Building a Security Policy Framework for a Large, Multi-national Company

Leslie VanCura

Building a Security Policy Framework for a Large, Multi-national Company

Leslie VanCura
GSEC Practical
Version 1.4c -- Option 2
January 20, 2005

Table of Contents

Abstract

Information Security is not just technology. It is a process, a policy, and a culture. Our organization had spent millions of dollars on technology to keep the "bad guys" out, but we had spent little time building the foundations of our Information Security Program. We did not have relevant, current policies or a culture of security awareness among our managers or end users. The technology was not able to prevent end users from disabling it or doing unintentional damage by opening strange email attachments or telling someone their password. This paper will discuss how we created a Security Awareness Program to address this problem. The program covers policy development, an awareness campaign, and compliance monitoring. The program starts with a plan and steps through each phase of:

- Developing the framework
- Defining policy
- Determining a review process
- Writing the documents and having them reviewed
- Generating end user awareness about the updated policies and general security topics

We are two years into a three year plan, and we begin the compliance monitoring this year. We are already gaining benefits from having well defined policies and security awareness is becoming part of our corporate culture.

Call to Action

Our call to action began when we hired an external consultant to perform a Security Assessment. The final report showed that we had many gaps. Most of the gaps, though, kept coming back to inadequate security policies and a total lack of an awareness program. Our current IT Security Team was focused on technology, not process. That was about to change.

The next couple of months were spent making the case to management that the security team's charter needed to change from selecting anti-virus, intrusion detection, and other security tools to a process oriented team that would build a Security Awareness program. "A Security Awareness Program involves defining your baseline (the policies), communicating them (awareness), and evaluating your success (compliance monitoring and vulnerability assessments)."[1] That awareness program included rewriting our policies and procedures, developing an awareness campaign, and compliance monitoring.

We built a three year plan to move us into this new role. Our three year plan defined that we would focus on policy development in year one, pick up the awareness campaign in year two, and pick up compliance monitoring in year three. Notice, that each year added effort, but didn't drop any. By year three we

would be working on all three prongs of the program at once. One of the biggest challenges was how to get this program to work in a very large global organization. We had several different business units with over 50,000 systems spread across the globe. Each business unit had their own information technology (IT) group and they were given freedom to do what seemed best for their business needs. Laying out the high level plan was easy, now we had to execute the plan.

Current State of Affairs

Our plan included assessing the current policies and procedures and identifying how much our end users knew about them. We did this by finding and reviewing the current policies and procedures and by having focus group sessions with end users.

The good news was that our policies were on-line on the IT Security Team's web site. That was the only good news. The 40 plus policies and procedures were organized in a long list with not grouping based on topic or technology. It was difficult to find the policy or procedure that applied to a given question. There were many gaps in what was covered. They were written in legal terms that required reading them several times to get an idea of what was trying to be conveyed, and most of them had not been updated in over four years.

Next we held the focus groups. We worked with a neutral, third party facilitator to draft questions about the policies and basic security terms. This facilitator also led the sessions with the end users and managers. We held separate sessions for the managers so that the end users would feel more comfortable to answer the questions truthfully. We learned a lot from these sessions. None of the managers knew what the data protection policies were, about half of the end users did. The managers had the mind-set that security wasn't their job; it was the IT Security Team's job. Very few of the participants knew what the term "Social Engineering" meant. The most telling of all was a comment made by an end user about how the current policies were written. His statement was "Don't try to impress me with all of the legal jargon, just tell me what I can and cannot do in plain English!" That was a great place to start when we began to rewrite the policies. We were starting from a position of no policy awareness and an idea that security wasn't part of everyone's job, only the IT Security Team was responsible for protecting our information.

How to Proceed?

