A Life Cycle Approach to Information Security Policy for Electronic Commerce

Jackie Rees  
*Purdue University, jrees@mgmt.purdue.edu*

Subhajyoti Bandyopadhyay  
*Purdue University, shubho@ufl.edu*

Follow this and additional works at: [http://aisel.aisnet.org/amcis2000](http://aisel.aisnet.org/amcis2000)

Recommended Citation  
[http://aisel.aisnet.org/amcis2000/18](http://aisel.aisnet.org/amcis2000/18)
A Life Cycle Approach to Information Security Policy for Electronic Commerce
Jackie Rees, Krannert Graduate School of Management, Purdue University, jrees@mgmt.purdue.edu
Subhajyoti Bandyopadhyay, Krannert Graduate School of Management, Purdue University, s_bandyopadhyay@mgmt.purdue.edu

Abstract

The explosive growth of Electronic Commerce (e-commerce) has forced many organizations into uncharted territory. As with any expedition into the unknown, firms must take on new risks, as well as cope with existing ones. These new risks include increased exposure to theft and fraud, privacy and confidentiality issues and denial of service issues. One way to manage such risk is by the adoption and enforcement of information security policies that take into consideration the dynamic nature of e-commerce.

Analysis of the current deployment of information security policies in e-commerce indicates that an improved framework for managing such risk is necessary. A comprehensive policy framework for managing e-commerce security risk has been developed, incorporating existing “best practices” and research as well as addressing shortcomings in current practice. Currently utilized risk assessment, policy development and enforcement methodologies will be placed within the framework, as well as the inclusion of change management issues.

Introduction

A majority of executives polled in a recent security survey (Ernst and Young, 1999) believe information security is a vital component of e-commerce success. Security is more than erecting physical and electronic barriers. The strongest encryption and most robust firewall are practically worthless without a set of security policies articulating how these tools are to be used. Given the dynamic nature of e-commerce, such policies are subject to continuous change, creating the need to establish a framework under which all security occurrences can be scrutinized. Therefore, the policy set should be dynamic; however, the issues addressed should be universal enough to be relevant and applicable in changing environments.

The objective of this research is to provide information security professionals and top management a framework through which useable security strategy and policy for e-commerce applications can be created and maintained in line with the standard information technology lifecycle. This framework, titled Policy Framework for Interpreting Risk in e-commerce Security (PFIRES), offers a possible starting point for understanding security policy’s impact on an organization, and is intended to guide organizations in developing, implementing, and maintaining security policy.1

Background

The basic requirements for e-commerce security include information confidentiality, authentication, authorization, data integrity, non-repudiation (Bhimani, 1996) and availability. Given the dynamic environment of e-commerce, effectively meeting these requirements is not straightforward. The challenge is to come up with the most technically and economically feasible plan for protecting e-commerce activities, knowing that today’s most secure technology will be vulnerable tomorrow.

As is the case for most systems problems, the best approach is a structured one, including analyzing risk and delegating resources to protect the most valued assets of the organization. Security policies are put into place to manage risk. Such policies are high-level and technology neutral. Their purpose is to set directions and procedures, and to define penalties and countermeasures for noncompliance. Literature on how to develop specific Internet and information security policies may be found in (Lichtenstein, 1997), (Straub and Welke, 1998) and (Wood, 1995). Security policies must not be confused with implementation-specific information, which would be part of the security standards, procedures and guidelines, none of which falls within the scope of this paper. Security policies are created by empowered representatives of the organization, including human resources, legal and regulatory matters, information systems, public relations, security and various business units.

1 This research was completed under the direction and assistance of the Center for Education and Research in Information, Assurance and Security (CERIAS) at Purdue University. Additionally, Andersen Consulting’s Information Security practice considerably participated in the research effort.
Some of the most important security policies include user identification and password policy, remote access policy, extranet policy, Internet security policy, access to data policy, administration policy, incident response policy, awareness procedure policy, user behavior policy, security monitoring and audit policy, and privacy policy. Security policies must be balanced and provide tradeoffs between level of security, user convenience and cost. Without an equitable balance between these elements, it is not realistic to expect that the security policies will be followed.

The one theme that repeatedly arose in the creation of this model was “change is constant.” Therefore, a lifecycle approach seemed appropriate, not only for e-commerce information security policy but for all security-related policies. To develop a tool that would aid in the formulation and management of e-commerce information security policies, other tools in similarly rapidly changing business arenas were examined. PFIRES was developed borrowing from the new product development life cycle (Heuss, 1965; Vernon, 1965), and the systems development life cycle (SDLC) (Hoffer, et al., 1999). Existing literature addressing frameworks for developing e-commerce policies use a matrix of organizational relationships and technology (Oliver, 1997). The shortcoming with existing approaches is that none address the problem of keeping up with the increasing rate of change in e-commerce technology and applications nor do they consider how to keep such policies consistent and aligned with organizational objectives. The PFIRES framework is intended to act as a communications tool between the strategic decision-makers in the e-commerce organization and the information security practitioners so that organizational objectives can be successfully met.

