



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.

### Leveraging a Securing Awareness Program from a Security Policy

This paper addresses the benefits of leveraging both a Security Awareness program and a Security Policy.

Copyright SANS Institute  
Author Retains Full Rights

AD

An advertisement banner for Watchfire. On the left, there is a graphic of a globe and a login form with fields for "for" and "password". The text "YZEIF I" is visible in the background. In the center, a dark blue box contains the text "Testing Web applications for vulnerabilities?". On the right, the Watchfire logo (a red flame) and the word "watchfire" are displayed.

Testing Web applications for vulnerabilities?

# Leveraging a Securing Awareness Program from a Security Policy.

Howard Uhr

Version 1.2e

## Terms

IT Security Policy

Policies are the rules that organizations use to govern themselves.

<sup>1</sup>“A security policy establishes what must be done to protect information stored on computers. It compels the safe guarding of information and reduces personal liability for employees”

Security Awareness Program

<sup>2</sup>Activities and procedures that give the Security Policies credibility and visibility. That is, a program that uses activities such as news and anecdotal stories, situational examples and discussion to lend relevance and pertinence to the policies. A program that incorporates procedures to mandate company wide participation and compliance. Finally, a program whose goal it is to raise the security consciousness of each employee, making a security policy a tool for all.

## Problem Statement

We enjoy the best of all situations; we need to take a successful business and develop an Internet exposure. This is an exciting prospect for all, because we get to do it internally. Introspectively, this doesn't seem too daunting a task. After all, we already have a security policy, a Business Continuity Plan (for disaster recovery) and all the physical and environmental security you could ask for. Let's do it!

As the euphoria diminishes, reality begins to grab us by the throat and shake us. We have been administering an infrastructure that has only limited extranet access from the outside. We need to architect a system that meets our initial needs and an infrastructure that provides the physical and logical access constraints needed to keep our data safe. We know how to do that, we have done it before! A couple of times. And our enthusiasm sores once again! Only to be tempered by a security policy.

What do we really know about the <sup>3</sup>security policy that the parent company boasts? Does it address our divisional business needs; do I even know where to find it? Worse yet, Operations doesn't know much about it and the dispatchers on the floor haven't heard of it. How do we make the security policy a tool that the organization will adopt as a lifestyle change? Now what do we do?

## **Proposed Solution**

Brainstorm: Using the risk analysis that was completed for the infrastructure design and the corporate security policy, draft a standard that is focused on our business needs. Then *combine a security awareness program that leverages off that policy*. A win-win situation for the employees, management, those charged with security, and the company as a whole. Again, we are in business!

The first step is to draft a security policy. Sure our parent company has a policy, so we start from there. It is BIG. I mean thousands of pages. Who can keep up with this? We want something a little more concise.<sup>4,5</sup> What do we really need in our policy? Using the corporate policy as a template is a great place to start. Then we gut it. Remove every thing that doesn't directly relate to our business plan. We can live with this, as we will indicate that our policy is subordinate to the corporate or master policy. After completing our plan and having received management approval, we are ready for the second step.

The second step was to create a security awareness program. What do we know about a security awareness program? There are consultants and references available on the Internet that provides a pretty good starting point. Going with the do-it yourself theme we have established so far, we get on the Internet and start our research.

We have defined what a 'Security Awareness Program' is (see TERMS) and next we define some basic goals. The experts say, <sup>6</sup> "Strong security architectures are rendered less effective if there is no process in place to make certain that employees are aware of their rights and responsibilities. Implementing an effective security awareness program helps all employees understand why they need to take information security seriously, what they will gain from its implementation and how it will assist them in completing their assigned tasks. An effective security awareness program could be the most cost-effective initiative a company can take to protect its critical information assets."

To bring home the above concept, we want each phase in our program to emphasize or in some other way be tied to individual risks addressed by our policy. This allows us to modularized our presentations so as not to over-whelm and still increase our knowledge base of security issues.

### **Now sell it!**

We stated that combining the introduction and sign-off of the security policy with a security awareness program has the potential to become a win-win situation. Win for the employees through successful participation, win for management on two fronts: a successful security plan and a realizing short term return on investments on a long-term plan. The security organization wins because they are perceived as welcomed team members, not antagonist's keeping the business from its mission. Finally, the company wins because the defense of the company's confidential information and reputation becomes as much apart of the organization as its business mission statement.

