Global Information Assurance Certification Paper

Implementing Changes to Security Policies Without a User Revolution

Thomas Grzelak
GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4

Option 2

Implementing Changes to Security Policies Without a User Revolution

Abstract

The operational environment of computing continues to evolve on numerous fronts. The dynamic of the user community and its importance to the security posture of an organization is becoming increasingly important. Information Technology (IT) professionals must carefully plan how to promote security awareness and implement security policy. Common strategies are presented to assist IT professionals in promoting user security awareness and education, in gaining sensitivity to user needs/fears, in maintaining open communications to/from the user community and in understanding how change (e.g., security policy improvements) affects users in the workplace.

A case study is presented to demonstrate how these strategies are implemented in the workplace relative to a significant security policy change that had a direct impact upon the user community. The case study outlines the actions undertaken to recognize and resolve potential user conflicts. The results proved to be a relatively seamless user-oriented security policy change – the cessation of telnet access on departmental servers in lieu of the activation of encrypted Secure Shell (SSH) connections.

Introduction

Information Technology (IT) professionals are finding themselves in an increasingly difficult position of maintaining the security posture of their organizations. As the realm of security threats broadens, the demand for technical expertise and proactive policy-making is significant. But in today's workplace it is not enough to master only the technical nature of each security issue. Another security dynamic is evolving that requires careful consideration – the user community. IT professionals must not only be able to turn their technical decisions into a comprehensive security policy, but they must effectively communicate that policy to their user communities. "A new breed of technologists needs to emerge. Strong technical skills combined with business knowledge, communication ability, and a client-centric idealism would be perfect" (Ivy Sea, Inc., 2002a.)

The best administrators are ones that can effectively evaluate situations and propose policies that not only alleviate the primary technical problem but also adequately address the ramifications of their solutions. IT professionals must be effective and articulate in promulgating security policy to their users. Perhaps the greatest challenge in such an effort is that the typical user community is not a homogeneous entity with regards to computing knowledge. In fact, the range in expertise among the user community is broadening rapidly –

ranging from personnel with little technical knowledge to users who may possess significant technical knowledge. Quite simply, new personnel entering the work force today may have never known life without a personal computer in their homes. Communicating to a user community with such a broad range of expertise is a facet of the problem that can require as much careful planning as the technical problem and policy itself. In order to effectively implement change in this environment, specific planning on both the technical and human aspects of a security policy change is absolutely required.

The purpose of this paper is to discuss strategies that can be used by IT professionals to help communicate policy/change to their user communities. Relative to these strategies, I will present a case study describing use of these tactics in implementing a security policy change that had a direct impact on much of my user community. I will forgo some of the technical planning issues and instead concentrate on the human communicative planning issues involved in implementing this policy. Change often elicits a significant human reaction. The careful planning of IT professionals when introducing change can help ease the transition of implementing security policy, thus stemming off what could be termed a "user revolt." It is imperative to understand that "different people perceive and use technology in different ways" (Ivy Sea, Inc., 2002b) which further emphasizes the need for IT professionals to be articulate communicators in tune with their user communities.

Taking a pulse before an attack

There are several measures that can be made prior to a security incident that can improve upon an IT professional's ability to successfully implement a change to a security and have it embraced by the user community. First and foremost, an educated user community is extremely helpful in getting complicated policies not only accepted, but quite possibly, understood. Many security analysts include the training of user communities in security awareness as a leading way to improve a company's security posture (IBM-RC, 2000; Middleton, 2002; SBIC, 2001.) This training can range from organized seminars for large user communities down to individualized training in smaller communities. IT professionals need to demonstrate to users how important they are to the security structure of the organization. Users need to be reminded that they are on the front line in the battle to keep the business secure (Ivy Sea, Inc., 2002c.) Awareness training should clearly emphasize why it is in their best interest to adopt good security practices. Ultimately, the key here is for IT professionals to communicate the importance of security to their users as part of daily life rather than only as part of a crisis.

It is important to work constantly to gain the respect of user communities and to have them view the company's IT organization as profoundly dedicated to their security. IT professionals need to be consistent and seize every opportunity

to educate their users, especially in methods that promote good security practices. When users consider IT as a resource, the result is an increased likelihood to have difficult policy decisions accepted. To this end, IT professionals must ensure that they are accessible to the user community. This serves two purposes: first, it permits users to rely upon IT as a resource; secondly, it also gives IT an opportunity to assess the knowledge and practices of the user community. The latter can be instrumental in predicting user community reaction to security policy changes. As stated previously, user communities are broader in terms of knowledge and experience than ever before. Users' comprehension and implementation of technology vary greatly and are key to IT appreciating the importance of knowing their user community (Ivy Sea, Inc., 2002b.)