A Policy Framework for Interpreting Risk in e-commerce Security

The PFIRES life cycle consists of four major phases: Assess, Plan, Deliver, and Operate. Each is sharply defined with specific exit criteria that should be met before transitioning to the next phase. Each phase is further broken down into steps detailing the activities that occur within each phase. These steps are to be executed with particular attention paid to people, processes and technology issues.

It is important to remember that policy development is an iterative process. Therefore, the model includes feedback loops at every step. Feedback is also necessary to ensure that the requirements of previous steps are being satisfied. Additionally, it is recognized that not all proposed changes are alike in nature or magnitude, but rather fall along a continuum. Therefore, proposed changes of a more strategic nature need to be more thoroughly examined in the context of the model, especially in the following Assess phase whereas proposed changes identified as more of a tactical nature might be expedited through the model.

Assess Phase

The Assess phase can be initiated by two distinct events: either a decision to implement (or completely overhaul) security policy or a response to a proposed change from the Operate phase. In either case, the goal is to assess the proposed change against existing policy and organizational environment. The Assess phase has three possible outcomes: the proposed change is accepted and the Plan phase is initiated; the proposed change is not accepted but the policy assessment determines that policy should be updated and the Plan phase is initiated; or the proposed change is not accepted and it is determined that policy does not need updating. In the last case the model resumes in the Operate phase.

Before beginning the process of implementing or overhauling security policy, the organization needs to review existing policy and complete a full risk assessment. These activities are conducted during the two
steps of the Assess phase, Policy Assessment and Risk Assessment. A Policy Assessment is conducted to review existing policies, standards, guidelines and procedures. The following four sub-steps have been identified and are contained within the Policy Assessment step: Analyze Policy Environment, Identify Policy Gaps and Contradictions, Summarize Policy Assessment Results, and Develop Policy Recommendations. Executed in sequence, these sub-steps result in a decision on whether to accept the proposed changes and an assessment of how the proposed change affects existing policy. Risk Assessment identifies the business assets an organization wants to protect, and identifies potential threats to those assets. The various sub-steps in the Risk Assessment process are: Conduct Security Assessment, which identifies elements in the current or proposed environment that may be subject to threats that could compromise information assets; Assess Business Risk, which identifies the most valuable assets in terms of security; Develop Security Recommendations, which involves identifying security options, determining payroll and non-payroll costs, determining the priority of options, verifying results and developing a cost/benefit matrix; and Summarize Assessment Final Recommendations, where results of both the Policy and Risk Assessments are documented so management can decide whether to accept the proposed change. Examples of risk assessment practices can be found in Oppenheimer, et al. (1997). If accepted, the life cycle for this particular proposed change continues to the Plan phase. If rejected, but it is determined that other policy changes are required, the Plan phase follows as well. Otherwise, the life cycle resumes in the Operate phase.

Plan Phase

The Plan phase prepares for the implementation of the proposed change including creating or updating policy and defining the requirements for the proposed change. The Plan Phase has two sub-steps, Policy Development and Requirements Definition. Policy Development itself consists of two sub-steps: Create/Update Security Strategy and Create/Update Security Policy. The Create/Update Security Strategy sub-step is an overview of future business direction along with the security controls needed to support these business functions. The Create/Update Security Policy sub-step includes identifying areas for security policy, drafting security policy, a review of existing security policy and publishing security policy. Examples of current best practices can be found in Wood (1995). Within the Requirements Definition step an organization analyzes its security policy in order to define the requirements of the new security architecture in light of the updated policy. It is important during this sub-step to evaluate the detailed requirements against industry best practices, examples of which can be found in Yourdon (1989). Additionally, market segments may need to meet requirements specified by their country or local government, or by some other authoritative body.

