Case study

Developing

A Security Policy

For electronic commerce organizations

& Comments
## Table of Contents

Table of Contents .................................................................................................................................2
1. Introduction ..................................................................................................................................3
2. Define Security Policy .................................................................................................................3
3. Nature of electronic commerce organisations..............................................................................3
4. Top down approach......................................................................................................................3
5. Security Principles .......................................................................................................................4
6. Purposes of a Security Policy .....................................................................................................4
7. Security Policy Communication .................................................................................................4
8. Holistic Security ..........................................................................................................................4
9. Security Stance ...........................................................................................................................5
10. Recommended Development Method ......................................................................................5
11. Data Centric Approach ..............................................................................................................5
12. Implementation in IT Systems ...................................................................................................5
13. Consequences of Manage Data Improperly ............................................................................5
14. Policy Flexibility ......................................................................................................................5
15. Policy Management ..................................................................................................................6
Conclusion ...........................................................................................................................................6
Comments ............................................................................................................................................7
References ...........................................................................................................................................8
1. Introduction

This case study analyses the issues faced by Sun Microsystems (SM) in developing a security policy for electronic commerce organisations and then suggests some comments. After the introduction, this case study defines security policy and then interprets elements of developing a security policy of SM, including, the nature of an electronic commerce organisation, top down approach, security principles, purposes of a security policy, security policy communication, holistic security, security stance, recommended development method, data centric approach, implementation in IT systems, consequences of manage data improperly, policy flexibility and policy management. Finally, this case study comments on the advantages and disadvantages of the top down approach, recommended development method and implementation in IT systems.

2. Define Security Policy

A security policy is a document created by an organisation which stipulates rules that allow internal and external users the full or part of rights to access the organisation’s computing system and data resources. This policy also defines the organisation’s business, security goals and objects of the organisation’s management. This policy is generally used to protect people who are attached to an organisation and the logical and physical resources of the organisation.

3. Nature of electronic commerce organisations

According to SM, an electronic commerce organisation is an organisation that uses the Internet to process their business, for example:

- Government organizations that want to automate form processing and their data processing is transferred to external environments,
- Electronic business organisations which process their customers’ personal and financial details and to send external environments.

4. Top down approach

According to SM, the development of a data security policy should take a “top down approach based on a well-stated policy in order to develop an effective security architecture” Weise, J & Martin, C. R. (2001). The top down approach also reflect the security expectations of the management which are “translated into specific, measurable, and testable goals and objectives” Weise, J & Martin, C. R. (2001). Another approach is that, the security policy is developed, built, installed and maintained on computer systems by individuals or separate departments. In this case the security policy will be disunited.
5. Security Principles

According to SM, the first essential step is to define the security principles in the security policy development. These principles present the specific type and nature of security policies that are appropriate to the specific organisation and its environment. Organizations “should evaluate and review these security principles before and after the development and elaboration of security policies. This is to ensure that management’s expectations for security and fundamental business requirements are satisfied during the development and management of the security policies” Weise, J & Martin, C. R. (2001). The security policies must be consistent of in terms who can access and process what resources. They should comply with the nature of the organisation’s business, technical, legal, and regulatory environment. The following are common principles:

- Make data and processing resources accessible to authorised users.
- Categorise the risk of customers’ and the organization’s data to find effective strategies preventing them from misuse.
- Apply strategies to guard the integrity of data processing operations and protect them from unauthorized use.
- Apply strategies to guard the customer and processed data, and prevent unauthorized disclosure.
- Apply strategies to guard the integrity of the customers’ and the organisation’s processed data, and prevent them from unauthorized modification, substitution, insertion, and deletion.

6. Purposes of a Security Policy

SM claims that the main purposes of a security policy is to inform users, staff and the management of the necessities to protect “various assets including people, hardware, and software resources, and data assets” Weise, J & Martin, C. R. (2001). Another purpose is to provide basic instructions to purchase, configure, and audit computer systems and networks for compliance with the policy and future development.

7. Security Policy Communication

The security policies must be distributed to relevant users, staff, management, vendors, third party processors, IT staff and people who use the services should be required to acknowledge physically that they understand the terms and accept the conditions.

8. Holistic Security

SM believes that there is no single component of a system which can provide security. Security policies work effectively only if the security measures manage people, hardware and software, processes and all access controls are implemented properly.
9. Security Stance

SM comments that organisations should take a security stance that gives staff only enough privileges of access to the resources that require to perform their assigned tasks.

10. Recommended Development Method

SM recommends that the development of a security policy approach should be followed the standards of ISO 17799. This standard it identifies all possible software and hardware, internal and external risks and countermeasures.

11. Data Centric Approach

SM considers that the data of an IT system are valuable assets and at great risk. The security policies should be based on a data centric model which follows the data through the system and processes to find an effective way to develop efficient security policies.

12. Implementation in IT Systems

SM stresses that to ensure the system works properly “all policies and procedures external to the information-processing system are also correctly enforced and performed” Weise, J & Martin, C. R. (2001).

13. Consequences of Managing Data Improperly

There is no doubt that, the hazard of improper management of data could be very serious for anyone whose personal details or finance data are obtained by crime organisers. In this case his/her identity and finance could be misused. It also greatly affects government organisations which are in charge data. The most recent case is that which concerns the Chief Commissioner Police Christine Nixon in Victoria. After some cases of confidential data were exposed to the public, the media requested she resign or be fired by the government. A private organisation which fails to manage customer data properly could also face numerous litigations and compensation actions.

14. Policy Flexibility

SM emphasises the flexibility of a security policy which will be workable in the long term. The hardware and software decisions should also be specific and independent to avoid the cost of replacement of rapidly obsolete technology. In addition, the process of updating which involves resources and people who do the changes should be documented.
15. Policy Management

SM suggests that organisations should implement a regular review process of security policy including updating obsolete hardware and software and policy. A specific team should be assigned to carry out the review.

Conclusion

No matter how many security measurements an organisation implements to guard its data, the risks of unauthorised access, lost data by natural causes or wilful damage remain. However, with a proper security policy, organisations can eliminate most of the unwanted risks of financial lost, staff low morale and litigation from users.
Comments

Top down approach

According to SM the development of a data security policy should take a top down approach. The following are the advantage and disadvantages of the top down approach:

- The advantage of the top down approach that it has a holistic view which presents the general objectives of an organisation.

- The disadvantage is that it will not reflect the practical ideas of technicians and customer service staff, who operate and maintain the organisation’s technology and business, who understand the system more than the management, who can identify problems and who can give practical solutions. If the management takes the bottom up approach which listens to frontline staff concerns and solutions for the problems of the system and mixes these with their views, then the security policies would be more appropriate.

- There are also disadvantages with the bottom up approach is that it might require time and resources to analyse the ideas of different staff from different departments. However, the management can find short cuts to obtain the most appropriate suggestions from frontline staff.

Recommended Development Method

SM recommends a development method which should follow the standards of ISO 17799, because it identifies all possible of software and hardware, internal and external risks and countermeasures,

- The advantage of IOS 17799 model that is it minimises all possible risks.
- The disadvantage is that it requires a huge budget to carry out. In other words, the IOS 17799 suits organisations which have adequate resources.

Implementation in IT Systems

SM stresses several risks from external environment and overlooks the risks from internal environment. For example, even if the system is properly controlled from external elements, the risks of lost and damage data and improper use of data could be from internal sources including, unauthorised access and wilful damage within the organisation.
References
