Topic 1: Obstacles to Successful Implementation

Implementing a developed computer network security policy is oftentimes difficult to accomplish. What are some of the obstacles to computer network security policy implementation? Post your findings and respond to at least two of your classmates’ posts.

9/27/2014 12:53:08 PM
I’ve worked in IT for 20+ years now, and I can honestly say almost anything can hinder policymaking in general. For the security policy specifically, I noticed in the chapter 10 slides it mentions financial, priority, time, staff, scope, procurement, organization feasibility, training, and governance (Whitman & Mattord, 2011). Those are quite a few things that can influence policy! I went looking for an article that would condense these down and explain some of them further, and I found *Five Reasons Why Security Policies Don’t Get Implemented*, by Charles Cresson Wood. The article elaborates on five issues; they are (Wood, 2011):

1. Failure To Explicitly Define Long-Term Implications
   This basically means the original scope of the project was not clearly defined and does not anticipate the activities and events that may negatively affect the company. For example, let’s say Security Manager X was trying to implement a policy to remove access to Facebook from all computers (because it’s a waste of time and possible security risk). Unfortunately, a few months later it comes to light that HR, PR, marketing and several other departments use Facebook on the behalf of the company daily. Without Facebook, the company would lose revenue.

2. Full Cost Analysis Not Employed
   This is exactly how it sounds; implementing a policy did not anticipate all the costs (current and future) associated with the policy. A good example of this could be seen in scalability. Security Manager X would like to implement a policy for training staff (which is good); however, neglects to mention how much it will cost to administer and maintain the technology itself.

3. User Training & Acceptance Efforts Not Undertaken
   Another obvious obstacle is obtaining user acceptance. This could be something as something as simple as convincing the company that granting (or taking away) access to social networking sites would be in the company’s best interest. If at any time executive management, or management in general comes, disagrees with implementing such a policy, the policy could come to a dead stop. A great of getting user approval is through training exercises, workshops, and even just meetings explaining the benefits of the policy.

4. Discovery Of Unforeseen Implementation Conflicts
   Something that can also hinder a policy becoming active is unforeseen problems. Let’s say a new security policy says all individual sites must have their own data center. This sounds great on
paper, but many issues could prevent a policy like from becoming active, such as proper funding, 
procuring of the space needed, power consumption, and hiring the appropriate IT staff to manage 
such facilities. Unless all the factors have been anticipated and discussed, there is a good chance 
the policy won’t become active.

(5) Communications Gap Between Technologists & Management
Finally, and almost the most obstacle, communication issues may arise between those driving the 
security policy and management---this would be considered part of getting buy-in from 
management. There is almost always a change management process that be strictly adhered to 
when creating and implementing a new policy. Likewise, while the policy is being designed, 
tested, and implemented, management must continually be updated. Failure in maintaining an 
open line of communication with management will most likely result in the security policy not 
making it into production.

References


Wood, Charles Cresson. (2011/1). Five reasons why security policies don’t get implemented. Retrieved from 
don%E2%80%99t-get-implemented/

Topic 2: Unit 2 Hot Current Security Breaches

What is a hot issue this week in the security arena as it relates to this unit’s topic? 
Summarize one of these issues on the message board, and respond to another person’s post.

9/27/2014 3:20:53 PM
The hot topic of the week I have found is raising awareness when it comes to computer security. 
Specifically, the article from Time of Oman, Call for awareness to prevent cyber security frauds, by Times 
News Service, sheds light on criminal activity surrounding cyber-attacks. These would include people and 
businesses that fall prey to hackers using email addresses, usernames, passwords, and social engineering 
to exploit company security systems. Once hackers have gained access to a company, major security 
breaches can continue to happen, including viruses, worms, malware, and spam. The primary focus of 
the article was awareness, and thus suggesting the only way to prevent such cyber-attacks is for IT security to 
be human-centric…and not just technology-centric (Times News Service, 2014). Meaning, that all security 
policies should factor in education and awareness programs to train staff on properly identifying what
cyber-attacks look like. The reason this article was written was to highlight a technology seminar of Muscat ICAI, or Muscat Chapter of the Institute of Chartered Accountants of India. What I got from the short article was that awareness itself is possibly the most important element in creating security policy.

Reference


9/25/2014 7:44:00 PM
Those are good points Carolyn. I’m also trying to think of just IT issues in general, and then relate those to security. An issue that comes to mind is perimeter security. The reason I say perimeter security is because, like you mentioned, it could include a firewall…but it also could include physical staff, as in security guards. For example, let’s say we were to implement a security policy where security cameras were installed in the data center and in busy IT areas---and required a guard to monitor those cameras. Right away, you see there could be a possible issue getting the security guard (a full-time employee) position authorized by the department and HR.

9/26/2014 5:08:57 PM
Done

9/27/2014 3:30:26 PM
You’ve made some excellent points about the security surrounding the iPhone biometric finger scanner. I am sure Apple meant well, but not really be known for security, has proved once again to be easily exploitable. If you have an iPhone, which I do, I follow the security exploits (and even test them). When iOS6 came out, there was an exploit to easily bypass the passcode to gain access to pictures and contacts (I tested this, and it worked). But, when Apple released the 6.1.3 bug fix (to fix some common bugs), it too was easily exploitable…and still gave people access to the phone. Take a look at this article: http://www.dailymail.co.uk/sciencetech/article-2296947/iOS-6-1-3-bug-fix-New-iPhone-lock-screen-hack-DAY-Apple-released-update-fix-passcode-flaw.html

I think what Apple needs to do is hire hackers...specifically ones that are experts in hacking phones.