The Deliver Phase

The Deliver Phase is where the actual implementation of the policy takes place. It consists of two steps: Controls Definition and Controls Implementation. In the Controls Definition Step controls are defined as practices, procedures or mechanisms that reduce security risks, and this step defines those needed to meet the requirements of the security policy. Controls Definition consists of four sub-steps: Design Infrastructure, Determine Controls, Evaluate Solutions, and Select Controls. These sub-steps are sequential in nature and follow the widely used in the systems development life cycle (Hoffer, et al., 1999). In the Design Infrastructure sub-step, the requirements from the Plan phase are used to design a high-level security infrastructure containing technical, procedural, and organizational components. To Determine Controls, the high-level designs are translated into controls and their requirements. Specific organizations may have additional requirements, such as a control provided by a partner-vendor or other preferred provider. The purpose of the Evaluate Solutions sub-step is to identify and evaluate the options for each control and select the best option. Recommendations for methodologies for evaluating solutions can be found in Boer (1999) and Thierauf (1994). To Select Controls, the solution that best meets the control requirements is selected and mapped to the infrastructure design. This is a good time to check the list of selected controls against the security policy requirements and verify that all requirements are being met – this is an instance of the feedback functionality that is emphasized throughout the PFIRE model. At this point, the controls list should be validated to assure that duplicate requirements are not being met by different solutions and will identify opportunities for controls reuse across the security infrastructure. The Controls Implementation step implements the controls selected in the prior step. Activities include building, testing, and implementing the final security infrastructure. This step is executed through four self-explanatory sub-steps: Create Implementation Plan, Build, Test, and Pilot and Deployment. Several resources are available which outline best practices on building and implementing security infrastructure (Hutt, et al., 1995).

Operate Phase

The purpose of the Operate phase is to monitor the controls that have been put in place to secure the organization and handle incidents as they arise on a daily basis. In addition, business and technology trends are watched and analyzed. This phase is unique because it is not clearly executed through a series of sub-steps.
Monitor Operations consists of several simultaneous activities that must co-exist to support the environment. Administration and Operations covers administrative functions and include, but is not limited to user administration (adding, deleting, and modifying system and application users), evaluating and applying security patches to systems and applications, system and application monitoring for security events, monitoring security news resources for new vulnerabilities and administering anti-virus applications. Communications communicates to different audiences, some requiring only an awareness of security, and others requiring time-sensitive information, the appropriate security messages. Investigations includes activities necessary to examine a situation or incident, determine root cause or verify facts, and recommend action. Common situations where an investigation will be necessary include: after a break-in or hack has occurred, when an employee is suspected of violating corporate policy, after an unplanned security event caused a system to crash, or after a fraud has occurred. Security Services provides security specialists to project teams as they design new capabilities, refine existing processes, or otherwise undertake change within the environment. Compliance includes those activities necessary to ensure the infrastructure is following security policy guidelines. It is typically thought of as an internal audit function, but a security compliance program is more proactive than quarterly audit reports and findings. Several resources describing best practices for managing an information security environment include Garfinkel and Spafford (1997), Hutt, et al., (1995) and Krause and Tipton (1999).

A security policy that is not constantly evaluated and updated is of little value. Review Trends and Manage Events, the final step in PFIRES, identifies those events or trends that may signal a need to re-evaluate the security policy. This step can be broken down into the following four sub-steps: Manage events (planned and unplanned); Identify internal trends; Identify external trends and Escalate to Assess phase. As in the Monitor Operations step, these activities are not executed sequentially. Although escalation is always the last step, event management and trend identification can take place at the same time.

Manage Events defines events as situations or circumstances outside the boundaries of normal activity. For example, an individual violating an acceptable use policy by surfing for sports scores during normal office hours is outside of normal or expected activity. However, procedures can be put in place so the event can be processed as part of planned operations. On the other hand, there are situations that cannot be planned for, such as fraud or destruction of data. Specific management procedures cannot be anticipated for each event. Rather, they require an incident response process (Guttman and Robach, 1995).

Identify External Trends looks for external trends that may indicate the need to reassess current security policy. Its key components are identifying information within the context of the organization’s industry and/or priorities that may have security relevance and determining whether to escalate a trend or event to the Assess phase. Identify Internal Trends can come from new business opportunities, new capabilities, or new applications. They might also arise from an existing business or security process.

Not all changes should be escalated to the Assess phase. In the Escalate to Assess Phase common sense and a set of criteria should prevail. These criteria need not be pages of detailed considerations, but they should validate a true impetus for change. The following key issues should be examined: scope of impact (will this change impact a single business unit or group within the organization, or will it have a global business impact?), timeliness (has the need for this change been proven over time?), and momentum (is there support among key stakeholders (system administrators, application owners, business unit leaders) that this change is necessary?).

Conclusion

As a high-level policy management tool, PFIRES facilitates communication between senior management and technical security management. With improved communication, the organization should realize immediate benefit - increased protection from and responsiveness to security incidents related to e-commerce activities. The PFIRES model is robust enough to assist the firm in implementing e-commerce security policy and because there is a recognized difference between strategic and tactical changes during the Assess phase, the model is flexible enough to accommodate the dynamic nature of the e-commerce environment. By effectively managing security risks, the organization is better positioned to successfully achieve its e-commerce objectives.

Just as e-commerce and information security are rapidly evolving fields, so is PFIRES. Work is currently underway to document the use of PFIRES in an organization implementing security policy for the very first time. Additional work is planned to follow the use of the model over repeated iterations of the lifecycle. Future work is planned to continually refine the model given the dynamic nature of the domain.
References


