasible for companies with low IT budgets.

3.1.2 A Pragmatic Approach for SMEs Donald Pipkin (2000) developed an interesting approach that — with a few modifications — is very suitable for smaller companies, even though it was originally developed for large corporations. Pipkin suggests an Information Security process model consisting of five aspects: (1) inspection, (2) protection, (3) detection, (4) reaction, and (5) reflection.

3.2 Stakeholders

IT security policies in SMEs must consider not only the requirements of information security from a technical perspective, but also psychological and social factors (Anderson, 2001), which influence the role of information security policies in companies. The main stakeholders in an established, typical SME can be identified as the Decision maker (upper management or owner), IT administrator, User and External consultants.

3.2.1 External Consultant

External Consulting security experts and arranging security audits can be viable schemes to reduce the potential risks from only having one or few IT administrative personnel or being supported by a single IT service company. Since external consultants can be easily perceived as a sign of management distrust of its employees, it is important to achieve the administrators’ goodwill for the consultants’ engagement. That said, combining the introduction of external consultants with training programs for the employees can reduce the risk of internal resistance to an external auditing program. Also, the results of an audit always have to be presented as suggestions for enhancement and not as criticisms of the personnel’s achievements. Having security audits on a regular basis, for example, once or twice a year, can significantly and effectively reduce the dependability of the IT administrators.

Another advantage to this is the ability of the auditing company to help out in case of a sudden drop-out of a key employee, e.g., due to a car accident, sudden illness, or resignation on short notice. This might otherwise put the company in a difficult and vulnerable state for quite a long time.

Changes in the IT administration staff present perfect opportunities to introduce a trusted third party into the IT security policy of a company. A new employee is not yet accustomed to the company and will, therefore, accept a controlling and consulting authority easier. A concrete scheme for realizing the integration of a trusted third party is as follows: the
administrators receive all the necessary user rights to fulfill all their tasks in the role of system operator. Some rights are revoked, especially those that would facilitate the manipulation of logging mechanisms.

![Diagram](https://via.placeholder.com/150)

**Fig. 2 Integrating a trusted third party**

### 3.2.2 IT Administrator

In SMEs, administrators are responsible for almost all technical issues. Changing laser printer toner, assigning and modifying user rights in operating systems, setting up and maintaining Internet connections, and in many cases even designing the Web pages of the corporate Web site are often among their responsibilities. Since administrators have so many responsibilities, they often neglect security. Security is not easily visible and therefore often not rewarded appropriately by management; engagement in security is sometimes even hindered or at least ridiculed. Usually security aspects receive higher priority only after the company has been hit by a serious incident. Regarding the amount of available IT personnel resources, the following three scenarios are most common:

1. **No dedicated administrator:** One of the employees manages the IT network in addition to his or her normal duties. This scenario is usually characterized by a fuzzy assignment of responsibility, missing policies, and minimal security safeguards. Financial investments in IT security are only considered after major incidents like a hacking attack or a loss of data due to non-existing backup strategies.

2. **One dedicated administrator:** This maximizes management’s dependency of the administrator. The same problem basically applies to a scenario in which an external administrator or IT service company is assigned to fulfill the necessary IT administration tasks.

3. **More than one dedicated administrator:** This reduces the dependency of a single administrator and allows mutual controlling and overlapping responsibilities.
3.2.3 IT User

An estimated 77% of information theft is caused by company employees (Cox, 2001). In SMEs, access control and logging mechanisms are generally less strict and the threat of information loss due to insiders is often neglected. The introduction of substantial restrictions of user privileges like Web surfing, private e-mailing, or individual desktop settings like backgrounds, cursors, or sounds, at once is usually not an appropriate step to increase the level of IT security in a company. On the contrary, this can induce passive resistance of the employees to security safeguards and thereby even reduce the overall security level. Therefore, even after a major security incident, new restrictions should be applied with care.