Understanding the capabilities and needs of the user community is critical to being able to assess their ability to accept and implement change. Successful IT personnel know, educate and respect their user communities. The claim "users don't care about security" is either a gross generalization or a direct reflection of a failure on the part of an IT organization to adequately assess and cultivate their user community. Such attitudes require educating the user community to the costs of relaxing security or maintaining the status quo. Identifying the costs of security lapses is often a primary argument in support of any plan designed to improve security (Mohling, 2000; Ivy Sea, Inc., 2002c.) With a well-designed, concerted effort, IT professionals will promote the development of a user community that computes more responsibly and in turn, improves their ability to conduct future security policy changes.

An attack/vulnerability occurs; things to consider

A hack occurs, an exploit arises or simply, the time to fix a security weakness arrives. Any of these events can manifest themselves as a need to implement a security policy change. First, IT professionals must understand the situation and the costs involved in not responding to it. They must determine a technically-sound solution that can be implemented and ensure it will achieve the technical goals of the security policy change.

In today's work environment, the IT professional must consider the impact this change will have upon his/her user community. It is important for IT to understand the results they want to achieve in the user community by implementing this change (Ivy Sea, Inc., 2002d.) Additionally, the IT professional must assess his/her user community's reaction to the changes. As done before on the technology side, they must determine the costs to users and their (users') security if this is change is not implemented. IT must anticipate defending the need to make these changes whether it is to management or to the user community. Being able to explain all costs/risk involved (technological and human) by not implementing the change adds significant credibility to the

necessity of the IT professional's proposed policy change. Effort should be made to refine the solution. Can the solution be made seamless/invisible to the user? Users are more likely to accept the change if the solution is made so (Mohling, 2000.) Does the plan have a precedent elsewhere?

IT professionals should "bullet-proof" their case and be articulate in communicating it. They should present their plan to management and discuss all facets of its impact – technically, business-wise and user community-wise. The presentation must clearly identify the threat, the risks/costs involved and why it is important that these measures be taken. It is critical to get the full support of management in making security policy changes (Middleton, 2002).

Prepare for the change; accept responsibility

No matter how minor, it is simple human nature to find change as uncomfortable (Ivy Sea, Inc., 2002d.) Effort should be made to plan how this change will be communicated to your user community. Multiple mediums should be employed to communicate the policy change such as email, web, verbal, etc. Redundant communication methods can help ensure widespread and effective communication of the message (Ivy Sea, Inc., 2002d; Saunders, 1999).

In formulating the specific communications, it is best to be direct. The background of this policy and why it is important to make these changes should be fully explained (Star, 2000.) This is an opportunity to educate and IT professionals should make full use of it. The communication of change must be clear, succinct and complete (Ivy Sea, Inc., 2002d.) IT professionals should avoid "acronym soup" and clearly describe the important aspects of the policy change. Users should be encouraged to contact the IT organization directly with questions or feedback. Experts widely tout two-way communication to be a cornerstone of introducing change in the workplace (Edgelow, 1999; Saunders, 1999; Ivy Sea, Inc., 2002d; Stark, 2000.) It is an opportunity for IT professionals to show users their questions/feedback are an important part of the process.

As an important final point, IT professionals need to realize that changes to IT policy also involve a question of ownership (Ivy Sea, Inc. 2002b.) A user, affected by the policy change, will have his/her own "virtual" workspace altered or possibly, in their mind, violated. The IT professional must not only acknowledge this, but must accept it and consider this reaction when plans are drawn up and announced. IT professionals who show sensitivity to this can gain additional respect and credibility amongst their users.

Make the change and analyze how it went.

It is very important to make a schedule for a change and stick to it. An IT professional must be predictable and deliberate in his/her actions; a good planner always is. The IT professional should attempt to avoid a piecemeal implementation plan whenever possible in order to avoid adding further confusion to the change. If possible, they should also have a disaster plan for reinstating "life" as it existed before the change just in case something goes terribly wrong.