Based on both assessments, there were many things to get started. But where do you start? Based on the focus group feedback, the program needed some sort of framework to convey what was trying to be accomplished as well a way to show progress. Also I needed a format for the documents that could convey what the topic was, who was impacted, and what the rules were. I would need to get a lot of groups involved to review the framework and documents to make

sure they would work at our global company and to get their buy-in to the new processes. I would need some technical writing skills to help put all of this into "plain English". Once some of the policies were written, how was I going to let the end users and managers know what the new rules were? Who were our target audiences?

This was not something that I wanted to invent on my own. There had to be models available from consultants or the Internet. One of my requirements was that the framework of our policies had to make sense to the end users, not just our IT Security Team.

Defining the Framework

My research started on the Internet. There were many options to look at based on the CISSP model, the ISO 17799 model, and how different universities had set their own policies up. I narrowed my review to the CISSP model, the ISO 17799 model, and Bindview/Meta Security Groups' solution. I first looked at using the 10 disciplines in the CISSP model. I went to the $(ISC)^2$ web site[2] and wrote down the 10 areas.

1. Access Control Systems and Methodology
2. Applications and Systems Development Security
3. Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)
4. Cryptography
5. Law, Investigation and Ethics
6. Operations Security
7. Physical Security
8. Security Architecture and Models
9. Security Management Practices
10. Telecommunications and Network Security

Next, I bought a CISSP Prep Guide[3] and reviewed the definitions and content of each of the 10 domains. I tried to put our existing policies and procedures int the domains. I realized this model would not work. Almost all of the existing documents fit into the Operation Security domain. With most of the documents in one category, our end users would still have a long list to search. They would have to figure out that the Email Procedure was in the Operations Security domain, and that was not likely. Some of the other domains like Cryptography and Security Architecture would generate confusion and questions that were not pertinent to our goal of improving security awareness.

I turned to the ISO 17799:2000(E) Standard[4] and looked at their classification of information. There were 10 areas listed:

1. Security Policy
2. Organizational Security

3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Systems Development and Maintenance
9. Business Continuity Management
10. Compliance

This seemed to be a possible fit for our organization. After reviewing the standard I still had a lot of questions. I tried to categorize our documents into the ISO model. I struggled with where to put them. I was pretty sure our end users would not figure out where the Acceptable Use Policy was (Compliance). I wasn't sure how to communicate what Organizational Security was to our end users and IT administrators in a way they would remember.

That led me to the third alternative, the Bindview/Meta Security Group Policy Operations Center solution. This solution had 7 categories to group policies in:

1. Asset Identification and Classification
2. Asset Protection
3. Asset Management
4. Acceptable Use
5. Vulnerability Assessment and Management
6. Threat Assessment and Monitoring
7. Security Awareness

This framework was much easier for the business managers to understand. As I categorized our existing documents, it was relatively easy to determine where each of them fit. Additionally, the solution came with lots of industry research compiled in one place and policy templates. This information gave me the confidence that this was the model for us to use. After reviewing all three options with the IT Security Team, the team agreed with my recommendation of using the the BindView/Meta Security Group solution. We added Physical Security and Business Continuity & DRP to better represent our organization. We weren't going to write the physical security policies. We were going to link to the existing ones from the other two security organizations to help the end user have all of the information in one place. Definitions of each category are in Appendix A. Our final framework is shown below:

Figure 1: Policy Framework

Defining Policy Structure

I needed to define what a policy is for our organization. What is a policy? According to the American Heritage Dictionary of the English Language a policy "is a plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters."[5] Our end users look at policy as "what I can and cannot do". I would use policies and procedures to guide our decisions and actions.

Initially I used the word Standards instead of Procedures, but after many explanations and confusion, I switched back to Procedures. This seemed to fit our company culture better. I could refer to policies and procedures, and our end users and business managers understood what we were talking about. It didn't really match industry terminology, but we went with what worked.

