Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Developing Security Policies: Charting an Obstacle Course

Developing a security policy for an organization may seem like a daunting task. Developing such policies in an academic institution can add unique challenges. This paper discusses the issues faced by those at my educational institution in trying to develop security policies. Some highlights include battling the myth of security, deciphering the meaning of security, receiving mixed signals about the importance of security, trying to keep it simple, trying to get it done quickly and trying to prevent it from failing. Eve...

Copyright SANS Institute
Author Retains Full Rights

AD

Developing Security Policies: Charting an Obstacle Course

Rosemary Sumajit
GSEC Version 1.3
April 4, 2002

Abstract

Developing a security policy for an organization may seem like a daunting task. Developing such policies in an academic institution can add unique challenges. This paper discusses the issues faced by those at my educational institution in trying to develop security policies. Some highlights include battling the myth of security, deciphering the meaning of security, receiving mixed signals about the importance of security, trying to keep it simple, trying to get it done quickly and trying to prevent it from failing. Every process will have its obstacles. Developing security policies can be very difficult but one has to keep trying. Knowing and understanding the challenges others have faced can be used as leverage when developing security policies in any organization. Eventually, something good and useful will come out of the process.

Security is a Myth

There is a great big myth about security. People believe that it exists. According to the Merriam-Webster Collegiate Dictionary, security literally means 'freedom from danger'. But danger exists everywhere, so this is simply not possible. Even though we may use the word security, we are really talking about taking measures that will reduce the likelihood of danger or mitigate the effects of a breach. We are actually talking about managing risk [1]. But the common term for managing risk is called insurance. People don't like to think about information security in terms of insurance because the very nature of insurance insinuates failure: a failure to adequately provide security.

I have been involved in meetings that should have been about policy development, plan implementation or other tangible items that can contribute to important milestones in the security framework for our organization. However, these meetings have often dwelled on what security means to different people. Participants could never seem to agree on the meaning of security and just how much of it we could create. On the one hand, someone would comment that no organization could ever be 100% secure. We should all accept that and just do our best. Another person would counter that while we cannot be 100% secure, we can do many things to improve our security. While both parties are correct, the conversation would go on and on as if one school of thought had to be victorious. The point is that people had great difficulty moving forward in tackling a problem if they could not agree on the exact nature of the problem first. Some might think that the importance of security should be obvious. After all, is it not apparent that protection is needed? Nevertheless, getting started is always the biggest hurdle.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Other Agendas

In my institution, I perform dual roles as a systems administrator as well as a college professor for information technology courses. It is sometimes advantageous to put on one hat in order to make strides for my job while wearing the other hat. For example, I was more likely to secure funding to attend a security conference in order to bring back ideas to develop a new course on the subject than if I simply wanted to learn how to improve security on our campus.

I work in a public educational institution where funding is limited and closely scrutinized. Keeping our doors open is not an easy thing to do. Less people are getting degrees and more people are looking to get certified instead. The competition for customers is fierce. We have to teach classes that other schools have not thought of yet. Once they do, we have to do a significantly better job at teaching. We have to give them something the competitors cannot give. My initiation into security did not occur as a response to an incident. It did not occur because we are learning from others' mistakes and trying to prevent them. It occurred because other people will need help in learning about security and it was decided that our institution should be one to educate them. In other words, I was sent to training so that I could quickly become an expert, create curriculum and offer customized training to our customers. But from my perspective, I was hoping to somehow establish the security of IT as a real and important business function in our organization.

Let's See Some Results

During training, it became frighteningly clear that I would not be able fulfill my duties in developing a new course so quickly. It would be more important to improve security in our organization. Perhaps through this experience, I would later be able to apply this in developing a new course. I came back from training energized. I was ready to take on the world, or at least addressing improving security at our organization. But I was quickly reminded that I was sent to training so that I could produce something of substance that could be used to improve our budgets. I had to be honest. I did not feel comfortable teaching and preaching about improving security before our organization had put into place some necessary measures.

