Taylor & Francis
Taylor & Francis Group

Information Systems Security

ISSN: 1065-898X (Print) 1934-869X (Online) Journal homepage: http://www.tandfonline.com/loi/uiss19

The People, Policy, Technology (PPT) Model: Core Elements of the Security Process

Steven Schlarman CISSP

To cite this article: Steven Schlarman CISSP (2001) The People, Policy, Technology (PPT) Model: Core Elements of the Security Process, Information Systems Security, 10:5, 1-6, DOI: 10.1201/1086/43315.10.5.20011101/31719.6

To link to this article: http://dx.doi.org/10.1201/1086/43315.10.5.20011101/31719.6

Published online: 21 Dec 2006.

Submit your article to this journal

Article views: 29

View related articles

Full Terms & Conditions of access and use can be found at
http://www.tandfonline.com/action/journalInformation?journalCode=uiss19

Download by: [Purdue University Libraries] **Date:** 17 March 2016, At: 19:30

Downloaded by [Purdue University Libraries] at 19:30 17 March 2016

The People, Policy, Technology (PPT) Model: Core Elements of the Security Process

Steven Schlarman, CISSP

From the humble beginnings of singular technologies to solve specific security vulnerabilities to the concepts of building enterprise-level security programs, security has grown and matured. Security has been accepted at some levels as a necessary component of a successful business — not just a successful IT organization. How can the security process be broken down into simple elements? Is there a simple method to look at information security as a process? How do you measure for success or coverage and how do you identify areas of improvement?

If any successful process is broken down into its core elements, the following three items will usually be the result of that analysis:

1. People execute and support the process.
2. The process is defined with supporting procedures and directions.
3. Mechanisms, tools, and materials are used to facilitate the process.

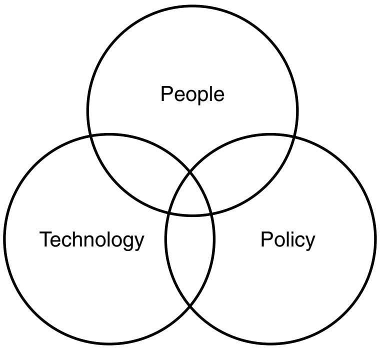
The process can be broken down into the simple core elements of people, policy, and technology.

□ *People* — the people executing the process
□ *Policy* — the support documentation and directions
□ *Technology* — the tools and materials

For example, take the process of building a house. There are the owners, the financers, and the builders. There are the blueprints, design specs, and building codes. And finally, there are the tools and materials for the house. From this simple analogy, it is not a stretch to apply this same concept to the world of security.

Steven Schlarman, CISSP, is a manager in the Technology Risk Services group of PricewaterhouseCoopers. He has been engaged in many differnt security consulting projects, including penetration studies, Enterprise Security Architectures, and computer crime investigation. In his eight years in the computer field, he has worked on system security, system maintenance, and applicaiton development on a variety of platforms.

EXHIBIT 1 People, Policy, and Technology Model



Downloaded by [Purdue University Libraries] at 19:30 17 March 2016

People, Policy, and Technology

The security process is a mixture of people, policy, and technology. Each element depends in some manner on the other elements. Also, issues receive greater coverage when the elements are combined. The control environment is greatly enhanced when these three elements work in concert. A simple drawing will suffice to illustrate this (see Exhibit 1).

This drawing shows the basic elements and also the coverage areas. As you move toward the union of the elements, the controls environment increases — there is greater coverage.

What are the core elements with regards to security?

People

This core element is the most important. The people element comprises the people and various roles and responsibilities within the organization. These are the people that are put in place to execute and support the process. A few key roles include senior management, security administrators, system and IT administrators, end users, and auditors.

Policy

This element comprises the security vision statement, security policy and standards, and the control documentation. This is basically the written security environment — the bible that the security process will refer to for direction and guidance.

Technology

This element includes the tools, methods, and mechanisms in place to support the process. These are the core technologies — the operating systems, the databases, the applications, the security tools — embraced by the organization. The technology then is the enforcement, monitoring, and operational tool that will facilitate the process.

The concept is that each core element could be measured for effectiveness and coverage. Also, issues can be measured against the model to determine what controls coverage there is for that issue. The objective then is to move issues into the intersecting areas of the elements — with the final objective of moving the issue into the middle area of greatest coverage. As risk issues are identified, each step to manage the risk will fall into one of the core elements of people, policy, or technology. If the issue is resolved with one of the elements, addressing one of the other elements can enhance this resolution. As the core elements are added to the controls environment and utilized in concert, the issue is then resolved on several fronts. The controls coverage is greater.

The PPT Model

The PPT Model can be illustrated with a few simple examples. Exhibit 2 shows the PPT Model with regards to Internet usage and misuse.

□ Users are educated on the proper usage of the Internet. The control environment relies solely on the user.