Policies would be the high level documents that would support our corporate level information security policy. Procedures would have more detail, but would not be an operational process document. Policies and procedures would be firm requirements that must be met. If they couldn't, the end user would need to get an exception approved by their management and the Security Manager. We also had a lot of best practices we wanted to communicate, but they weren't firm requirements. I elected to call those guidelines and checklists. These were not requirements. The structure of our policy information is shown below:

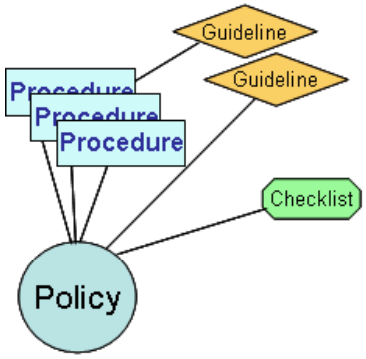

Figure 2: Framework Details

As an example, we would outline our Acceptable Use category like:

A. Acceptable Use Policy
    a. Frequently Asked Questions
    1. Email Security Procedure
        a. Email Security Guidelines
    2. Instant Messaging Procedure

Now that I had the framework and details defined, I needed to group the existing policies and procedures into the framework and identify the additional policies that needed to be written. We had about 40 existing documents. After all of the research into ISO 17799 and the CISSP domains, I added an additional 25 procedures to the list. There is no set rule on what policy or procedure is needed for a company. You must look at your own company's culture and risk posture and make that decision. I grouped the documents by category in an Excel spreadsheet so that we could track progress.

Define the Review Process

I was ready to start writing, but knew that we needed a well defined review process to assure that what was set as policy could actually be done in our environment, wasn't too strict, and could be enforced. Our company is very entrepreneurial and risk tolerant. So, as an example, I could not restrict Internet usage to only business activities. That was not the current practice at our company and would be seen as too draconian. Based on information from the focus groups and meeting with various IT managers, I developed the following process:

1. Identify policy or supporting procedure to be written
2. Research best practices on the topic
    a. Industry experts (Security Focus, CSI, SANS, ISO 17779, CIS, etc)
    b. Current company practices
3. Start with a template
4. Apply technical writing techniques
5. Incorporate current policy or procedure

6. Review the document and make updates with the:
    a. IT Security Team
    b. Content Experts (some times they were on our IT Security Team)
    c. Security Advisory Team (SAT)
7. Once a policy was approved by the SAT, it was submitted to the Chief Information Officer (CIO) for final approval. The SAT and Security Manager had final approval authority for procedures.
8. Review each policy and associated procedures at least every two years for currency and relevance.

Management Review

Now that I had the framework, categorization, and process defined, it was time to present this approach to management for buy-in and approval.

I presented this approach to our CIO and his direct reports. All agreed that this was a good approach and volunteered people from their organizations to be on the Security Advisory Team. This assured me that I would get feedback from all of our various IT organizations and from the regional organizations. Additionally, I included representatives from our Worldwide Security (the physical security side of the organization), Legal, Audit, and HR organizations to make sure our policies were in compliance with regulations and corporate policies. By using the Bindview/Meta Security Group solution, instead of making up our own, our program gained instant credibility because it was based on industry standards from well know security companies. The IT Leadership Team felt even more comfortable with the process, knowing that their organizations would have input into the policies and procedures.

We communicated the framework, process, and expectations to the Security Advisory Team members through several conference calls and meetings. We wanted to make sure they understood that their input was vital to the success of our program.

Getting Started

It was time to pick the first policy and start writing. Actually, first I attended a technical writing class that taught me how to write technical information for the general user. The key points from the class were:

- use more personal pronouns
- write in an active tense
- use shorter sentences
- use bulleted lists, not long paragraphs

Being from a technical background, I realized I had a lot of bad habits to break. I use the techniques I learned when writing policies, end user communications, and emails.