I serve as co-director of the IT department on campus. Prior to attending the security conference, we had made a pitch to management that we had to do something about improving security. We did not even have a security policy in place. So that was our start. We were assured of management support and I was to make another presentation to the rest of the organization. After thoroughly depressing everyone with the would-be scenarios if we did not actively address security, we seemingly had the backing of everyone on campus.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

So my first task was to develop a security policy for our organization. As suggested in the security conference, representatives from various departments should develop the policy. We have a technology advisory committee whose charter is to advise the coordinators of the IT department on technology issues concerning the campus. It was to also encourage college-wide participation and discussion on these matters. During one meeting where we discussed the subject of security, I was hoping we would develop the policies together but was disappointed to find the ball back in my court. In practice, developing the policy became my responsibility. I was the one asking for everyone's cooperation and so it was assumed that I should be the one to manage it. Everyone was willing to provide input. But not too many were willing to develop it from scratch.

Being in the IT department, I thought we would start with our own needs. The staff had been clamoring for a very long time how they needed certain policies in place in order to back them up in their day-to-day duties. So I assigned someone to interview each staff member to gather input on the types of things they would like to see in our long awaited security policy. I was looking for some details that would supply the meat of the policy but was instead greeted with a lot of background information. There were lots of definitions and explanations about how technology worked. There was very little in the way of true policy statements and actions. Although this information is important and necessary, I felt it skirted the issue of policy development.

Disappointed, I set out to rectify the situation. I was going to supply the apparently difficult-to-articulate policy statements. I was partially successful. I found many resources for sample policy statements on the Internet. It was my hope to create short, simple, no-nonsense policy statements that everyone would agree on. I started to create a single document listing all that was needed. It soon became clear that the document would be too long and varied in both content and consideration of the target audience. It was necessary to split up the document into several specific policies.

I put out the documents for comment within our department and received less of a response than I expected. There were many, "It looks good to me." There were small comments about grammar and wording. I then brought the draft documents to our technology advisory committee. Sadly, the meeting that was set up to address the draft policies was poorly attended. The plan was to have the committee feel comfortable enough with the policies that they could help sell it to everyone else or at least gather input to make it sellable.

While most of the comments were agreeable, there were far too many suggestions that would not be backed up with true commitment. For example, it was suggested that specific guidelines be drawn up to aid end users in maintaining virus protection. Other guidelines corresponding to the remaining policies were requested as well. But it was expected that the IT department should develop all of these guidelines instead of the committee members. I suddenly realized that I did not have the full backing that I

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

thought to have previously secured. The poor attendance demonstrated at the meeting was just one of the signs.

Mixed Signals in Staffing

All throughout training, I could feel the importance of improving security and felt so sure that everyone would not hesitate to agree. I was right. Everyone back at campus did agree that it was important. But it stopped there. There appeared to be very little commitment to back up that claim. For example, it is popular belief that no security program can be successful without management support. Some view security beyond Information Technology; it is a business issue that merits an executive-level voice. But how many educational institutions have the equivalent of a Chief Security Officer (CSO)? CSOs are not commonplace even in industry [6]. Schools generally have Vice-Presidents of Academic Affairs or Deans of Student Services. Information Technology is typically not represented at the top levels of management. So how can the subject of security gain much more exposure? Oftentimes, the Chief Information Officer (CIO) will absorb any duties concerning security. The lack of executive voice for security issues can perhaps be attributed to the lack of acknowledgement of the importance of security.

At another level, I encountered further mixed signals with regard to technical staffing. While most organizations have different staff members conducting network engineering and systems administration, at our organization, the same people handle these varied duties. So whose job is it to handle security? Of course, the same ones who already handle everything else that has anything to do with information technology. During training, I was often struck by comments such as "Contact your mail server administrator," or "contact your web server administrator" or "contact your systems administrator." In our office, the same person handles these duties. Of course, educational institutions are often burdened with tight budgets and sacrifice some functionality based on limited resources. The security process dictates that an incident response team should be formed to address incidents as they occur. With our limited resources, the same people cannot reasonably absorb these duties.

Security is Everyone's Responsibility

Again, nobody had trouble deeming security to be important. Nonetheless, it seemed to be something that was relegated to the IT department. It became the IT department's responsibility to ensure the safety of our network and computers residing in it. It is suggested that standards developed through open processes tend to provide broadly accepted real world solutions [9]. Therefore, security should be everyone's responsibility. That is, no matter what policies or technological instruments are in place, security cannot be successful without the full cooperation of the people it seeks to protect. In drafting some of the policies I was surprised at how many of the policies I am currently violating. Some of my passwords are not strong enough. I do not change them often enough. I store them unencrypted. I see others write them on post-it notes and

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

leave them in their desk. We, the IT department, should know better and we ourselves are already breaking the rules we seek to enable. How do we expect others to follow suit when we are having trouble doing it ourselves?