□ An Internet usage policy is written to document proper use of the Internet and the consequences of misuse. The control environment now is supported by two of the three

Downloaded by [Purdue University Libraries] at 19:30 17 March 2016

EXHIBIT 2 Internet Usage and Misuse

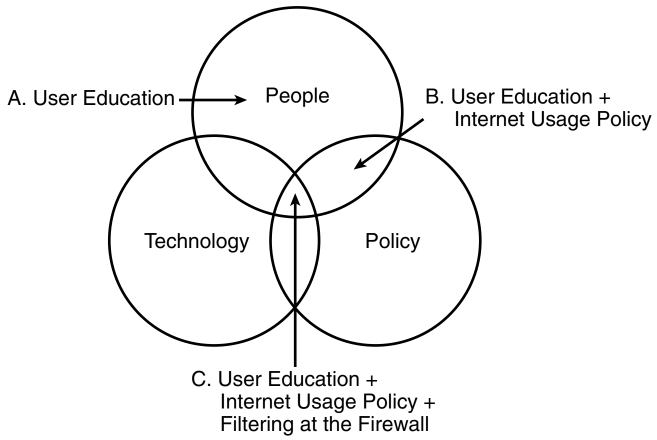
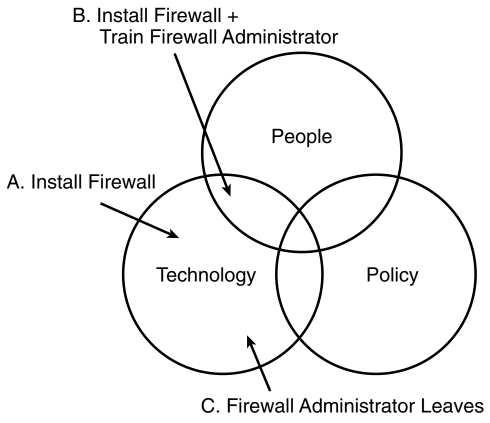


EXHIBIT 3 Internet Connection: Coverage with Two Elements



core elements.

□ Filtering software is deployed on the firewall. Now the control environment is covered by all three elements.

Exhibit 3 demonstrates when an issue is covered only by two of the three elements. It also shows the consequence of a limited controls environment.

□ The Internet connection is protected by the deployment of a firewall. Core elements coverage = 1.

□ The firewall administrator receives specialized training and develops the skill set necessary to administer the firewall. Core elements coverage = 2.

□ The firewall administrator leaves the organization. The controls now rely back on just one element — the technology.

How can the model be used to identify an alternative solution to Exhibit 3? This is depicted in Exhibit 4.

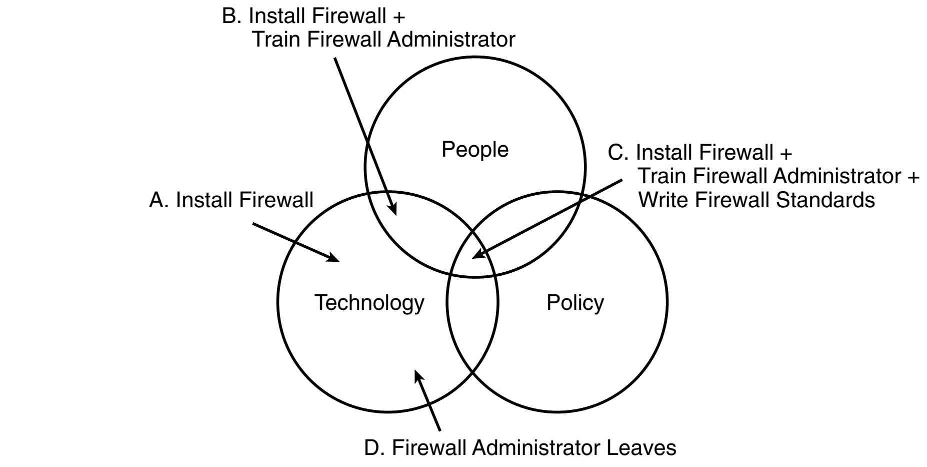
□ The Internet connection is protected by the deployment of a firewall. Core elements coverage = 1.

□ The firewall administrator receives specialized training and develops the skill set necessary to administer the firewall. Core elements coverage = 2.

□ Firewall operating standards are written and controls are documented. Core elements coverage = 3.

□ The firewall administrator leaves the organization. The controls environment relies on two of the core elements. The controls, standards, and technology are documented so that the skill and knowledge does not completely leave the organization. Core elements coverage = 2.

EXHIBIT 4 Internet Connection: Coverage by Three Elements



From these examples, it is easy to see how the PPT model can simplify the analysis of a risk issue. If the issue is broken down into the three core elements, action items can be determined for each core element. In this manner, control coverage can be moved from one element to two, and ultimately to coverage by all of the elements.