I decided to re-write our Acceptable Use Policy first because it was out of date, currently focused only on Internet use, and generated a lot of questions from end users. I reviewed many templates including those from the Policy Operations Center (the Bindview solution we purchased), SANS, TechRepublic, and SecurityFocus. I met with our Investigations Team to see what they needed to be in the document for their purposes. I reviewed our HR policies to see what they said about acceptable behavior at our company. I had a lot of information gathered, and now needed to put it into a reasonable format that everyone could understand. The document needed to:

- state the purpose of the policy
- identify who was affected
- define what type of systems were covered
- define the requirements
- define end user and management responsibilities
- define the exception process
- outline the repercussions of not following the policy

I also wanted change control and effective dates associated with each change that would be made as we moved forward. The documents would need to be considered relatively dynamic at first as the Security Advisory Team refined what could actually be done and enforced in a global environment.

After looking at the many templates and our corporate standards, I decided to use the following outline for all policy and procedure documents:

- Purpose
- Scope
- Who is Affected
- Requirements
- Responsibilities
- Enforcement and Exception Handling

I elected not to include a glossary with every policy, but to have an overall glossary with hyperlinks from each document. I wrote the policy, using a lot of information from a TechRepublic white paper[6] that laid out areas to consider in an Acceptable Use Policy like:

- Authorized usage
  - Defines when corporate systems could and could not be used. Was it only for business or business and incidental personal use?
- Default privileges
  - Defines what default access is given to a user account and that other information requires specific authorization.
- User separation

    - Defines that each user must have a unique account and password to access resources with.
- User accountability
    - Defines that the user should never share their password and that the account owner is responsible for anything done with his/her account.
- No guaranteed privacy
    - Privacy of information on the corporate network cannot be guaranteed. It isn't intentionally being reviewed, but may be during the course of regular system maintenance and troubleshooting.

The final policy ended up with 11 specific requirements including the 5 from the TechRepublic paper. My goal was to create a policy that at least 80% of our end users could follow most of the time – not one that was ignored.

Now that I had a draft, I sent it to the IT Security Team to review. We had several meetings to review every sentence in the policy. The IT Security Team's responsibility was to make sure we could all stand behind the document once it was approved and verify that it was technically sound. Ideas that were controversial were discussed and edited until we could reach consensus on the issue. It was a grueling process, but we ended up with a much better document. Once those updates were made, the policy was sent to the Security Advisory Team. I specifically asked each member to consider whether the overall flow and organization was clear, if they could follow the key concepts, did they understand the terminology, did I leave out something important, and did they agree with the overall philosophy of the document. I gave them a due date for their feedback and waited for their responses. I also asked them to have others in their organization review the document to make sure that we didn't miss something important.

I was amazed at the response and feedback I received. The team thoroughly reviewed the document and made a lot of changes. They asked for more detail and examples in some areas and asked for clarifications in other areas. It took several iterations to get full approval from all of the members. One of the big changes that took me by surprise is that they wanted each document and requirement to be numbered so that they could ask questions and refer to requirements more easily. I sent our final version to the CIO for review and approval. He approved it with no changes. The process had taken five months to complete. I had one finished and about 70 more to go.

Creating Awareness

Now that I had a new policy, how was that going to be communicated to the end users? First, I needed to define who the key audiences were. There are three major audiences: the IT organization, the end users, and management. Our end user group is very technical and computer savvy. I needed to consider this fact when creating communications. They tended to read things very literally, so the

information had to be presented in a straight-forward manner. There were several communication options available to use:

- Email all end users
- Article in on-line internal newsletter
- Tri-fold brochures available in break areas
- Posters
- Lunch time seminars
- Policy on-line

I decided that a global end user email was probably too much for our first policy change. I elected to write several articles for our internal newsletter and to create a tri-fold brochure that could be passed out at department meetings and made available in break area information centers. I sent the article and brochures to the regional representatives so that they could use the information and have it translated into local language as needed. A sample article is in Appendix B. Working with the team, we also revamped our IT Security Team website to better communicate our goals and the policies. The policy page uses the same framework to present the policies as we presented to the Leadership Team. A key word search was added to make it easier to find specific procedures. The forms of communication that were selected hit the broad spectrum of our end users. It did not target any of them specifically.

