Policy Framework for Interpreting Risk in eCommerce Security

Executive Summary

A Joint Research Project by

Accenture

and

The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University
# Table of Contents

1. Introduction ................................................................................................................. 3
2. Background .................................................................................................................... 3
4. Conclusion ..................................................................................................................... 7
5. Contact Information ...................................................................................................... 7
1 Introduction

Is your security perfect? How would your organization handle a security breach? Can security ever be perfect? Changes occur every day. One minor, seemingly insignificant change can make your entire organization vulnerable to attack. Are you performing the due diligence to prevent this? Policy can help.

The Policy Framework for Interpreting Risk in eCommerce Security (PFIRES) is a comprehensive model addressing the entire life cycle of security policy. The framework provides organizations the means to keep policy up-to-date as change proliferates through the organization at eCommerce speed. Without a model to continually address policy as changes occur, organizations greatly increase the risk to which they are susceptible.

The PFIRES model is a holistic approach to information security tying security policy to the business strategy. This approach ensures that policy and the security controls put in place to enforce it are synchronized with organizational goals and not a knee-jerk reaction to the latest vulnerability or technology trend. In addition, the model addresses human performance factors providing a higher probability of acceptance by affected personnel. These features differentiate the PFIRES model from other approaches to policy and provide a workable solution to the problem of keeping a usable policy up-to-date.

2 Background

The Policy Framework for Interpreting Risk in eCommerce Security is a joint research project by Accenture and the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University. The purpose of this research paper is to provide a framework for managing information security policy for eCommerce applications.

Two statements best summarize the state of computer security policy in most organizations today. First, most organizations have a set of information security policies defined for day-to-day operation of network activities but do not encompass all aspects of computer activity. Second, most organizations do not have a mechanism to identify the need for new policy and to update current policy as the business and technical environments change. Using the PFIRES model assists in creating clearly stated and communicated policies about all computer-related activities, thus limiting the organization's exposure to risk. By modeling the life cycle after a typical software development life cycle, we attempt to give organizations a framework for creating, maintaining and updating security policy in line with an ever-changing eCommerce environment.
2.1 Audience

This Executive Summary is intended for the Chief Information Officer (CIO) or Information Technology (IT) department—the individual or department charged with steering information technology strategy. The framework is intended to help guide the Information Technology organization through the difficult stages that must be addressed during the life cycle of security policy.
3 Policy Framework for Interpreting Risk in eCommerce Security

The PFIRES life cycle is defined by four phases closely tied to the software development life cycle (SDLC): Assess, Plan, Deliver, and Operate. Each phase is then divided into two steps that define high level actions necessary to develop and maintain security policy and the controls necessary to monitor and enforce it. Feedback loops are introduced to validate the output of each step against the requirements for that step. Each step examines the effect of Human Performance and eCommerce on that step of the life cycle.

An organization's initial pass through the model will be intense. During this initial effort, a great deal of time and attention will be paid to the assessments in the Assess phase to ensure all aspects of the organization are analyzed. A repeat or iterative pass through the life cycle is triggered by a proposed change from the Review Trends and Manage Events step. In an iterative pass, the magnitude of the life cycle steps will be in proportion to the change being considered.

3.1 Assess Phase

The Assess phase represents the starting point within the life cycle for a proposed change or an initial assessment. The purpose of this phase is to assess the proposed change against the existing policy environment.
(Policy Assessment) and existing infrastructure (Risk Assessment). In addition, human performance considerations are addressed in the Organizational "As-is" assessment.

3.2 Plan Phase

The Plan phase prepares the organization for the implementation of the change, the policy updates brought about by the change, and the risk mitigation measures chosen to support the change. Policy Definition is the step in which the security strategy and security policy are created and updated. The Requirements Definition step outlines the requirements for the new or updated policy and the controls needed to secure those changes.

3.3 Deliver Phase

During the Deliver phase the security policy, controls and training are designed, built and rolled out to the organization. The phase consists of two steps: Controls Definition and Controls Implementation. The Controls Definition step designs the security infrastructure to meet the changes in security policy. In the Controls Implementation step, the security infrastructure designed in the previous step is built, tested and rolled out along with the training to support the solution.

3.4 Operate Phase

The Operate phase is the phase in which policy compliance is monitored and events and trends are handled. The phase consists of two steps: Monitor Operations and Review Trends and Manage Events. The Monitor Operations step monitors the controls that are in place to ensure policy adherence for violations. The Review Trends and Manage Events step handles the violations or events, also reviewing trend data and external forces such as regulatory changes, industry trends, changes in business direction, technological advancements and new security threats for opportunities to update security policy and controls.
4 Conclusion

In order to remain competitive, all businesses will have to adopt some form of eCommerce business model. Security is the enabler of eCommerce; policy is the enabler of security. New security technologies have improved an organization's ability to monitor and enforce policy. All of these elements - eCommerce, security, technology and policy - are constantly evolving. The PFIRES model will help organizations adjust to these changes and adapt for the future.

5 Contact Information

The Policy Framework for Interpreting Risk in eCommerce Security white paper can be downloaded from http://www.cerias.purdue.edu/

For further information regarding this project, please contact:

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>John C. Clark</td>
<td>Accenture</td>
<td><a href="mailto:john.c.clark@accenture.com">john.c.clark@accenture.com</a></td>
</tr>
<tr>
<td>Andra Short</td>
<td>CERIAS</td>
<td><a href="mailto:acs@cerias.purdue.edu">acs@cerias.purdue.edu</a></td>
</tr>
</tbody>
</table>