Creating and maintaining effective security strategy and policy for software applications.

23

PFIRES: A Policy Framework for Information Security

As organizations increasingly rely on information systems as the primary way to conduct operations, keeping such systems (and the associated data) secure receives increasing emphasis. However, the prevalent model within many organizations appears to be an ad hoc approach to security, where the latest breach becomes the model for future occurrences. For example, Microsoft issued over 80 critical patches for its IIS Web Server software over the past three years. Despite the low initial cost of the software, the maintenance costs over time are prohibitive [2]. A well-designed and maintained security policy potentially can reduce such costly forays, as well as provide protection from disaster.

Our objective here is to provide information security professionals and top management a framework through which useable security strategy and policy for applications can be created and maintained in line with the standard information technology life cycle. This framework, the Policy Framework for Interpreting Risk in E-Business Security (PFIRES), was initially developed for e-commerce activities and has since been generalized to handle security policy for all types of organizations engaged in computing and Internet operations. This framework offers a possible starting point for understanding a security policy's impact on an organization, and is intended to guide organizations in developing, implementing, and maintaining security policy.

Information Security Policy

Security policies are generally high-level, technology neutral, concern risks, set directions and procedures, and define penalties and countermeasures if the policy is transgressed, and must not be confused with implementation-specific information, which would be part of the security standards, procedures, and

By Jackie Rees, Subhajyoti Bandyopadhyay, and Eugene H. Spafford

guidelines. Security policies are created by empowered organizational representatives from human resources, legal and regulatory matters, information systems, public relations, security, and the various lines of business. A guideline for developing Internet-specific security policy was discussed in [5], while more generalizable security policies and guidelines can be found in [8]. The problem with current approaches is that none address the problem of keeping up with the increasing rate of change in technology and applications nor do they consider how to keep such policies consistent and aligned with organizational objectives.

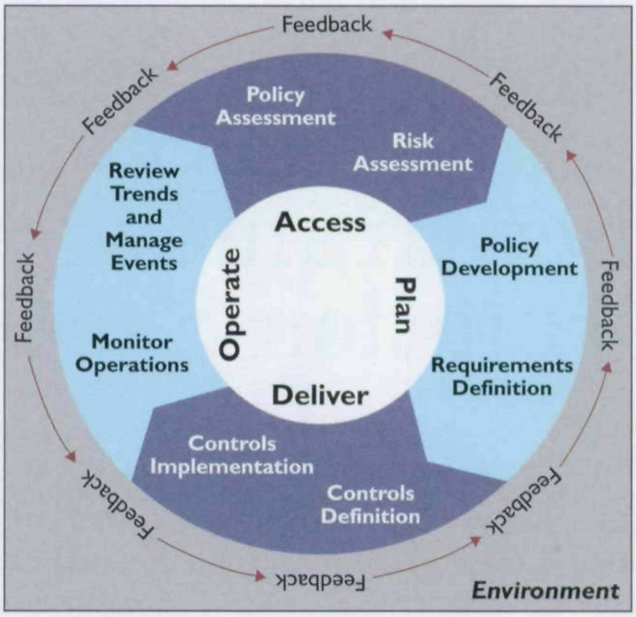

Figure 1. PFIRES life-cycle model.

To develop a tool to aid in the formulation and management of security policies, other tools in similarly changing business arenas were examined. As is the case for most systems problems, the best approach was found to be a structured one, including analyzing risk and delegating resources to protect the most valued assets of the organization [1]. PFIRES was developed borrowing from both the new product development life cycle [7], and the systems development life cycle (SDLC) [4].

While creating security policy is not an exact science, well-defined processes can be put into place so that all security-related requirements are systematically considered. An analogue is the SDLC, which embodies a well-defined process for considering business requirements, translating such requirements into an information systems context, and then developing an information system that supports those requirements. PFIRES is intended to be systematic, yet dynamic. The framework is detailed enough to ensure that an organization does not overlook anything while addressing a security issue, but dynamic enough to ensure the speed and execution required to adapt rapidly to changing business scenarios.

A Policy Framework for Interpreting Risk in E-Business Security

The PFIRES life cycle consists of four major phases: Assess, Plan, Deliver, and Operate, as shown in Figure 1. Because policy development is an iterative process, the model includes feedback loops at every step. Feedback is also necessary to ensure the requirements of the previous step are satisfied.

Organizational change is defined as a continuum, with the two end points being tactical and strategic. Tactical changes involve short-term goal achievement and how to control and evaluate the process of achieving goals, whereas strategic changes are long-term, broad-based initiatives involving positioning within the marketplace and typically involve members of senior management [6]. Most organizational change falls somewhere between these two end points.

Assess Phase

The Assess phase can be initiated by two distinct events: either a decision to execute the model from scratch or a response to a proposed change output from the Review Trends and Manage Events step. In either case, the goal is to assess the proposed change against the existing policy and organizational environment. The Assess phase has three possible results, as shown in Figure 2.

For a company executing the PFIRES model for the first time, the Assess phase is the logical starting point. However, before beginning the process of implementing security policy, the company needs to review existing policy and complete a full risk assessment. These are conducted during the two steps included in the Assess phase: Policy Assessment and Risk Assessment.

Policy Assessment. Whether PFIRES is initiated as a result of initial policy creation or a change to existing policy, Policy Assessment is conducted to review existing policies, standards, guidelines, and procedures. The determination of whether the proposed change is strategic or tactical will affect how steps later in the life cycle will be explored; however, if this is the organization's first time executing the model, the effort is by definition strategic in nature.

There are four sub-steps 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 regarding whether to accept the proposed changes and an assessment of how the proposed change affects existing policy.

Once the policy assessment is complete, a decision needs to be made on where the proposed change falls within the change continuum. The position on the change continuum that the proposed change falls in will help determine the scope of the Risk Assessment step, thus influencing the execution of the subsequent steps of the life cycle.

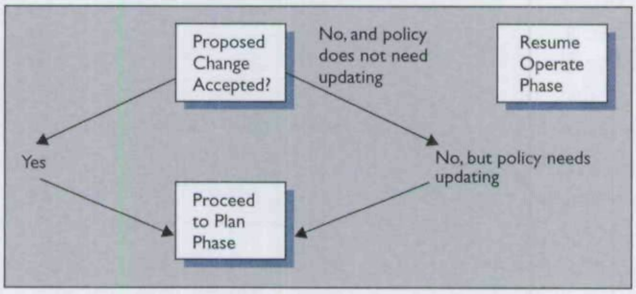
Proposed Change Accepted?
No, and policy does not need updating
Resume Operate Phase
Yes
No, but policy needs updating
Proceed to Plan Phase

Figure 2. The Assess phase flowchart.

Risk Assessment. 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 identifies elements in the current or proposed environment subject to threats that could compromise information assets.
- Assess Business Risk identifies the most valuable assets in terms of security. While intangible assets are difficult to valuate, it is beneficial to rank them.
- Develop Security Recommendations involves identifying security options, determining payroll and non-payroll cost, determining the priority of options, verifying results and developing a cost/benefit matrix.
- Summarize Assessment Final Recommendations documents the results of both the Policy and Risk Assessments so management can decide whether to accept the proposed change. If accepted, the life cycle for this particular proposed change continues in 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. It is vital to develop security strategy and policy that is in line with existing business strategy and policy. Activities during Policy Development assure this. Policy Development itself consists of two sub-steps: Create/Update Security Strategy and Create/Update Security Policy.

Create/Update Security Strategy. Security strategy is an overview of future business direction along with the security controls needed to support these business functions. A security strategy session should be held consisting of the following tasks: identify future business initiatives; identify risks to each initiative; identify security options; prioritize security initiatives and document security strategy. This session should include key management personnel not only for their thought leadership but to gain their confidence in the entire process.

Create/Update Security Policy. Specific tasks of this sub-step include identifying areas for security policy, drafting security policy, reviewing security policy and publishing security policy.

Requirements Definition. Within Requirements Definition an organization analyzes its security policy in order to define the requirements of the new security architecture in light of the updated policy. The three sub-steps are outlined here.

Translate Recommendations to Requirements. The high-priority recommendations developed in the Risk Assessment are used in this sub-step to create the security infrastructure necessary to support the change.

Develop Detailed Security Requirements. The high-level requirements from the previous sub-step are expanded to a sufficient level of detail so that control selection can begin. This sub-step carefully considers the overall technical environment so that the proposed change will tightly integrate and support the

Because policy development is an iterative process, the model includes feedback loops at every step.

existing environment. Interoperability requirements such as systems and network support, and standards and application programming interface support must be considered.