The reasons for the restrictions should be communicated to the employees. Getting a sense of the threats that are addressed by new restrictions might help to develop a better understanding and support of the employees. In the end, it is usually user interaction that opens the door for external intruders. For example, clicking to open an attachment containing dormant malicious code, following links to a hacker’s Web site or downloading a Trojan horse. Therefore, gaining employee understanding and support for an improved IT security policy is paramount to increase the overall IT security level significantly. This human factor is much too often overlooked or neglected.

4. Workflow

Large corporations make more and more use of workflow management tools to optimize their core business processes. Today, even small- and medium-sized businesses are increasingly process oriented. Despite their ad-hoc way of addressing upcoming problems, most businesses explicitly or implicitly define their main business processes. In the context of security, we have two major aspects of workflows: security and dependability of workflows; and security and dependability workflows.

4.1 Security and Dependability of Workflows

Systems that implement business processes evolve over time. This evaluation can be organized in a simple two-life cycle consisting of a development phase and a use phase. During the development phase, the following entities have to be taken into account to ensure dependability: the physical world, human developers, development tools, and test facilities. The use phase is influenced by the physical world, administrative personnel, users, service providers, infrastructure, and unauthorized outsiders.

4.2 Security and Dependability of Workflows

Systems that implement business processes evolve over time. This evaluation can be organized in a simple two-life cycle consisting of a development phase and a use phase. During the development phase, the following entities have to be taken into account to ensure dependability: the physical world, human developers, development tools, and test facilities. The use phase is influenced by the physical world, administrative personnel, users, service providers, infrastructure, and unauthorized outsiders.
5. Information Level

One of the fundamental security concepts of role-based access control (RBAC) is separation of duty. It provides enhanced capabilities to specify and enforce enterprise policies compared to existing access control standards. Static separation of duties (SSD) is based on user-role membership. It enforces constraints on the assignment of users to roles. This means that if a user is authorized as a member of one role, the user is prohibited from being a member of a second role. Dynamic separation of duties (DSD) is based on role activation. It is employed when a user is authorized for more roles that must not be activated simultaneously. DSD is necessary to prohibit a user to circumvent a policy requirement by activating another role.

![Diagram of RBAC](image.png)

Fig. 3 Constraints in RBAC allow the implementation of separation of duty

6. Securing Infrastructure

In this section, we only provide a very brief overview since security is usually addressed adequately at the technical level, even in SMEs. For a couple of years now, viruses, worms, and Trojan horses are omnipresent; hence, most companies have installed antivirus software and firewalls. Administrators are usually knowledgeable about basic technical security safeguards. SMEs often provide solutions for large companies. As IT solution providers, they face two challenges. First, they need to secure their own infrastructure. Second, they need to secure the solutions they install at client sites.

7. Conclusion

Security needs to be addressed at four levels (organizational level, workflow level, information level, and technical level). SMEs differ from large companies in many aspects. These differences explain why IT security is usually not that well addressed in SMEs, even though SMEs increasingly depend on their IT systems as much as large companies do. Additionally, SMEs may be more often attacked in the future, as large companies become increasingly difficult to hack.
References


Acknowledgement

This work was supported by a grant from Security Engineering Research Center of Ministry of Knowledge Economy, Korea
Authors

Rosslin John Robles
He received his B.S. in Information Technology from Western Visayas College of Science and Technology, Philippines. He is currently a Multimedia integrate Masters-Ph.D. Student at Hannam University, Korea. His research interests are Software Engineering and IT Security.

Ji-Yeu Park
She is currently a Multimedia Student at Hannam University, Korea. Her research interests are Network Security and Software Security.

Sang-Soo Yeo
He received B.E., M.E., and Ph.D. degrees from Chung-Ang University in 1997, 1999, and 2005 respectively. After that, he worked at Dankook University from March, 2006 to February, 2007. He is currently a visiting scholar of Kyushu University, Japan. His main research areas are system security, cryptographic protocols, embedded system securities.

Tai-hoon Kim
He received B.E., M.E., and Ph.D. degrees from Sungkyunkwan University. Now he is a professor, School of Information & Multimedia, Hannam University, Korea. His main research areas are security engineering for IT products, IT systems, development processes, and operational environments.