As I added more policies and procedures, I continued with the communication plans, using all of the options available. The more I communicated the more questions our Security Team was asked. In year two, I developed an awareness program for the IT Operations Team. This was IT Security's first chance to educate one of our target audiences about security best practices and the new policies. The outline of the training was:

- Review of the Basic Principles of IT Security
- An externally developed video that covered topics like social engineering, password protection, and mobile computer use
- Company Specific Security Metrics
- Company Specific Case Studies based on actual investigations
- Specific policies and procedures that were pertinent to the organization

It was mandatory training for the organization and 95% of their team of 300 people attended. The regions and several business units asked for us to present the same training to their organizations. At the same time the Security Manager was also asked to start presenting the state of security at our company to the Business Executives and Managers.

The team had been communicating to our three primary audiences, but I felt we still needed something else to communicate to the general end users. We all get so many emails and newsletters that we stop paying attention to them.

As I presented the Security Awareness training to the CIO and his direct reports, I requested that the CIO assist us with sending an email to all employees about the importance of information security. The CIO agreed that this was worthwhile and started brainstorming with us. The email developed into a short, internally developed video about Information Security Awareness with our CEO, CIO, and Directory of Worldwide Security speaking on the video. The speakers outline the importance of information security as it related to each of our employees, share holders, and company. I worked with our Worldwide Internal Communications organization to disperse the video globally into all of the department meetings in the fourth quarter. The Communications Team helped me provide a version with English sub-titles for Europe and Asia, and a Kanji sub-titled version for Japan. The subtitles and translation as well as using our internal communication processes really helped spread the awareness corporate wide.

Where Are We Today?

We are two years into our Security Awareness Program and it is going well. Our program was based on policy development, awareness, and compliance. Our end users are more knowledgeable about our policies and actually quote them when asking questions. Our original framework is still in place. We have tweaked the location and names of various policies and procedures. We continue to get great feedback from our Security Advisory Team. We are making good progress on rewriting and adding policies and procedures. We are about 50% complete. The policy effort did slow down as the awareness activities increased. This was due to resource constraints. Our awareness campaign is in full swing with monthly awareness articles, site visits, and training programs for new hires, contractors, and IT organizations.

Our third year starts our compliance efforts and a renewed focus on policy development. We have many organizations asking for policies in specific areas to make it easier for them to do their job. That is an absolute turn around from where we were two years ago. We are looking at tools to help us measure and enforce compliance and developing a mandatory training program for our IT Administrators to enable compliance. We are still making incremental steps towards bi-annual mandatory end user training about security issues and policies.

We have seen many benefits from our Security Awareness Program. I found a list in an article by Charl Van De Walt on the Security Focus website that states them quite clearly. “They [the policies]:

- Form a benchmark for progress measurement
- Help ensure consistency
- Serve as a guide to information security

- Define acceptable use
- Give Security Staff the backing of management "[7]

We have gained all of these benefits and more. We use our policies and procedures to determine what security tools are procured and as the guide to audit our IT systems. By having the "rules of the road" documented on our internal public internet, every employee and contractor can read them and follow them. There are fewer questions about what you can and cannot do on our corporate network because it is documented in great detail in our Acceptable Use Policy and supporting procedures. The review process has given these documents and the IT Security Team credibility when helping the business groups and applications developers understand how to secure their environments based on the policies. We have addressed the original call to action by developing and implementing a Security Awareness Program.

Summary

In conclusion, there are a couple of key points to developing a successful Security Awareness Program. First, and most important, is executive support. This support helped clear a lot of roadblocks. Second, you need to define a framework; any one of them will work, and stick with it. Third, you need to get the full involvement from the organizations that have to help implement the policies. By letting the organizations collaborate on the writing and setting of the rules, it makes it easier for them to spread awareness about the policies and help enforce them.