We plan to enact a policy specifically governing activities of outlying departments that will be administrating new services. Obviously, they will look to our department for guidance and help. However, we are in the learning stages ourselves and can only offer limited help. Our solution is to punt the ball back to the proposed administrator to use whatever resources necessary to find some solutions. We are finding that even amongst our own systems administrators, we lag far behind in security issues. There is always the tendency to look for a quick solution. For example, maybe we could find a tool that will secure a Win2K box or a Solaris box. If it were that simple, security would not be the big issue and business that it is today. But there are many more nuances to consider. Perhaps tools exist to turn off likely unneeded services. But no such tool can exist that will tailor its security to your needs. The needs of every organization or department will be different. It depends on the proposed functionality of the program or service. Securing a machine that will provide web services is different from securing one that will act as a mail server, etc. There is no silver bullet. This means that security will often grow into a complex solution.

Systems administrators usually have their responsibilities spelled out. All need to do their part as well. These responsibilities are generally explained in an Acceptable Use Policy (AUP). In fact, our University system already has such a policy. But the cold truth is that the vast majority of our staff and students do not really know what is spelled out in the AUP due to its length and complexity. We would be better off creating our own policy and providing a training program targeted to our audiences. Hopefully in time, integrating security will become second nature to all concerned: ranging from the end users to IT professionals to top-level management.

Please Ensure Our Privacy

One of the biggest comments received about the draft policies is that the IT department should do everything it can to ensure privacy. That sounds reasonable. After all, confidentiality is one of the tenets of basic security? But these people were not referring to administrative data such as human resource records or student records. They were concerned about people reading their email. They wanted something in the policy to specifically guard against this.

There was the misconception that security equates privacy. As far back as 1996, many educational institutions noted in their policy documents that the privacy of email or other employee-created documents could not be reasonably expected [10]. Privacy is always suggested but never guaranteed. Some institutions will go so far as to say that business email is the property of the company and therefore it is the right of the company to read employees' email when requested. Most organizations will turn over email or other files

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

to authorities if requested for a formal investigation. Some organizations develop issue-specific policies concerning auditing procedures that state that email can be read in the course of periodic audits or network monitoring. That is, while every effort will be made to not specifically read a person's email, the message may have to be inspected to determine the cause of mail delivery errors, prevent virus spread or other related security activities. So the very policies that our users had hoped to use to protect their privacy will ultimately be the same ones that violate such privacy.

As much as we hate to admit it, added security will inevitably impose upon our privacy. Shortly after 9/11, I had to travel a lot and was amazed at how much airport security changed from month to month. At first, I did not mind too much. But as time wore on and more measures were added, I found myself annoyed at the invasion of privacy I experienced. At each checkpoint, I was questioned on my itinerary, my purpose for travel, the people I would be interacting with and my local accommodations. Aside from being annoyed at having to repeat myself, I resented the invasion of privacy. Did I not live in a free country that allowed me to do as I pleased so long as I did not infringe on other's rights to do the same? Why should my activities or whereabouts be scrutinized in such a manner? The event troubled me so much that I could not help bringing it up in everyday conversation with many different groups of people. After some discussion, I finally came to the conclusion that my inconvenience and invasion of privacy was worth the added security. But I had to be convinced on more than one occasion and only after a lengthy analysis. Hence, our users will probably need the same recurring discussions and reminders of why improving security (and the resulting invasion of privacy) is important to all organizations.

Security Goes against Traditional Business Values

You will rarely find a person that does not agree that security is needed in every organization. But people follow this claim blindly. They often do not realize that security actually hinders the speed of progress. Most businesses seek to put out a product or service as quickly as possible using as few resources as possible. Improving security works in opposition of this goal. Applying security measures slows down any project. It requires more human resources, physical resources and therefore costs more money up front. Security executives can attest to the difficulty in trying to balance security needs with fast-paced profitable ventures [6]. The job requires a backbone in situations that can grow ugly very quickly. I did not expect it but I was sitting on the unenviable side of the table during these tough discussions. I was pressured to put into production a service that was not properly secured. I explained the reasons that it was not yet appropriate and hoped that my reasoning was self-evident and sufficient. Instead, I was met with increasing opposition in the form of raised voices, anti-business overtones and frankly I felt ganged up on. I stated that we needed to remind ourselves of the whole process we developed in the first place. I had to remember that this was not a battle of wills; it was a test of the process. In separating the issues, we were better able to find a mutually agreeable solution.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

What Does Improved Security Really Buy for Us?