9/28/2014 1:37:29 PM
I saw several great points in your post, especially the ones that had to do with complex security policies and enforcement. Something I believe many companies battle with is time. Even if you have a great security team, it does not mean they will have time to educate the staff about security,
and may have even less time to spend enforcing the policies. I've seen several great mechanisms put into place to assist with the time factor. One is using software and sites like Netlearning to educate the staff. Netlearning is setup like an online course. Security concepts can be added into course-like material, and then an employee can study, take quizzes, and receive updated information. I also like email...well, I used to anyways. Email can be a great way to communicate with employees; however, only if employees aren't being inundated with other emails. I say email, because it would be nice to receive security alerts, as they can affect the company. Some companies even broadcast radio or TV. These mediums can be a great way to relay information, especially security alerts, to the masses.

Security Policy Implementation

In this unit you will learn how to implement a computer network security policy. Once the security policy is developed, it must be implemented.

Implementing the security policy is often the most difficult aspect of the security systems development life cycle. The process includes changes to procedures, people, hardware, software, and data (Whitman & Mattord, 2012).

Outcomes

After completing this unit, you should be able to:

- Implement a security policy within a Microsoft Windows environment.
- Demonstrate how to join a Linux® system to an Active Directory Domain.
- Discuss the importance of a strict password policy.

Course outcome(s) practiced in this unit:

IT540-1: Implement a computer network security policy.

What do you have to do in this unit?

- Complete assigned Reading.
- Complete the Learning Activity.
- Participate in Seminar or complete Alternative Assignment.
- Participate in Discussion.
- Complete unit Assignment.

**Project Plan:** A program that delivers instructions to individuals for carrying out the implementation stage of the security systems development life cycle.

**Predecessors:** In a project plan, the tasks or steps that are taken before the specific task at hand.

**Work to Be Accomplished:** The work to be accomplished includes activities and deliverables.

**Deliverable:** A completed document or program module.

**Assignees:** Persons who are assigned to the project based upon their specific skill sets.

**Task Dependencies:** The dependence of the action step at hand upon action steps that come before or following.

**Project scope:** Describes the amount of time and effort-hours needed to deliver the planned features and quality level of the project deliverables.

**Bull's-Eye Model:** A proven method for prioritizing a program of complex change.

**Change control:** A process to assure an organization that the changes to systems are managed.


**Assignment Grading Rubric**
Course: IT540 Unit: 2 Points: 116
Copyright Kaplan University
Unit 2 Assignment
Outcomes addressed in this activity:
Unit Outcomes:
- Implement a security policy within a Microsoft Windows environment.
- Demonstrate how to join a Linux system to an Active Directory Domain.
- Discuss the importance of a strict password policy.
Course Outcome:
IT540-1: Implement a computer network security policy.
Instructions

Deliverables
Provide the Lab Report file, including screen captures of the following step(s):
- Part 1, Steps 29 and 36
- Part 3, Step 33

Write your report in the standard APA style. Your output should be at least four double spaced pages, exclusive of the title page, abstract, table of contents, and references section.

Assignment Requirements:
- Answers contain sufficient information to adequately answer the questions
- No spelling errors
- No grammar errors

*Two points will be deducted from grade for each occurrence of not meeting these requirements.

For more information and examples of APA formatting, see the resources in Doc sharing or visit the KU Writing Center from the KU Homepage.

Also review the KU Policy on Plagiarism. This policy will be strictly enforced on all applicable assignments and discussion posts. If you have any questions, please contact your professor.

Review the grading rubric below before beginning this activity:

Course: IT540 Unit: 2 Points: 116

<table>
<thead>
<tr>
<th>Assignment Requirements Points</th>
<th>Possible Points</th>
<th>Earned Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Create a domain level security policy in Windows.</td>
<td>0–48</td>
<td>0–48</td>
</tr>
<tr>
<td>2. Join a Linux system to a Windows Active Directory domain.</td>
<td>0–44</td>
<td>0–44</td>
</tr>
<tr>
<td>3. Explain the significance of a strict password policy.</td>
<td>0–24</td>
<td>0–24</td>
</tr>
<tr>
<td>Column Total 0–116</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Less deduction taken for spelling, grammar and APA errors. Plagiarism is totally unacceptable.

New total after deductions

Attending live Seminars is important to your academic success, and attendance is highly recommended. The Seminar allows you to review the important concepts presented in each unit, discuss work issues in your lives that pertain to these concepts, ask your instructor questions, and allow you to come together in real time with your fellow classmates. There will be a graded Seminar in Units 1 through 5 in this course. You must
either attend the live Seminar or you must complete the Seminar alternative assignment in order to earn points for this part of the class.

**Option 1: Attend Seminar:**

The following will be covered in this week’s Seminar:

- Principles of implementing a computer network security policy
- Importance of accepting change pointers for the Unit 2 Assignment

**Option 2: Alternative Assignment:**

You will benefit most from attending the graded Seminar as an active participant. However, if you are unable to attend you have the opportunity to make up the points by completing the alternative assignment.

**Assignment Instructions:**

Complete the following research assignment. Submit your answers in a single word document to the Dropbox.

Research and answer the following: Why implementation of the network security policy must be carefully planned.

Your paper should be a minimum of three to four pages in length, double spaced, in APA format and cite all references used. Submit to the Seminar Dropbox.