The IT organization should always take time to review how well the change went looking at various indicators of success (technological, communicative, user feedback, etc.) It is an opportunity to learn from, especially in terms of interacting with the user-community. IT should continue to give users further opportunities to provide feedback. Their problems and concerns are a significant indicator of the community as a whole. If they are indifferent, IT professional should be able to gauge this too. The user community is an important dynamic in the IT security and operational organization. It must be addressed and respected.

Case study: Workplace Transition from Telnet to Secure Shell (SSH)

The following case study will serve as an illustration of the considerations and planning strategies outlined above. The description will focus not as much on the technical aspects of the security policy change, as on the effect the change would have on users and normal business operation. It will describe of the planning that took place in advance/during and after a recent policy change regarding access to our departmental Unix and Linux workstations and servers. Specifically, the issue was the cessation of support for inbound telnet access in lieu of the mandatory use of Secure Shell (SSH).

The background operational environment

My workplace is a typical major university academic department and research facility. I have over 300 computer workstations and servers using nearly every major operating system. Our hardware breakdown is approximately:

- 70% Windows (DOS → XP),
- 18% Linux,
- 10% Solaris/IRIX
- and 2% Mac.

I have a staff of one full-time systems administrator and two part-time student technicians. My user community covers the entire spectrum of expertise – from novice users who simply want things to work to astute technical users who want to how, why and everything in between.

My IT organization fully accepts responsibility for everything that goes wrong (or right) with our computing environment. I have always had a dislike for the "blame game" and felt it was easier to let my users know that it was OK to blame me for all of their problems. My IT staff has a strong sense of responsibility for our user community and makes addressing their concerns a top priority. I maintain several avenues for gaining access to my IT organization: helpdesk phone/email, visible presence in the department, open door office policy (no key card required to see me!), etc. Often I joke that it takes me two hours to walk down the hallway back to my office because users are asking questions and seeking assistance. In reality, I consider this a good sign. My users are demonstrating to me that they consider me (and my IT organization) a valuable and approachable resource. In turn, I am able to assess what is important to them, what level of knowledge they are at, how they use their systems, etc. These are critical facets of the user community to know when I have to make changes to our operating environment.

Planning issues prior to policy change

Our understanding that permitting telnet access was an unnecessary risk had evolved over the past year. Our Unix/Linux systems permitted regular inbound telnet connections. Since these connections are made in clear text, telnet connections into our machines were susceptible to having their traffic read by any packet-sniffing program that was monitoring traffic anywhere along the path between the telnet client and the host Unix/Linux machine. We had made great strides in improving our security posture through employing a regular system patching schedule, improved system monitoring procedures and access control mechanisms (e.g., TCP wrappers.) However, the use of unencrypted services was a risk that we understood needed to be minimized.

The transition to using SSH actually began several months prior to our complete SSH transition. University researchers typically conduct studies at numerous off-site locations (including other universities and research facilities) besides their own machines. Some of our users requested that we support SSH clients on our Unix and Linux machines in order to facilitate them being able to access off-site SSH-only facilities. We tested and installed the clients on a few machines, and then as a matter of our normal practice, rolled out the clients to all Unix/Linux in our organization.

We understood the background why SSH was developed. We realized it appeared to be good idea. However, we needed to assess a number of aspects to this issue if we were anticipating applying it as local policy:

- how prevalent was this transition at other facilities, universities, etc?
- did other organizations merely support inbound SSH connections or did they completely eliminate unencrypted telnet?

- was there precedent at our own university?
- were the available clients mature enough for all platforms?
- did users find the clients on Unix and Linux machines to be as easy to use as telnet?
- what level of change was required to each Unix/Linux box to enable SSH connections (i.e., run the service daemon.)

Our investigation clearly established that there was a trend toward eliminating telnet access and support SSH-only connections. In fact, we found numerous other organizations moving away all unencrypted services – ftp, mail, web, etc. Even at the university's monthly Unix administrators' meetings, SSH and its widespread implementation as an encrypted alternative to telnet was being discussed. Clearly, we had established a precedent that we would be part of a growing trend to eliminate inbound telnet connections and instead only support inbound SSH connections.

The next step in the assessment process was to determine the technical aspects of implementing the SSH service and the shutting down of the telnet service. Since my purpose here is detail the user considerations/decisions relative to this case study, it suffices to say that from a technical standpoint the installation of the service was rather straight-forward: the service software was installed and the service/daemon was set-up to run out of inetd. In our initial planning, we decided that we would support password connections that used the server machine's public key to set up the encrypted channel. We did this in order to ease transition of the users to the new service. We first selected, installed and enabled the SSH daemons (services) on test Unix/Linux platforms. Upon completion of testing, we were convinced we could employ this as a service replacement on our Unix/Linux machines.