If successful, then security measures can save a significant amount of money for any organization in the long run. Again, we return to the insurance model of security. But we have learned the hard way that building in security hinders progress and costs more money. How do we reconcile the numbers? We should quantify it in dollars so that we can graph exactly how security stacks up to our other business concerns. Surveys of large companies have shown that many organizations cannot effectively determine their return on investment (ROI) when it comes to security spending [7]. They often factor in the price of replacement equipment. But how does one accurately account for the loss of productivity should an incident occur? Other losses include the loss of future business due to a tarnished reputation. A possible explanation for the inability to systematically estimate costs could be that managing security is often left with the IT department. The IT department has a good handle on how to develop technical solutions and contribute alternatives. They do not typically have the broad overview of the business to make an accurate assessment. This brings us back to requiring executive level representation.

Risk Assessment

I learned at the security conference that you cannot implement security solutions unless you have the policies to back them up. At the very least, a company should have a security policy in place. But how does one know what to secure if they do not know the risks involved? Such a risk assessment is also important in that it helps an organization develop policies that are in alignment with their business function. One analysis of the security process actually places policies in the final phase [3]. This author suggests that asset definition, threat assessment, vulnerability analysis, and selection of countermeasures all come before the ultimate phase of implementation. Interestingly, policies and procedures fall under implementation. We seem to be looking at the chicken and egg problem. Which comes first? Implementing security is already considered slow. Businesses would like the process to speed up as much as possible. Unfortunately, risk assessment often gets sacrificed. As many as a third of companies polled by PricewaterhouseCoopers were found not to have conducted any risk analysis at all [8].

In my organization, we worked around this by performing various projects in parallel. One group worked on developing security policies. Although they were in draft format, we tried to abide by them as much as possible. Simultaneously, the IT department worked on identifying assets and examining risks. The same IT group then worked on developing a framework for building security into new projects. We took steps to minimally secure existing assets but poured our energies into ensuring that new ones would be properly secured. To prevent further complexity and confounding of the problem, we placed a moratorium on adding new services that did not follow the suggested framework.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Simple Policies?

During training, we were told to make sure that our policies are kept simple. If they are not, then no one will understand them and therefore not be able to follow them. Some may not even bother to read them. Ultimately, this would undermine the policies we seek to enable. My first inclination was to have a single, simple, no-nonsense security policy. After scouring the Internet for sample policies, I have yet to find such a policy. In fact, to reduce complexity, it is suggested that separate policies be developed based on issues or target audiences [11]. Oftentimes, those providing sample outlines of security policies will try to be as complete and comprehensive as possible [4]. Unfortunately, the all-inclusive nature of these types of policies contributes to the unmanageable length that turns off so many would-be policy abiders. Worse yet, the generic samples did not align to any single business function. It would have been helpful if there were sample policies based on different industries such as education, finance, health care, government, etc. I found some excellent examples of issue-specific policies and used these for the basis of the security policies for our organization. Although almost each policy was simple in itself, the list of policies grew long. It became so long, that it soon became clear that the multitude of policies became an inhibitor. How do we educate the masses when it seems there is too much out there for the common person to grasp in one sitting? Finally, just because there were lots of sample and real policies to choose from, there was no indication that any of these were successful in their mission. That is, having a policy did not necessarily mean success.

Why Security Policies Fail

During my research for sample policies, I happened upon a document that I perhaps should have avoided reading until making more headway in our organization's security efforts. This document discussed the reasons that security policies often fail. I'll briefly outline them here [2].

1. Security is a barrier to progress
   Even common sense security measures reduce productivity.
2. Security is a learned behavior
   If a user is unaware of the value of a particular policy, they will believe the policy is stupid and therefore, not follow it.
3. Expect the unexpected
   No one can anticipate every problem. Therefore, to maintain one's skills, one has to constantly prepare, plan and practice.
4. There is no perfect mousetrap
   Developing a security policy is not the final solution. Improving security is a continuous process.