### **The Employee Wins.**

One of the most difficult things to implement in a company is change. Change comes hardest at the employee level. There is always some new program or other being foisted on them to improve their production, their motivation, and their corporate life as a whole. A successful security awareness program is neither a frontal assault upon them, nor is it a manipulative device to garner change. Instead, an effort to raise awareness of security issues around them is introduced. Awareness of behaviors that invite loss of personal privacy through social engineering, awareness of not only what is policy and how to respond to deviations or violations of it, awareness of the role each employee plays in the defense of company information.

By simply raising their consciousness, the employee will look about them for real life examples to fit a profile or a risk they have just become aware of. In way of an example, introducing benefits and risks of a 'clean, locked desk', the employee has the chance to explore and grasp the personal opportunity, responsibility and liability of the concept before they sign off on the related policies. The opportunities range from a new cognizance to suggestions that may improve or simplify a given policy. These activities lend themselves toward discussions that reveal weakness in policy and eagerness for ownership. Pursuing this type of feedback as a procedural part of the awareness program is a small part of what makes this policy a living document.

It is also a win for employees because the policy has a sense of ownership through routine participation, interaction and review from employees. As employees are taught and or shown the potential risk and the corresponding policy, they have the opportunity to offer feedback, possibly sharpening the focus of the policy. If this process is repeated on an annual basis, the focus of the policies may be refined or redirected from direct employee involvement. The initial expense in identifying assets and information to secure, risk analysis, and the drafting of the policy are not lost, but constantly reviewed and evaluated.

### **This is a Win for Management.**

This is a win for management because of a new awareness becomes a culture change instead of a short-lived dying program. This can be accomplished by maximizing the reach of the program with a consistent message. The key is the consistency of the message. Security is everyone's job. Most of us have the same failings: we all forget passwords at one time or another, and we are all tempted to write them down. We are all tempted to take the short cut to get the job out the door. However, seeing and or knowing that policies are taught and enforced equally at all levels of the corporation suggest that all levels of the corporation need to comply. This helps middle management know the cost of security is less than the cost of no or un-enforced security. The uniform message and maximum coverage encourages middle management because they are aware they have the support from upper management to move on security issues.

Maximizing the coverage of a consistent program assures upper management of a commitment to securing confidential corporate assets. They can rely on middle management to foster an environment that put the company in the best, defensible position and not sacrifice a strong business plan.

Generally, management can encourage the proactive protection of valuable information assets. The security policy and the signatures of employees make them accountable in the event of a security compromise, but the damage will have already been done. Where as in a win situation, the awareness program AND the signature on the policy may have raised consciousness to the level that situations are remedied and avoided. Knowing that all the employees are playing defense, makes your job a lot easier.

### **The Security Organization Wins.**

The security department or organization wins all the way around. They are an integral part of the security awareness program. As such, they are responsible for content and effectiveness of the program. They must establish rapport, a team connection with their audience. Everyone must know they are part of the solution and their participation is desired and required. They must know that the security policy is theirs to help keep alive, that the security organization will respond and incorporate employee feedback where applicable. It is through a team approach, with the security organization acting as a coach that you achieve security in depth (at least numerically). It allows employees to act as a discovery agent and security personnel to coach them thru the process. The employee becomes a better intrusion detection agent and better acquainted with security people. By observing the discovery process, management and security can assess the intrusion detection, and forensic skills of the employee. (Always looking for another skilled security technician).

Security also wins because there is an open line of communication between employees and management and we're all working toward the same single goal: protect confidential information.

### **The Company Wins**

The company wins on many fronts: corporate wide involvement, great return on investment, and a defensive strategy that clearly benefits the good name of the company. The corporate wide involvement is pretty well explained above and has an added feature of being aware of the many facets of social engineering. Having a company knowing they should raise an alarm when observing someone (unauthorized) dumpster diving or asking for a password over the phone, is a powerful defensive asset.

The return on investment comes from the diminishing costs of developing and re-educating employees in the security policy. Because the policy is a living policy, it never needs re-inventing. The employees are encouraged to provide feedback, to keep the focus of policies relevant and precise. Network security is constantly growing to meet new challenges, so the security organization/person always has input to the security policy. The security community also provides current information about events that may need to be addressed by security policies.

The ability to do business on the Internet may be severely hampered by the <sup>7</sup>reputation a company has for lax security, or lack of security awareness, or of continued security breaches. Further, the reputation of a company has everything to do with market value, with business-to-business opportunities and with sales. A defensive strategy centered on protecting confidential information and sharing security programs and events can reap a bonanza of promotional opportunities.

Promotional in that the corporate <sup>8</sup>reputation as a security minded entity is enhanced. Our reputation becomes that proactive player in the security community, working with our customers, business partners and law enforcement.

Finally, the awareness program will have identified where the documents may be found. This is useful for clients, regulators, management, and by the employee who discovers any irregularity at two in the morning.

### **In Conclusion**

In summary, the awareness program has benefits that reach the foundations of our new Internet exposed company. If we are to survive, we must survive on the Internet. To survive on the Internet, we must be aware of how to safeguard company assets. We must have a Security Awareness program and a security policy. Why not benefit everyone by leveraging one from the other.

© SANS Institute 2001, Author retains full rights.

## References

- 1) GIAC Security Essentials 1.1, Chapter 5, p3 and p4
- 2) Rudolph, K. "Computer Security Handbook", 4<sup>th</sup> edition.  
Chapter 29, p2.
- 3) Netigy Corporation, Security Awareness page  
[http://www.netigy.com/solutions/security/sec\\_foundation/infosec\\_aware.html](http://www.netigy.com/solutions/security/sec_foundation/infosec_aware.html)
- 4) Farnsworth, William. "What do I put in a Security Policy". (Aug. 10, 2000)  
<http://www.sans.org/infosecFAQ/policy/policy.htm> (June 27, 2001)
- 5) Risk Associates. "ISO 177799: What is it". Copyright 1993-2001  
<http://www.iso177799software.com/what.htm> (June 27, 2001)
- 6) Guttman & Bagwell, Internet Security Policy: A Technical Guide (July 31, 1997)  
NIST Special Publication 800-XX  
<http://csrc.nist.gov/isptg/html/ISPTG-1.html> (June 15, 2001)
- 7) Baltimore Technologies plc. "Damage to Reputation", Content Security  
<http://www.mimesweeper.com/products/cs/reputation.asp> (June 20,2001)
- 8) CERT Coordination Center. "Responding to Intrusions"  
<http://www.cert.org/security-improvement/modules/m06.html> (June 21,2001)

© SANS Institute 2001. Author retains full rights.



# Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

|   |                        |                             |            |
|---|------------------------|-----------------------------|------------|
| SANS SOS London 2009  | London, United Kingdom | Jul 13, 2009 - Jul 18, 2009 | Live Event |
| SANS Future Visions 2009 Tokyo  | Tokyo, Japan           | Jul 15, 2009 - Jul 17, 2009 | Live Event |
| SANS IMPACT 2009  | Kuala Lumpur, Malaysia | Jul 27, 2009 - Aug 01, 2009 | Live Event |
| SANS SEC563: Mobile Device Forensics Debut                                | Baltimore, MD          | Jul 27, 2009 - Jul 31, 2009 | Live Event |
| SANS Boston 2009  | Boston, MA             | Aug 02, 2009 - Aug 09, 2009 | Live Event |
| SANS WhatWorks in Virtualization and Cloud Computing Security Summit 2009 | Washington, DC         | Aug 17, 2009 - Aug 21, 2009 | Live Event |
| SANS Atlanta 2009   | Atlanta, GA            | Aug 17, 2009 - Aug 28, 2009 | Live Event |
| SANS Virginia Beach 2009  | Virginia Beach, VA     | Aug 28, 2009 - Sep 04, 2009 | Live Event |
| SANS SCDP SEC556: Comprehensive Packet Analysis - Sept. 2009              | Ottawa, ON             | Sep 09, 2009 - Sep 10, 2009 | Live Event |
| SANS Critical Infrastructure Protection at Oceania CACS2009               | Canberra, Australia    | Sep 10, 2009 - Sep 11, 2009 | Live Event |
| SANS Network Security 2009  | San Diego, CA          | Sep 14, 2009 - Sep 22, 2009 | Live Event |
| SANS SCDP Cutting Edge Hacking Techniques - June 2009                     | Ottawa, ON             | Sep 15, 2009 - Sep 15, 2009 | Live Event |
| SANS Rocky Mountain 2009  | OnlineCO               | Jul 07, 2009 - Jul 13, 2009 | Live Event |
| SANS OnDemand   | Books & MP3s Only      | Anytime                     | Self Paced |