We next assessed how our users used telnet. Not only were we concerned about how to get the users to migrate away from telnet to an SSH client, but we knew that we needed to be able to successfully educate them in determining which client to use to connect to other machines (namely external machines that do not support SSH connections). Just as some offsite research facilities support SSH, others do not. Therefore we needed to continue support outbound telnet on all platforms. We devised a table as to what we would support and would not support.

Machine	Telnet Inbound	Telnet Outbound	SSH Inbound	SSH Outbound
Unix	No	Yes	Yes	Yes
Linux	No	Yes	Yes	Yes
Windows	N/A – No	Yes	N/A	Yes
Mac	N/A – No	Yes	N/A	Yes

We knew that before we could recommend a change in our security policy, we needed to have viable clients for "Yes" outbound platforms and viable SSH daemons for each "Yes" inbound platforms (previously established.) The Unix/Linux clients had already been tested through our previous support for outbound connections to offsite SSH-only systems. The critical issue to implementing this policy was to find viable Windows/Mac clients that users would find as easy to use their current telnet clients (i.e., contributed toward the goal of a seamless transition.) We were able to identify several free or free-to-academia SSH clients that closely resembled current telnet clients. This would eliminate the need to purchase individual licenses for each user.

Our next planning requirement was to determine as many user scenarios that had yet to be addressed. Since many faculty and staff connect into our servers from home, the issue of installing and using the SSH clients from home was not very problematic. However, faculty and staff often depart the university and go out of state, out of country, etc. and use machines that are not their own. Since we could not guarantee these external machines would have SSH clients installed, we devised two solutions:

- The vast majority of users who found themselves in this situation simply needed access to their email. Previously they telnetted in and read their mail our mail servers. In order to give this class of users access, we installed a Secure Socket Layer (SSL)-protected web mail server that interacted with the various departmental mail servers using an Internet Message Access Protocol (IMAP) over SSL connection.
- The other group of users who absolutely required access to the servers would use a freeware SSH client called Putty. The advantage of Putty is that it fits onto a single floppy disk that could be carried around by the user. Therefore, as long as the PC could support a floppy and a network connection, this was a viable solution.

We also considered the scenario of what we would do if a user attempted to make a telnet connection to our Unix/Linux machines. We decided to replace the telnetd system call in /etc/inetd with a call to /bin/cat which would display a denial message. The message stated to the inbound connection that we no longer supported telnet connections, to use an SSH-connection instead and to contact our help email address for assistance or questions.

Our analysis and planning had incorporated as many scenarios that we felt could complicate the successful implementation of the policy to permit only inbound SSH connections. Our IT organization is overseen by a departmental computer committee. This committee is responsible for advising the IT organization on major policy, planning and purchase issues. We summarized our plans to the committee having all major and minor known aspects addressed from an established precedent for the policy change at our own and other institutions to the ability to provide viable, intuitive user clients. Our intended plan received the committee's approval.

Implementing the policy change

As described previously, we brought up inbound SSH support on all Unix/Linux boxes as well as ensured the web mail server was fully operational (its announcement had preceded the SSH-transition.) We announced to the user community:

- we would no longer support inbound telnet connections to any of our machines.
- we would require the use of SSH clients to make connections.
- we explained why we were making this change and why this would help to improve our security.
- we explained how to obtain/install SSH software.
- we would still support outbound telnet connections from all machines.
- we gave users a grace period of one week to have the SSH client software installed and to begin using it.
- we directed any and all questions to our helpdesk email address or to come speak with us directly.
- we announced that SSH-connections were immediately supported so users could connect directly as soon as they installed the client software.

The policy change announcement was made simultaneously on several different media. We made this announcement through general email, directed email to specifically-affected users (e.g., Unix/Linux-based research groups), front page of departmental web site, Message of the Day banners and through face-to-face discussions. The majority of users who emailed for help/feedback requested assistance in downloading, installing and using the software. This was immediately provided. Other feedback/requests asked for further information on how this would affect other services (e.g., outbound telnet), how to connect from offsite locations, etc. Questions were answered and assistance was given so that when the transition was finally made a week later there was a little fanfare.