I had discovered most of these truths empirically while developing security policies at my school. But to see it in written concisely in black and white in a single document

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

foreshadowed impending doom. First I am told how important security is to the success of any organization. Then I learn that there is no such thing as 100% security. But even as important as this is, I find that I am receiving mixed signals about this topic. Yes, I need to make it happen, but I cannot use any more resources than we already have. Then I find that it will take the cooperation of an entire organization to make it work. But how does one make this happen without executive backing? Make sure the campus is secure but try not to infringe on anyone's privacy. Make sure this new service is secure, but get it done quickly. How much do we earn because we are more secure? We do not earn anything monetarily but at least we do not lose as much as we would without the security measures. Develop simple policies and people will be able to follow them. But you will not know what to include unless you perform a risk assessment first. By the way, make sure all bases are covered. Finally, this had better work, or all that insurance we built will be for naught. With all of these pressures coming at security professionals, it is no wonder that incidents are occurring at an alarming rate.

Conclusion

While the tone of this paper may seem fatalistic, it is really meant to be one of encouragement. When you have so many strikes against you, there is no direction left to go but up. By even recognizing that improving security is an important issue, half the battle is over. Sure, there will be many obstacles along the way. Remember that the business of Information Technology is very immature. Governments have been around since the dawn of society. Militaries have been around since communities discovered they needed to defend themselves from neighboring communities. Frankly, security has been around a long time. But Information Technology has not. So securing information technology is a very new business indeed.

At a young age of less than 50 years, the business of IT is learning what it takes to mature [5]. It has encountered a lot of problems and had to deal with them head on. Part of this maturity is the awareness of the problems and learning to take security into consideration. IT is finally becoming of age. Without an awareness of the problems, one cannot even attempt any solutions. We must remember that we cannot surrender to these problems lest we wish to have anarchy. We must accept the problems of security that are presented to us. Even though it seems that each problems will force us to take a step back, a step in any direction allows the industry to grow and improve.

You will see it over and over again. In order to make security a success in your organization, you need tools that have nothing to do with technology at all:

- Executive-level backing
- Cooperation and input of everyone in the organization
- Organizational-wide discussions and training

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Developing a suitable security policy has its challenges, but is not impossible. Navigating the security obstacle course does not have to be painful. It would be helpful if you could at least see the obstacles. Hopefully, I have been able to draw them clearly enough to prevent others from stumbling as my colleagues and I have.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References

[1] Cavanagh, James P. "Network Security, The Business Value Proposition." January 2002. <http://www.consultant-registry.com/delivery/SWP2.pdf>.

[2] Control Data Systems, Inc. "White Paper, Why Security Policies Fail." Copyright 1999. <http://downloads.securityfocus.com/library/Why_Security_Policies_Fail.pdf>.

[3] DePasquale, Sal. "Security Process" Not dated. <http://consult-registry.com/archives/SalDePasquale/securityprocess.htm>

[4] Farnsworth, William. "What do I Put in a Security Policy?" August 10, 2000. <http://secinf.net/info/policy/policy.htm>.

[5] Feldman, Jonathan. "Everything You Always Wanted to Know About the Business of IT (but were afraid to ask)." March 4, 2002. <http://www.networkcomputing.com/1305/1305f1.html>.

[6] Hayes, Mary. "Impact Player." February 25, 2002. <http://www.informationweek.com/story/IWK20020222S0002>.

[7] Hulme, George V. "Management Takes Notice." September 3, 2001. <http://www.informationweek.com/story/IWK20010831S0014>.

[8] Hulme, George V. "Security Policies: How Much Is Enough?" September 3, 2001. <http://www.informationweek.com/story/IWK20010830S0022>.

[9] Molta, Dave. "Too Many Cooks in the IT Kitchen?" March 4, 2002. <http://www.nwc.com/1305/1305f7.html>.

[10] Oribello, Anne. "A Survey of Selected Computer Policies from Institutions of Higher Education." Copyright 1996. <http://www.brown.edu/Research/Unix_Admin/cuisp/>.

[11] Robiette, Alan. Joint Information Systems Committee. "Developing an Information Security Policy." February 19, 2001. <http://www.jisc.ac.uk/pub01/security_policy.html>.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**