Verify Requirements. The requirements defined in the previous two sub-steps are validated against the inputs to the Requirements Definition step. All requirements should map back to a specific risk (as documented in the Risk Assessment) or to a specific point in the Security Policy. It is also important during this sub-step to evaluate the detailed requirements against industry best practices. Additionally, particular market segments may need to meet requirements specified by their country or local government, or by other authoritative bodies.

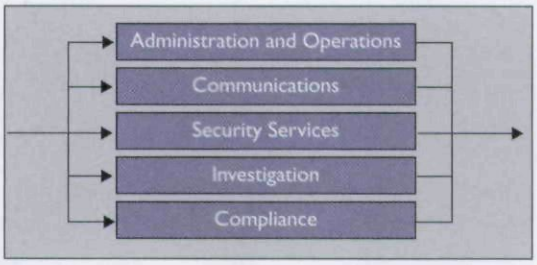

Figure 3. Activities in the Monitor Operations step.

The Deliver Phase

The Deliver Phase is the actual implementation of the policy. The phase consists of two steps: Controls definition and Controls implementation, as shown in Table 1.

Controls Definition. Controls are 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 SDLC [4].

Design Infrastructure. In this sub-step, the requirements from the Plan phase are used to design a high-level security infrastructure containing technical, procedural, and organizational components.

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.

Phase	Step	Sub-step
Assess		
Plan		
Deliver	Controls Definition	Design Infrastructure Determine Controls Evaluate Solutions Select Controls
	Controls Implementation	Create Implementation Plan Build Test Pilot and Deployment
Operate		

Table 1. The Deliver phase steps and sub-steps.

Evaluate Solutions. The security marketplace is growing rapidly, and it is likely there will be several choices meeting the general requirements. The purpose of this sub-step is to identify and evaluate the options for each control and select the best option.

Select Controls. The solution best meeting the control requirements is selected and mapped to the infrastructure design. The controls list should be validated to assure duplicate requirements are not being met by different solutions and to identify opportunities for controls reuse across the security infrastructure.

Controls Implementation. This 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 sub-steps: Create Implementation Plan, Build, Test, and Pilot and Deployment. During deployment, once the infrastructure is in place in the "live" environment, a final risk assessment should be performed to assure that all known threats have been addressed and the solution is secure.

Create Implementation Plan. A specific plan is created in order to translate design into reality. With a detailed plan, the security infrastructure is more likely to be built on time and to meet requirements.

Build. The scope of this sub-step will vary widely depending on the controls. However, there are some specific planning considerations. It is in this sub-step where detailed procedures and performance support are developed to support the selected controls. These procedures are critical to the successful ongoing management and monitoring of the security architecture. This sub-step also includes activities to develop training products including help files and manuals.

Test. Once the security infrastructure has been built, it must be tested to ensure the design was completely executed, the identified threats have been addressed, and no new vulnerabilities have been identified. Activities during this sub-step will include three types of testing: vulnerability assessment, security infrastructure validation, and application security support.

Pilot and Deployment. Once tested, the security infrastructure is deployed to the production environment. Whether a pilot is required depends on scope. Deployment includes configuring and installing security architecture components and

With a detailed plan, the security infrastructure is more likely to be built on time and to meet requirements.

rolling out new processes and procedures through communication and training. Deployment should ensure that security requirements as set forth in the policy are met, and that no new security risks are introduced.

Operate Phase

The Operate phase occurs on a daily basis. Its purpose is to monitor the controls that have been put in place to secure the organization and handle incidents as they arise. In addition, business and technology trends are watched and analyzed.

Monitor Operations. The purpose of this step is to define the daily activities throughout the organization to ensure the security policy is enforced across the security infrastructure. These activities can be broken into a few general categories as depicted in Figure 3. This step is unique because it is not clearly executed through a series of sub-steps, but instead consists of several simultaneous activities that must coexist to support the environment.

Sample Audience	Sample Key Messages
End Users	• Protect your authenticaton credentials • Do not download material from unknown sources • Comply with Internet acceptable use policies
Unix Security Administrators	• Review recent CERT alerts on new vulnerabilities • Change security standards based on new threats • Installation procedures for tested security patches to install

Table 2. Examples of communications messages.