DEPTH OF COVERAGE

Measuring an issue against the PPT model hinges on determining the level of coverage for each element. If a core element is missing, then activities should be identified to address that element, i.e., ensure that there is coverage by each element. The next step after identifying that the issue is covered by each element is to measure how deep the coverage is for each element. For instance, users may be educated on Internet usage policies. But if that education is not continual or updated, the coverage will fade over time. Also, technologies may be deployed to resolve certain issues, but if the technology is not monitored, updated, and maintained, the coverage deteriorates. Therefore, each element should be measured independently for depth as well.

The following are some suggestions on different aspects of each core element to measure.

□ People
- What level of management commitment is there? What role does the management play in the process?
- What resources have been put in place to execute the process? Support the process? Monitor the process? What skill sets are utilized? How experienced are the people executing the controls?
- For the resources deployed, how much training has been given to the people community surrounding the issue? For instance, the firewall administrator received specialized training. What level of training was received?
- What is the continued education process? How often does the person receive training? Is the training available for all people elements of the issue?
- How often does the people element turnover? What process is there to replace skills or continue to improve controls awareness?

Downloaded by [Purdue University Libraries] at 19:30 17 March 2016

Downloaded by [Purdue University Libraries] at 19:30 17 March 2016

A complete controls environment should lie in the intersection of each core element. Coverage in each element provides a layered approach — controls are not relying on one element alone.

□ Policy

– What documented direction is provided surrounding the issue? At what level is the policy authorized? How detailed are the policies, standards, or documentation?
– Is the issue addressed within the general security policies of the organization? How often is the issue reviewed from this perspective?
– How is the policy communicated to the organization — the people element? What methods are used to communicate the standards?
– For technical issues, is each component addressed from both a controls perspective and an operational perspective? For instance, in the case of the firewall, are standards written for the firewall deployed? The operating system? Are there operational standards written for activities such as change control, log retention and review, system monitoring, etc? Is this part of the overall security policy?
– What policies are documented to monitor and review the controls environment? Is there a documented compliance process?
– What supporting processes — such as information classifications, risk assessments, or self-audits — are documented for the controls environment?
– Do the policies or standards address consequences for violations? What policies are laid out for incidents or response?

Technology

– What technologies are in place to execute the controls? To monitor the effectiveness of the controls? To sustain the controls environment?
– What functions and features are utilized in the core technologies (operating systems, databases, etc.) for controls? What security or controls-related technologies are deployed to supplement the core technologies?
– How often is technology solution reviewed? How are the technologies implemented? What is the implementation process?

By drilling down into each core element, the depth of coverage can be determined as well. Exhibit 5 uses the Internet connection example.

From this example, there are obvious layers of coverage within each element. A simple coverage is better than none — but there is strength in depth.

CONCLUSION

The PPT Model is not intended to be a detailed review of the controls environment. The model provides a technique to analyze the controls environment against a simple benchmark. This measurement can identify controls coverage as well as identify possible holes or areas that can supplement the environment. By dissecting a risk issue into the three elements of people, policy, and technology, a measurement of the controls coverage can be ascertained. From this, action items can be determined to address the missing items. Then, each element can be drilled down into to provide not just coverage, but depth of coverage.

A complete controls environment should lie in the intersection of each core element. Coverage in each element provides a layered approach — controls are not relying on one ele-

Downloaded by [Purdue University Libraries] at 19:30 17 March 2016

EXHIBIT 5 Drilling Down Using the Internet Connection Example

Element	Coverage	Greater Coverage
People	Firewall administrator receives specialized training.	Firewall administrator receives specialized training. Firewall administrator is required to attend annual training sessions to remain current with the technology. A firewall team has been deployed to provide backup coverage for the main administrator. An IT auditor has been assigned to perform compliance testing against the firewall on a periodic basis.
Policy	Standards are written for the specific firewall product.	Standards are written for the specific firewall product. Standards are written for the operating system the firewall is deployed on. A technical security architecture is drawn up for the Internet connection. This diagram illustrates the entire Internet connection. Policies and standards are written for firewall rules, backup and recovery, log retention and review, incident identification, and escalation procedures. A standard is written to document ongoing periodic technical compliance reviews of the firewall, operating system, and overall Internet connection. A risk assessment policy is written to impose an annual risk and vulnerability assessment of the Internet connection. A job description with responsibilities and standard operating procedures is written for the firewall administrator.
Technology	A firewall is deployed.	A firewall is deployed. The firewall is supported by a secure router configuration. A demilitarized zone (DMZ) is utilized as a standard Internet environment. An intrusion detection system is deployed to monitor and log activities. Vulnerability scanning tools are used against the firewall to test configurations.

ment alone. Therefore, there is a mixture of people, policy, and technology involved in the security process. If each core element is addressed, then the depth of each core element can be addressed. With this depth of coverage, the controls environment is enhanced on many fronts.

In the end, security relies on the controls environment in place. Security always will succumb to the weakest link. However, if the controls environment covers issues from many angles, a system of checks and balances can mitigate some of the weaker links. Risk can be managed — not necessarily eliminated. The PPT Model gives one perspective on how to develop this overlapping environment. ■