Developing and implementing effective research paper examples

Business, Management

INFORMATION SECURITY POLICES AND PROCEDURES

Current information security policies and procedures focus on employee practices and on system infrastructures. There needs to be a balance between these two aspects to achieve company goals in an efficient and secured manner. This research paper attempts to explain how organizations develop and implement effective information security policies and procedures. It discusses what happens in each phase and enumerates the factors that need to be managed for the success of information security objectives.

First is the discussion of the overall process of company-wide information security. Knapp et al. (2009) explains that information security policies have to be viewed from the company-wide process model. The organization plays a significant role in addition to the technical infrastructures in place. This is what IT professionals call the sociotechnical approach. Company best practices are recommended by these professionals to institute not just an information security policy, but also a culture of responsibility among employees.

Information security is a fundamental set of guidelines and procedures covering individuals on the use of company information systems. Its goal is to protect the organization from external and internal attacks. Current organizations maintain a database of transactions, inventories, and data that can be compromised. Usually the two general steps are: (1) policy approval and (2) policy implementation (Knapp et al., 2009). For the latter phase, auditing and monitoring tools are important to know when the policies are

violated. This needs support from the top management. The resulting process model from their study includes: (1) Cycle of risk assessment, policy development and policy review; (2) policy approval; (3) policy awareness and training; (4) policy implementation; (5) monitoring; and (6) enforcement. Overall, it corresponds to a cycle where step 6 goes back to step 1. If the policy is not effective anymore, then the policy is retired. This is usually the case when breakthrough advances in technology corresponds to a change in how things need to be done. Furthermore, emphasis on training and awareness is given since the employees need to be knowledgeable to support the implementation of the policy.

For the model identified, internal and external influences were identified. Internal factors are the top management support, business objectives, organization culture, technology architecture and internal threats. For instance, modern universities use database software for student records and online instruction to support school mission and vision. Usually, these software require licenses and have hardware/ operating system requirements for implementation and use. On the other hand, external influences are the economic sector, technology advances, industry standards, legal and regulatory requirements and external threats. For example, user-defined access to functions and transactions (in enterprise resource planning software) give accountability to certain actions. Thus, new job roles have been defined such as controllers who are accountable of creating purchase orders and inventory audits within specific areas.

Second is the influence of human and organizational factors. The interface has to be well aligned. Nine contributory areas were identified by Kramer et

al. (2009) in their study of threat vulnerabilities. These include: (a) external influences, (b) human error, (c) management, (d) organization, (e) performance management, (f) resource management, (g) policy issues, (h) technology, and (i) training. Each of these needs to be managed and accounted for. External influences have been discussed in the previous paragraph. Human errors are related to degree of usability and error-free behaviour. Usually, this accounts for password error, input error, etc. Management need to influence the organization by providing a culture of responsibility and integrity. Ultimately, the leadership in the organization has to provide the vision where the employees can see themselves and a mission that cares for the society through the organization goals. Also, performance relating to the skills and the competencies of the IT team in particular has to be considered since they are the experts of the system. Resources such as bandwidth data, data infrastructures, and software have to be managed such that their use is maximized and costs are minimized. Proper documentation of policies has to be followed too. This concerns traceability and appropriateness of the policies. Technical terms have to be discussed in simple language. For better understanding, flowcharts can be used, for instance, in standard operating procedure documents. Lastly, the IT team has to be updated in current trends through continuing professional education and training.

Apart from these nine areas, organizations need to consider insider threats as real. Unscrupulous data mining have been done on unaware companies and government agencies in the past. Carl Corwill (2009) outlined some

proactive measures which can be done by organizations to minimize this type of threat. Some of these are:

Providing training in detecting manipulative attempts to all customer representatives.

Warning employees to be alert to people asking for sensitive or restricted information.

Being alert to unknown people who try to extract information in a rush manner, with intimidation, stressing authority or refusing to give contact details.

Encouraging managers to be alert to persons who are excessively negative about the organisation or their work.

Establishing a formal grievance procedure for employees to vent their feelings.

Setting up an easy and confidential system for employees to report any abnormal behaviour from their colleagues.

Backing up electronic information from time-to-time and keeping a secure copy in another location.

When employment is terminated, employee access to systems, sites and information needs to cease.

These are required measures. Information is particularly valuable to some types of organizations- consulting, architectural, engineering and design firms.

In sum, organizations need to be proactive in every step of the policy implementation so that potential problems are avoided. The policies have to

be well documented and specific. Furthermore, internal and external threats to information security have to be considered in totality since influence factors are interrelated. In the end information security is everyone’s responsibility.

References:

Colwill, Carl. “ Human Factors in Information Security: The Insider Threat - Who can you Trust these Days?” Information Security Technical Report 14 (2009). 186-196. Print.

Knapp, Kenneth J. et al. “ Information Security Policy: An Organizational-Level Process Model.” Computers and Security 28 (2009). 493–508. Print.

Kraemera, Sara, Pascale Carayonb, and John Clem. “ Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities.” Computers and Security (28) (2009). 509-520. Print.