The Ultimate Defense of Depth: Security Awareness in Your Company

By Brian D. Voss

Introduction

Defense of depth is one of the key, basic principles of security taught by SANS as part of their Security Essentials curriculum. The idea is the more lines of defense a company has in place, the less likely there will be a successful penetration, the more chance there is that an attack can be detected and the most likeliness an attacker will give up and move on to another more vulnerable target. In this light, many people might think of multiple layers of technology such as firewalls, networks, host and network intrusion detection systems, bastion hosts, etc. that would comprise this defense of depth. However, we know based on published surveys and analyses that the biggest threat to our technology environment is often ourselves.

> *Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the* ***human*** *and technical dimensions. They also need to properly fund,* ***train****, staff and empower those tasked with enterprise-wide information security.*

In addition, human error is often the root cause of problems in some of the most sophisticated technological implementations. This is why security awareness in your company is so critical.

Understanding the Mind-set

During the later stages of WWII, Japan was convinced of an impending invasion of their island by the Allied forces and they proceeded to execute perhaps one of the most comprehensive security awareness programs in history. Every Japanese man, woman and child was educated on the threats to their national security and they were trained extensively on what to do at the time of an invasion. In the sense of awareness and preparedness, there was no distinction between Japanese military soldiers and their civilian counterparts because everyone was trained to fight, even if it meant using broomsticks or their bare hands. Death was the only alternative to victory. This could be considered the most ultimate defense of depth.

It's highly unlikely in today's corporate environment that the managers and the related corporate security team can foster the level of national loyalty and fortitude that was present in Japan in 1945. That's the challenge we face in the security industry because it means changing the way people think about their role in their company in relation to protecting their company's most valuable assets. There cannot be the attitude among employees that an individual (themselves in particular) cannot make or break the security of a company, because we know that security begins with each individual in an organization.

Developing a Security Awareness Program

There are key areas that must be covered in order to develop and implement an effective and successful Security Awareness Program. These components are discussed in the following section:

Upper management support and sponsorship – This area is critical by the fact that unless the corporate executives of an organization believe in Security Awareness, how is anyone below them supposed to buy in on the idea? Without this sponsorship, priorities will never be given to awareness activities and resources (both financial and personnel) will not be available. Upper management must support the security awareness program because the motivation factor to comply and participate will be that much greater. Who ever listens with any interest to the local security officer or a lowly system administrator, unless the big boss is standing behind them?

Budget the funds for the program – How can a program be successful without some sort of seed money and then ongoing budget? A company must be willing to put their money where their mouth is and financially support a Security Awareness Program. Hopefully there is already money set aside for corporate security, but the question might arise about how much to spend on an awareness program. A recent ComputerWorld article discussed this issue and the following is the breakdown on how to spend a dollar on a first year security budget:

- 15 cents: Policy
- **40 cents: Awareness**
- 10 cents: Risk assessment
- 20 cents: Technology
- 15 cents: Process, process, process

As you can see, the highest allocation of the security budget should go towards Security Awareness. The article points out that

> *Education and support generate the single biggest return on security investments. Even with perfect technology, employees can be talked into unwittingly helping a hacker…*

On the other hand, if a company literally spends only a dollar or less on security (like some I have encountered) then 40 cents won't get you very far…

Organizational structure – a team or at least an individual must be assigned the priority of developing and implementing a Security Awareness Program. It's not going to happen by itself and again this team must have executive sponsorship.

Create a plan and related documentation – the old saying goes, "If you fail to plan, then you plan to fail." Components of the Security Awareness documentation could include:

- Who is on the Security Awareness Team and what their roles are
- A description of why the Awareness Program is necessary and what it means to employees
- A roadmap/calendar of activities for the coming year related to awareness and who is responsible for executing the activities.
- Programs for new employees as well as ongoing reviews for existing employees on Security Awareness
- References to corporate security policies and procedures

An example of a quite detailed and extensive "Security Awareness Handbook" was developed by the US Department of Energy. Your plan and documentation do not need to go to this level, but at least have something written down to guide your efforts.

Use multiple means of communication – People receive and retain information effectively via different methods. Some like details and some like simple pictures. Some are online all day and others walk around the office or stand by the coffee machine. There is a wealth of resources available to communicate Security Awareness ideas to employees, including web pages, posters, videos, screensavers and newsletters. The more diverse your methods of communication that can implemented, the more chance everyone will remember, or at least be regularly reminded of your message.

Make it fun – To most of the general corporate population, the subject of security can be pretty darn boring. It can also instill feelings of fear and frustration because of the idea that security in the company only gets in the way of getting a job done. (Note that if this is the general feeling at your company, you may want to revisit how realistic your Security Policy is and how well it is being implemented). To avoid negative feelings and promote a level of interest and participation, include in your Security Awareness program activities such as like contests, games and a designated Security Awareness Day or Week. During an Awareness Week, you could have special events like an ice cream social as well as guest speakers from upper management, local law enforcement or the FBI.

Your ultimate measure of success will be if you can win over and instill security awareness in the secretary who plays Solitaire on the computer all day. (That triggered an idea – rewrite Solitaire to include security awareness slogans that scroll across the screen or flash up as commercials – any takers on that one?)

