The recent well-publicized incidents of compromise in information systems security (e.g., the denial-of-service attacks on well-known web sites) have emphasized clearly one fact: while there are many products, tools and procedures for managing information security, there are none for managing security policy. This has resulted in an ad hoc approach to tackling problems as and when they arise. Simultaneously, the explosive growth of electronic commerce has forced many organizations into uncharted territory, with associated new risks. These new risks include increased exposure to theft and fraud, privacy and confidentiality issues and denial of service issues. We propose a policy framework called PFIRES, which takes a holistic view of the security issues of an organization, and at the same time, takes into consideration the dynamic nature of e-commerce.

PFIRES incorporates the current best practices and research, and addresses shortcomings in current practice. It borrows ideas from both the new product development life cycle and the systems development life cycle. It has four major phases: Assess, Plan, Deliver and Operate. Depending on an organization's current requirements, the progress through these phases might be accelerated or short-circuited altogether. PFIRES's unique approach emphasizes change in the organization's operating environment as the driver of its life cycle activities. This ensures that the organization takes a proactive rather than a reactive role in managing its security infrastructure. Finally, as a high-level policy management tool, PFIRES facilitates communication between senior management and technical security management, an indispensable requirement in today's business.

Background - why PFIRES?

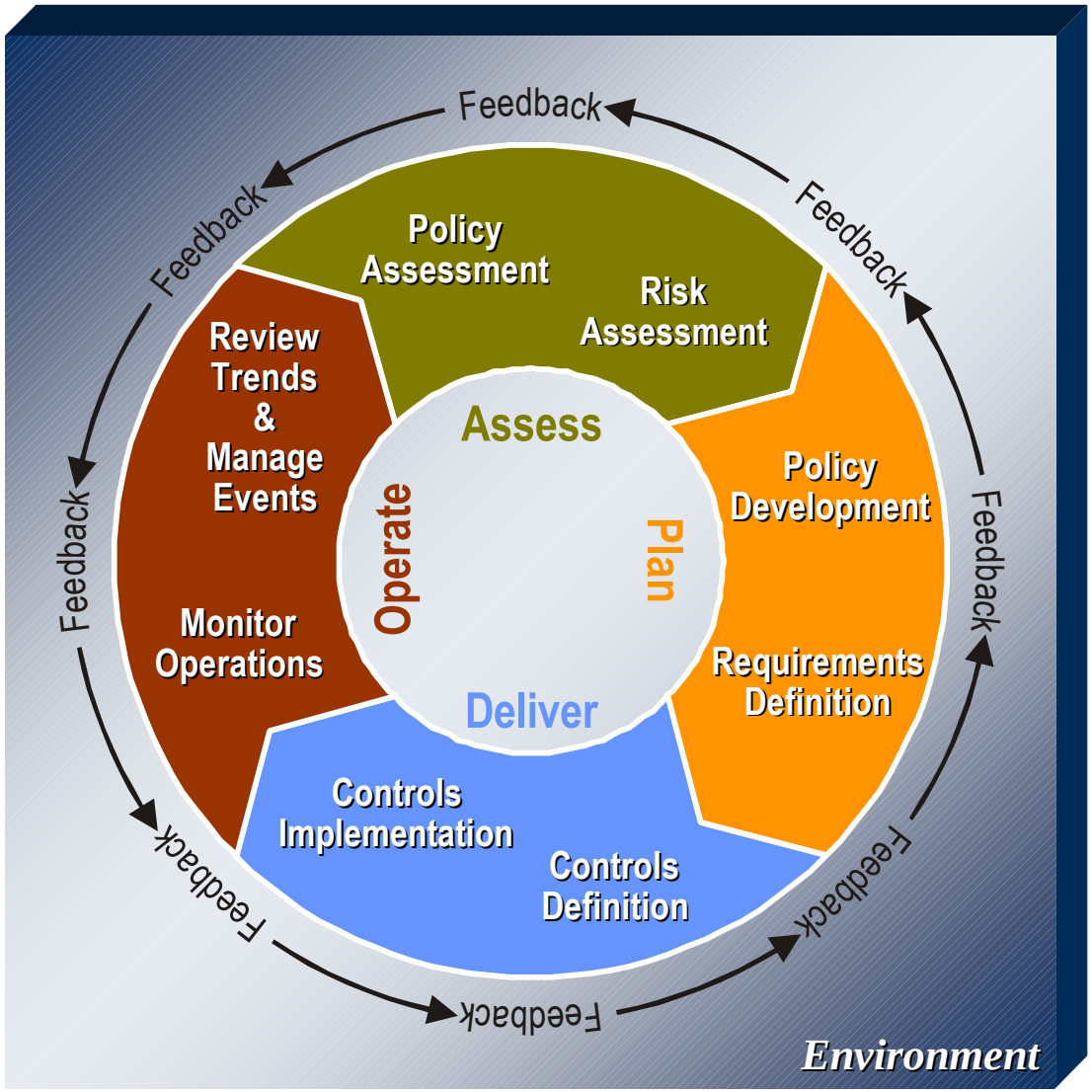
The basic requirements for e-commerce security include information confidentiality, authentication, authorization, data integrity, non-repudiation and availability. Given the dynamic environment of e-commerce, effectively meeting these requirements is not straightforward. The challenge is to come up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

One fundamental problem with current approaches to information systems security 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.

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. 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. PFIRES was developed borrowing from both the new product development life cycle and the systems development life cycle (SDLC).

The PFIRES model is not static. Depending on the situation, the various phases can either be gone through in detail or short-circuited. It is detailed enough to ensure that an organization does not overlook anything while addressing a security issue, while it is dynamic enough to ensure speed and execution to adopt rapidly to changing e-commerce scenarios.

The PFIRES model



Each of the phases consists of sub-steps as shown. It can be seen that policy development is an iterative process. Therefore the model includes feedback loops at every step.

Feedback is also a mechanism to ensure that the requirements of the previous steps are being satisfied.

The four principal phases in PFIRES

➢**The *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. In either case, the goal is to assess the proposed change against the existing policy and organizational environment. The outputs of the *Assess* phase are: a completed Policy Assessment; a completed Organizational "As-is" Assessment; a completed Risk Assessment; a decision on whether to implement the proposed change and a communications strategy and plan.

➢**The *Plan* phase**: Plan prepares for the implementation of the proposed change including creating or updating policy and defining the requirements for the proposed change. The outputs of the Plan phase are: the created/updated security strategy; the created/updated security policy; requirements for the change to be implemented and the continued execution of the Communications plan.

➢**The *Deliver* Phase**: The Deliver Phase is when the actual implementation of the policy takes place. The outputs of the *Deliver* phase are: an implemented proposed change; complete standards, guidelines and procedures and complete security controls for the proposed change.

➢**The *Operate* Phase**: The Operate phase of PFIRES 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.

In conclusion...

There are many products, tools, and procedures for managing information security, but none for managing security policy. These tools are fine in and of themselves, but if not organized around a solid security policy, they are likely to fail. PFIRES is a different kind of tool, one for high-level management of an organization's information and financial assets related to e-commerce – its security strategy and policy.

PFIRES's unique approach emphasizes change in the organization's operating environment as the driver of life cycle activities. By allowing environmental change to drive life cycle activities, the organization can assume a more proactive rather than purely reactive role in managing its security infrastructure. PFIRES also recognizes a continuum of change -strategic to tactical – providing relevant guidance for managing change in every shade of gray.

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

The entire document can be accessed via the WWW at:

http://www.cerias.purdue.edu/techreports/public/pfires.pdf

For more information contact:

Jackie Rees at jrees@mgmt.purdue.edu