Administration and Operations. This activity covers administrative functions and can 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. This activity communicates to different audiences the appropriate security messages (see Table 2). Each organization will have several different audiences, some requiring only an awareness of security, and others requiring time-sensitive information.

Investigations. 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 and after a fraud has occurred.

Security Services. Security services deals with providing security specialists to project teams as they design new capabilities, refine existing processes, or otherwise undertake change within the environment. The security services function can be viewed as a consulting role and can be filled by a dedicated group within the security organization or by an external service provider.

Compliance. 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.

Review Trends and Manage Events. A security policy that is not constantly evaluated and updated is of no value. This final activity identifies those events or trends that may signal a need to reevaluate 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 sequential. Although escalation is always the last step, event management and trend identification can take place simultaneously.

Manage Events. Events are situations outside of normal activity, for example, individuals violating an acceptable use policy by seeking sports scores on the Web during business hours. Although outside of approved or normal activity, such an event can easily be planned for by establishing procedures so if it does occur it can be processed as part of planned operations. Conversely, there are situations that can be anticipated but not in exact detail, such as data destruction. These unexpected events require an

By effectively managing security risks, the organization is better positioned to successfully achieve its objectives.

incident response process including documenting the incident, maintaining records of what was altered during the incident, providing appropriate information to support legal action, procedures for tracing the source of an event, guidelines for when or how to escalate an event through chain of management, and procedures for containment of events to limit damage [3].

Identify External Trends. This sub-step looks for external trends that may indicate the need to reassess current security policy. Its key components are identifying information that may have security relevance and determining whether to escalate a trend or event to the Assess phase. To determine if an event or trend should be escalated, it must be considered within the context of the organization's industry, and should be evaluated in terms of organizational priorities.

Identify Internal Trends. Internal trends can come from new business opportunities, new capabilities, or new applications. They might also arise from an existing business or security process.

Escalate to Assess Phase. Not all changes should be escalated to the 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. Three key issues should be examined: scope of impact (will this change impact a single business unit 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?).

The Future

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 benefits—increased protection from and responsiveness to security incidents related to computing activities, including e-business operations. By effectively managing security risks, the organization is better positioned to successfully achieve its objectives.

Much work remains to be done in this area. International and regional concerns, organizational behavior, legal issues, supply chain factors, and industry-specific concerns are a few areas that would benefit from an in-depth exploration of related information security policy. Enhanced models and tools for analyzing and managing information security infrastructure investments are also needed. Certainly, research needs to be conducted into how well the life cycle meets the policy management needs of today's organizations and what improvements need to be made to ensure future success.

References

1. Baskerville, R. Information systems security design methods: Implications for information systems development. *ACM Computing Surveys 25*, 4 (Apr. 1993).
2. Gartner, Inc. *Nimda Worm Shows You Can't Always Patch Fast Enough.* Note FT-14-5524 (2001); www.gartner.com
3. Guttman, B. and Robach, E.A. *An Introduction to Computer Security: The NIST Handbook.* National Institute of Standards and Technology, 1995.
4. Hoffer, J.A., George, J.F., and Valacich, J.S. *Modern Systems Analysis and Design.* Addison-Wesley, Reading, MA, 1999.
5. Lichtenstein, S. Developing Internet security policy for organizations. In *Proceedings of the Thirtieth Hawaii International Conference on Systems Sciences.* J.F. Nunamaker, Jr. and R.H. Sprague, Jr., Eds. IEEE Computer Society, 1997.
6. Porter, M.E. *Competitive Strategy: Techniques for Analyzing Industries and Competitors.* The Free Press, New York, 1980.
7. Vernon, R. International investment and international trade in the product cycle. *Quarterly Journal of Economics 80.*
8. Wood, C.C. Writing InfoSec policies. *Computers and Security 14* (1995).

Jackie Rees (jrees@mgmt.purdue.edu) is an assistant professor of management at the Krannert Graduate School of Management at Purdue University, Indiana.

Subhajyoti Bandyopadhay (bandyos@notes.cba.ufl.edu) is an assistant professor of Decision and Information Sciences at the Warrington College of Business Administration at the University of Florida.

Eugene H. Spafford (spaf@cerias.purdue.edu) is a professor of Computer Science at Purdue University and the director of the Center for Education and Research in Information Assurance and Security (CERIAS).

This research was supported by the Center for Education and Research in Information Assurance and Security (CERIAS) and Accenture.