References

[1] Desman, Mark B. "Building an Information Security Awareness Program". Pages xiv-xvi. Copyright 2002

[2] Author Unknown. CISSP CBK Domains
https://www.isc2.org/cgi-bin/content.cgi?category=97

[3] Ronald L. Krutz and Russell Dean Vines. "The CISSP Prep Guide, Gold Edition" Copyright 2003

[4] ISO 17799:2000(e). A copy can be purchased at
http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3=

[5]The American Heritage® Dictionary of the English Language: Fourth Edition. 2000.
http://www.bartleby.com/61/20/P0412000.html

[6] Author Unknown. "A framework for e-mail and Internet usage policies for your enterprise"
http://techrepublic.com.com/5138-6305-729500.html?tag=search

[7] Van De Walt, Charl. "Introduction to Security Policies, Part One: An Overview of Policies" August 27, 2001
http://www.securityfocus.com/infocus/1193

Appendix A: Framework Category Definitions

- Asset Identification and Classification
  - Standards to define, identify, classify, and label information assets and resources
- Asset Management
  - Standards for managing networks, systems, and applications that store, process or transmit information assets throughout the entire life cycle
- Asset Protection
  - Standards set for configuring and using specific systems. It is a "superset" of more narrowly focused policies such as Unix Server Policy.
- Acceptable Use
  - Defines objectives for ensuring the appropriate business use of information assets
- Vulnerability Assessment and Management
  - Defines our vulnerability assessment activities, like penetration tests and contractor account analysis, and ongoing vulnerability management efforts
- Threat Assessment and Monitoring
  - Defines our threat assessment activities, like intrusion detection and virus protections, and our ongoing threat monitoring efforts
- Business Continuity and DRP
  - Defines our activities to counteract business interruptions caused by major failures or disasters and to recover from any interruption with the least business impact
- Physical Security
  - Defines the precautions required to physically protect our IT infrastructure
- Security Awareness
  - Defines the activities to increase security awareness corporate wide, from the new employee to the long-tenured employee to anyone with physical or logical access

Appendix B: Sample Article

Do you know what is, and is not, acceptable to do on Company systems?

To help you make those decisions, our Company has created an Acceptable Use Policy. This policy defines those behaviors and activities that are and are not appropriate when any employee or contractor uses company resources. All computer resources are covered by this policy; desktops, laptops, telephones, networks, cell phones, PDA's, servers, printers, software, etc. that make up the computing infrastructure. The policy applies anywhere you use or access a Company asset.

You must use Company computer resources for company business in accordance with our company's Values and local laws. You may use Company computer resources for incidental personal use as long as:

- ✓ It doesn't consume more than a trivial amount of resources
- ✓ It doesn't interfere with staff productivity
- ✓ It doesn't pre-empt business activity

You should not expect privacy on Company computer resources. All of the resources are monitored for security, quality and availability.

Our Company values diversity and expects the highest levels of performance and integrity from each of us. Based on our values and local laws, you must **not** use Company computer resources to:

- Create, receive, or send:
  - ✓ Derogatory racial comments
  - ✓ Sexual content (pornography/nudity)
  - ✓ Offensive language
  - ✓ Political statements
  - ✓ Anything that negatively reflects on the Company
- Conduct private business for personal gain
- Circumvent security measures to gain access to resources (NO hacking or scanning)
- Make unauthorized copies of copyrighted material (this includes music files)
- Make fraudulent statements
- Provide information about Company employees to 3rd parties
- Use e-mail for spamming
- Use internet streaming media for personal use (this includes web radio)
- Use multi-player games for personal use

You should avoid creating either the appearance or the reality of inappropriate use of our Company's resources. Breaking any of these "rules" can lead to

disciplinary actions, including termination. Be smart and do the right thing.

You can read more about this policy and others that define the “rules of the road” for computer use at our Company, by visiting the IT Security Team web site. If you are a victim or a witness of inappropriate use, please notify the IT Security Team immediately. If you have any other questions, please contact us. Thank you for your cooperation.

NOTE: I have replaced our company name with Company and removed all hyperlinks.