

This story appeared on SC Magazine at
<http://www.securecomputing.net.au/Feature/73905,train-employees--your-best-defense--for-security-awareness.aspx>
2/21/07

Train employees - your best defense - for security awareness

By: Luis Navarro

With so many security threats on the horizon, it may be comforting to know the strongest security asset is already inside the company employees.

New security threats and identity theft schemes are being developed every day, and large corporations continually invest millions of dollars and thousands of man-hours to keep their information and identity safe and their network secure.

But investing time and money into securing the organisation and its customers can be completely undermined if employees don't understand their role in the security plan.

Even when an organisation has state-of-the-art technology, strict security policies, and a highly skilled IT staff to manage policies, some organisations are not as secure as they could be. In fact, a recent survey conducted at Interop New York 2006 showed 40 percent of IT managers surveyed reported that their organisation had experienced at least one security breach in the last year.

Unknown security risks

Employees can unknowingly pose security risks to the organisation they work for in a number of ways:

- * Poorly designed passwords may increase the risk of network attack.
- * Improper control of laptops or other mobile devices can lead to the loss of proprietary information.
- * Failure to update virus software may lead to the infection of one or many computers.
- * Surfing the web and downloading files from the internet can reduce network bandwidth and loss of worker productivity.
- * Falling prey to a social engineering attack may lead an employee to divulge confidential information.

However, with the right training, employees can become an organisation's strongest security asset.

A security awareness program enables organisations to improve their security posture by offering employees the knowledge they need to better protect the organisation's information through proactive, security-conscious behavior. To successfully protect information assets, employees at every level - from the top down - need a basic understanding of security policies as well as their respective responsibilities in protecting these assets.

Management personnel with security responsibilities require additional training. Without this understanding, organisations cannot hold employees accountable for protecting the organisation's resources and ultimately, its profitability.

To be effective, a security awareness program must be ongoing and include continuous training, communication and reinforcement. A one-time presentation or a static set of activities is not sufficient to address the ever-evolving threats to the security landscape. The key messages, tone and approach must be relevant to the audience and consistent with the values and goals of the

organisation. Equally important, an awareness program must influence behavior changes that deliver measurable benefits.

Internal evaluation

One of the most overlooked, yet significant steps in creating an effective employee security awareness program is assessing existing security practices and employees' level of security awareness. Organisations must evaluate their current environment and determine if there are any security awareness problems or particular needs to address.

Answering the following key questions will help provide a useful assessment:

- * Is there a security policy that is enforced across the entire organisation?
- * Do employees know the security policy?
- * What are the practices and technologies in place that can help detect a security breach?
- * Do employees know what to do if they detect a security violation?

Answering these questions can help organisations define objectives and goals for any awareness training program. The objectives should also align with the overall goals of the organisation. Current security practices should be used as a benchmark to determine if training is helping to achieve the objectives and goals that have been set. It also makes it possible to set clear, measurable objectives in the beginning.

Sell security awareness internally

Another important initial step is getting upper management and senior officers on board with the program by showing them how an effective training program can positively affect the organisation's bottom line. Show senior management a cost/benefit analysis that includes an estimate of how much money the organisation loses each year due to security breaches. If possible, show how the root cause of many of these breaches was caused in part from human behavior.

Once these costs are understood it is easier to demonstrate how training and/or education programs can help prevent or, at least, reduce costs associated with these threats. If senior management is shown the value of the program, then they are more likely to approve and support it.

When presenting the case for these programs it is important to emphasise that while these security incidents are damaging, employees can help prevent many of these vulnerabilities.

Designing of the program

An effective security program brings together a team of personnel from a broad range of departments in the organisation, including IT and physical security, human resources, accounting, legal, marketing, and internal communications. Having input from various sources within the organisation will help to produce a complete security program for the entire company, with specialised messages and delivery methods for each department.

The program design requires the development of a significant amount of documentation, including:

- * High-level charter that explains the program's objectives
- * High-level design that defines current security issues and how they will be addressed
- * Detailed documents that describe how the program will be implemented, managed, and measured

In conjunction with the design, the task force should consider branding issues to ensure that employees associate the program materials with the organisation. Additionally, this group will need

to determine the look and feel of all materials (for instance, online materials, printed copies, videos, and presentation materials) and establish how they will implement the training.

Implementing the program

Employees need to clearly understand their role as it pertains to each security policy. If employees understand the importance of their role in keeping the organisation's data secure they are more likely to alter their behavior and think twice about opening a questionable email attachment.

Therefore, the training program is critical because it explains the organisation's security policies and the necessity for implementing these policies. Using security industry best practices as the basis for the content of the training program will ensure that companies are addressing security concerns with proven methods. Once employees have a basic understanding of security policies, they can apply simple steps to help them protect the organisation's information.

As with any program, the success of a security awareness program will rely heavily on how the information is delivered. Security awareness training should be incorporated into new employee orientation, as well as special training sessions by department, while executives and managers may be more receptive to training that is incorporated into regular management meetings.

A good way to reinforce what has been learned is to offer rewards and positive feedback to employees for improving their security behaviour. Rewards can be presented to individuals or company-wide. Announcements can be made through company newsletters or mass emails that show employees a comparison of statistics from before and after the training. Seeing that others in the company are making the effort to become more security conscious will further encourage employees to continue good security behaviour.

No matter the scope of the program, employees are an asset to any organisation's security posture. The more businesses define them as such—and the more training they receive on security initiatives—the more secure an organisation's data and information will become. As organisations continue to implement and reinforce training programs, they will continue to see an increase in both security and employee productivity.

Copyright © 2009 Haymarket Media. All rights reserved.