After the change – reaction and lessons learned.

The security policy change permitting only inbound SSH-connections and ending support for inbound telnet connections proceeded quite smoothly. We credit this transition to prior preparation on both the technical and user community sides. Selection of good intuitive clients, clear information flow to and from the user community, adequate testing of the daemons and clients all contributed to a fairly seamless transition.

We did experience a problem walking users through use of the Mac-SSH clients. Due to the extremely low number of Mac users we did not have an available platform to test the client prior to transitioning. However, within a day a suitable Mac client was found.

We learned that email and face-to-face discussions were the most effective in getting the word to users. The least effective methods seemed to be posting to the departmental web site. However, we attribute this latter result to the fact that posting news to the front page of the web site is a fairly new means of notifying users.

I am convinced that the professional rapport and mutual respect that our IT organization shares with the user community significantly contributed to this efficient policy implementation. Users realize that they are one of our top priorities. To that end we formulate our planning with their needs at the foremost in our minds. Our users are our primary defense in keeping our systems operational and secure. If we fail to educate and keep our users "security conscious," it is our own fault and we must employ user community-oriented strategies to resolve this.

Conclusion

The dynamic of user community has a more significant impact upon the IT decision-making process then ever before. IT professionals must be cognizant of this dynamic and include it as a primary consideration in their IT planning and implementation. The range of knowledge of the current user community adds a further complication to addressing the concerns of the user community. IT professionals must make the effort to consider how their implementation of technology and policy will affect their user communities. They must be advocates of the user communities and promote security awareness at every opportunity.

The security awareness and responsibility of a user community are a direct reflection upon the IT organization. IT professionals must seize every opportunity, formal or informal, to educate their users and promote solid security habits. Working with a user community allows IT professionals the ability to assess the level of knowledge, discipline and responsiveness the users have toward security policy and other aspects of computing. This assessment helps prioritize and guide IT professionals when policy planning is conducted.

When security policy change is required, careful user-oriented planning must be conducted. Communications with the user community must be purposeful and direct. The security change must be represented with the real costs of "doing nothing" identified. It must be well articulated, multimedia and succinct. A seamless, well-communicated solution increases the chance of its successful implementation. There should be an opportunity for users to provide feedback or ask questions about the policy change. IT professionals must be diligent in their efforts to be accessible and in-tune with their user communities.

A case study was provided in order to exemplify how proper working with the user community can contribute to a smooth transition of a potentially difficult security policy change. The case study showed that with proper user-oriented planning and an accessible IT organization, change can occur without a "user revolt" and instead build a user-community willing to embrace security improvements.

References

Edgelow, Chris. "7 Truths When Communicating Change." 1999. URL: http://www.sundance.ca/resources/articles/7_Truths_When_Communicating_Change.

IBM Research News (IBM-RN). "Securing Your e-business: 10 Tips for Protecting Online Companies." 15 February 2000. URL: http://www.research.ibm.com/resources/news/20000215_10_tips.shtml.

Ivy Sea, Inc. "Information Technologists and Business Managers Must Circle the Wagons." 2002a. URL: http://www.ivysea.com/pages/ca0198_4.html.

Ivy Sea, Inc. "Decreasing User Backlash to IT Changes." 2002b. URL: http://www.ivysea.com/pages/ca1197_2.html.

Ivy Sea, Inc. "Getting Employees to Actively Buy in to Information Security." 2002c. URL: http://www.ivysea.com/pages/ca0198_2.html.

Ivy Sea, Inc. "Ten Tips for Communicating Change." 2002d. URL: http://www.ivysea.com/pages/ct0600_2.html.

Middleton, Bruce. "Mapping a Network Security Strategy." 2002. URL: http://www.securitymanagement.com/library/000619.html.

Mohling, Torleif. "Overview of Class Thirteen – News, Security" 30 April 2000. URL: http://bigworm.colorado.edu/Saclass/class13.html.

Saunders, Rebecca. "Communicating Change: A Dozen Tips from the Experts." Harvard Management Communication Letter Vol. 2, No. 8, August 1999. URL: http://managementezine.com/mgchange.htm.

Small Business Info Centre (SBIC). "Cyber Security Checklist for Small Businesses." 2001 URL: http://www.smallbizinfocenter.com/checklistreview.asp?ID=48.

Stark, John. "Communicating Change." PDM and Change Management. 16 March 2000. URL: http://www.johnstark.com/mc6.html.