



FEATURE



The Problem with End User Security Training: Part One

[By James Stanger]

If you were to get any CIO, IT administrator, or manager to sit down and discuss the common causes of security problems on their networks, you'd get the standard litany of worries. You'd hear about improperly configured systems. We've all seen an improperly configured firewall open up security holes. Just as often, we've seen a problem firewall make it impossible for authorized workers to do their jobs, thus bringing legitimate, time-sensitive projects to a halt. Another big contributor to security problems is improperly written software. Carelessly or rapidly-written applications can introduce buffer overflows, the possibility of zero-day attacks, and dreaded enterprise-wide worm attacks. However, problems created by end users — what I often refer to as “wetware,” likely contribute the majority of problems on a network. We all know how often the beleaguered IT worker loves to sit down and tell tales about the latest adventure they had with an end user or, even worse, a group of end users.

Some Numbers to Explain the Problem

In April 2006, the MSP Alliance conducted a report of a survey it conducted concerning wetware-based problems. The survey revealed that 59.2% of the security-related incidents that occurred in companies that year were due to human error. However, the same survey revealed that only 36% of these companies had any sort of end user security training program. So, it would seem that even though wetware causes the majority of our problems, relatively few people are interested in doing anything about it.

Why Don't Companies Do It?

So, why doesn't end user security training occur more often? Teaching end users how to keep security is an essential task for any IT administrator who wants to keep the company secure, after all. End user security training is also problematic, because the administrator is faced with several key problems. At CIW, we were able to poll a few CIOs, as well as gather together some thoughts from across our worldwide network. The following are responses to why end user security training is often not a priority.

- **Lack of Time.** Any IT department has limited resources, and often

end-user security training is the first casualty as departments trim projects. After all, most training is conducted in-person, as it's difficult to use a purely online training option.

- **Lack of Employee Motivation.** Most end users are either intimidated by the very concept of networking, or they simply don't care enough about the topic to actively learn.
- **End Users Won't Get It:** Typical IT administrator is to assume that end users wouldn't understand the training, anyway.
- **Employee Indifference.** One of the most frustrating things to any CIO — or anyone for that matter — is spending time to create a useful information exchange, only to have that time wasted by employees who simply refuse to comply. Therefore, many IT managers and executives have lost faith that their employees will comply.
- **Lack of Managerial Support.** It's often a struggle for IT managers to get fellow department managers to provide time for employees to

receive security training.

- **Undue Focus on Technology to Solve the Problem.** Many IT administrators have equipment they need to justify. The CIO might have difficulty justifying a new firewall or intrusion detection device if the story gets out that end user training has increased security so much.

Training as a 'Culture War'

One CIO, in his response to our question about why end user training is such a struggle, pointed out that employees generally resist any rules given to them.

“Employees, who refuse to implement reasonable security at home before establishing a VPN connection to the office, believe that a ‘no USB device’ rule is ‘Draconian,’ and feel they have a ‘right’ to continue to download unauthorized software and content (often spyware — and/or virus-infested). Security training may seem like wasted effort.”

Is the problem, then, the fact that people increasingly work from home? No. That USB has become truly ubiquitous? Not really. Or that software is freely available? Strike



FEATURE

three. According to this quote, it's that end users have a sense of entitlement about "their" PCs and how they access information on them.

In short, to get any end user security training going at all, the IT administrator is faced with a task no less daunting than changing a company's culture. After all, a simple end user security training request might be perceived as an attempt to interfere with time-honored practices concerning how the company transmits and stores information. Even worse, your attempts will be construed as a way to monitor how an individual works. After all, security measures are often inherently inconvenient. Security training is at least that inconvenient.

More Information: The Employee Perspective

To get some perspective on these issues, consider what motivates your employees. While some are truly interested in helping the company, most are, well, much more ambivalent. Consider the following unwritten rules in companies.

A fairly well-known study conducted by the Gallup Management Journal in 2007 provides some useful insights into how to approach end user security training. This survey has been conducted for several years now, I should note. While the 2007 study doesn't discuss security per se, it does give insight concerning the thought processes of the employees you will be instructing. The survey focused on the extent of employee interest in accomplishing company goals. Specifically, the survey was designed to determine how engaged employees were in accomplishing company goals. The following are the results of the survey.

- 26% of the employees are actively

involved in accomplishing their company's goal.

- 55% are basically "fence sitters." They're effectively just putting in their time.
- 19% of the employees in a company are actively involved in actually resisting the company's goal, and are unhappy, spreading discontent.

Earlier surveys, such as in January 2006, had slightly different statistics (27% actively engaged, 59% not engaged, 14% actively disengaged). The most important points to consider from these results are the following.

- You will need to make an extra effort to even begin communicating with over half of your company.
- Even if just over a quarter of the people in your company are actively engaged in accomplishing its goals, only a fraction of those people have any real knowledge of how to keep the company secure, outside of "common sense computing steps." And many don't even know those steps.

Will All These Users Attack the Company? Not Directly, at Any Rate

The above statistics hardly state or even imply that 19% of the employees are actually trying to subvert the company's security. Obviously, it would make sense to estimate that the potential "internal hackers" who defeat company security probably belong to that 19%. Yet, as a corporate manager or director, it would make sense for you to consider that you don't just have to worry about a portion of the 19% of the people

in your company. You actually have to worry about at least 80% of the company because the last thing that fence sitters and discontented employees are going to do is worry about maintaining or improving company security.

But a percentage of these users will be responsible for indirect attacks. Through carelessness or sheer ignorance, they'll take steps that will cause critical security problems for you. Some might even actively try to introduce a security problem, but that's not the main concern here. You want to figure out how to motivate your employees to reduce risky behavior and to compute securely.



Motivating Employees: The Key

If you wish to increase the security level of your company through end user training, then find a way to motivate employees. Successful teaching implies the ability to motivate. So, in future articles, we'll be discussing ways to motivate and train individuals to improve security in your company. In future articles in this series, we'll look at ways to motivate employees, for example, and also why legislation over the past few years (Sarbanes-Oxley, anyone?) has driven the need for end user security training at the corporate level.

Next in this series will be an article entitled "The Personal Privacy Angle," which is where we give end users specific steps that help them secure their own online identities. The angle is, effectively, finding a way to get people to act in their own self interest in



FEATURE

such a way that it helps your company secure itself at the same time.

Works Cited

MSP Alliance.com. "End-user security training saves money." Thursday, 27 April 2006.
www.mspalliance.com/psysb/index.php?option=com_content&task=view&id=670&Itemid=57.

Gallup Management Journal. "Gallup Study: Feeling Good Matters in the Workplace." January 12, 2006.
gmj.gallup.com/content/20770/Gallup-Study-Feeling-Good-Matters-in-the.aspx.

About the Author

Dr. Stanger is an accomplished security consultant, writer, curriculum designer, and web designer. As Chief Certification Architect for VCampus Corporation, he manages the CIW, CTP, and CCNT certifications. He is also Chair of the Linux Professional Institute (LPI) Advisory Council and has helped design certifications and curriculum for Symantec, CompTIA, and the Telephony Industry Association (TIA).

An award-winning author, Dr. Stanger has written titles for O'Reilly, IBM, McGraw-Hill, Wiley, Elsevier, and ComputerPREP. His writings have been translated into over a dozen languages. James has spent

the last two decades writing, lecturing, and consulting about network security, web design, open source, Linux system administration, and convergence networking (e.g., VoIP). Past clients include Securify, The Association of Corporate Council, the University of California, and Brigham Young University. He regularly gives presentations on security, web development, and open source worldwide, from Edinburgh to Beijing to San Francisco. He lives and plays near the Puget Sound in Washington State.

EmploymentCrossing is the largest collection of active jobs in the world.

We continuously monitor the hiring needs of more than 250,000 employers, including virtually every corporation and organization in the United States. We do not charge employers to post their jobs and we aggressively contact and investigate thousands of employers each day to learn of new positions. No one works harder than EmploymentCrossing.

Let EmploymentCrossing go to work for you.