Make it rewarding – Human nature generates the thought of "What's in it for me?" One way to answer that in a Security Awareness Program is to include financial rewards. During my GIAC Security Essentials training, SANS instructor Eric Cole described a situation where the CEO of the company would place a call to the local help desk requiring assistance with his password. If the call got handled appropriately and complied with the corporate security policy and procedures, the CEO would walk down to the help desk area, publicly congratulate the employee who handled the call and present them with a monetary check. Eric did not describe what would happen if the employee mishandled the call, but we can easily imagine the effectiveness of public humiliation (or worse) in that situation.

Get professional help – (This does not mean engaging a shrink.) There are companies that specialize in Security Awareness training and providing resources (as mentioned above) so you don't have to re-invent the wheel. Some companies will even publish and distribute a customized newsletter to your employees. If you have the budget, but not the people or time, hiring a firm to do this is money well spent to raise your employees' security awareness.

Security Awareness Topics

Now that the basic components of developing a successful Security Awareness Program have been discussed, let's move on to looking at specific topics that should be introduced and promoted within your organization.

Who are the threats? – An understanding should be promoted as to who is a threat to the company. Typically people might think of teenage hackers, but other threats to discuss include corporate spies, foreign government spies or disgruntled employees. Don't forget to mention the employees themselves as they might make honest mistakes causing loss of business.

What are we protecting? – Employees need to understand which corporate assets should be protected. These could include intellectual property, competitive information, physical technology or computers, disclosure of private individuals' personal information or any other assets critical to the success of the business.

Physical security awareness – This topic brings to mind armed security guards, key card access to data centers or stolen property of the company. Employees should also be cognizant of their immediate physical surroundings. An example might be that they always leave their keyboard a certain way when they go home. If the keyboard is moved the next morning, it could mean someone was using their computer during the night. Things as subtle as this should be reported and investigated.

While working at a secure defense industry contractor, a person came to my desk selling pencils one day. He was offering a good deal, but he had no badge and there was a supply closet available where we got all the pencils we needed. My security awareness kicked in and the security guards were called to remove this unauthorized person from the premises. Needless to say there was an immediate review of the site's physical security.

Technical security awareness – Although it is critical to educate the masses on Security Awareness, the technical staff must especially be up to speed on the latest security issues. Adequate training must be available, as well as access to resources, seminars, training and bulletins. For example, awareness of the latest virus or worm threats will expedite diagnosis if a security incident arises at the company.

Policies and procedures – This can be an especially dry subject, but all employees must be briefed on the company's Security Policies and Procedures so that they understand the rules and related consequences of breaking the rules. Hopefully the policies are simple, realistic, easy to understand and are enforceable. Policies should be readily available to all employees and should be reviewed not only by new employees, but also on a schedule for existing employees.

Who's who at your company for security – Make sure your security team is known and accessible. Mug shots of the team and related contact information should be posted for use by employees.

Document handling – "One man's trash is another man's treasure…" really applies in the world of security. So-called "dumpster divers" rifle through company garbage to uncover information that can be used to gain access to or for use against the company. Employees must be aware of this and be briefed on proper procedures for disposing of (shredding) corporate documents. Also certain documents should not even be copied and these should be brought to the attention of personnel.

Incident response – Employees need to know what to do and who to call if they suspect a security incident has happened or is in progress. Clear instructions to personnel can avoid the wrong people getting involved in an incident. For example, calling in law enforcement brings a whole new set of rules as opposed to handling an incident internally within a company. Poorly timed press reports of incidents that are improperly disclosed can also do severe damage to a corporation.

Social Engineering – This term is foreign to most people outside of the realm of security study. However this technique can be the most devastating to the security of a company. Social Engineers are smooth talking criminals who have a way of drawing sensitive information out of unsuspecting victims. Employees must be aware of this because they can inadvertently disclose the wrong information to dangerous people which can lead to further security breaches at their company.

One of the most infamous Social Engineers is Kevin Mitnick. Real life stories of how he used Social Engineering can be found in the two books Takedown by Tsutomu Shimomura and The Fugitive Game by Jonathan Littman.

Password management – Too many users keep passwords under keyboards, telephones or on sticky notes at their desk. Emphasis needs to be placed on password management including creating secure passwords, changing them on a regular basis and NEVER sharing passwords with anyone else.

Email threats – attachments and viruses - "Curiosity killed the cat…" Employees need to understand the risk of opening email attachments. The most pervasive and insidious viruses play on people's curiosity. White papers can be shared and discussed regarding email threats. Email is a fundamental tool of business and the risks of using it must be understood by all.

Web threats - Surfing the internet/intranet has also become a fundamental productivity method for businesses. People need to have an understanding of what sorts of actions put them at risk while using the web. Again, there are white papers available that discuss this in great detail

Share War Stories – There is nothing like a good story to raise awareness, keep things interesting and prove a point on a certain topic. Sharing current news items regarding security incidents provides this sort of communication. Also describing events leading up to security incidents that really happened within a company and then discussing the lessons learned prevents employees from repeating past mistakes.

What does all this mean to me and how can I help? – Promote discussion around the big picture of Security Awareness at your site. Employees must feel they are part of a larger success of the business and hold responsibility for maintaining security. Clarify what is expected of them and what they can do to protect the corporate assets.

Summary and conclusion

Implementing a successful Security Awareness Program at your company may seem like an impossible task. However, with the proper executive support, appropriate planning and an organized approach, the message of "I can make a difference to my company's security" will ring loud and clear to your employees. By including the human factor in your security infrastructure via an effective Security Awareness Program, you will be implementing the ultimate defense of depth.

Cited References: