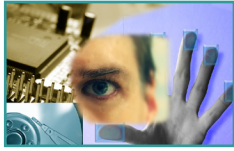




FEATURE



The Problem with End User Security Training, Part Two: The Personal Privacy Angle

[By James Stanger, PhD]

In my [previous article for TechieCrossing](#), I looked into why end user security training doesn't occur on a regular basis. I concluded that end user training fails — is just plain not conducted — because of the following simple fact: CIOs and IT managers have failed to understand what motivates end users.

One Company, Two Cultures

At the risk of sounding overly dramatic, a cultural cold war exists between end users and their IT departments. To one side (the end users), it's an "all about me" proposition. Do you remember the "I Love My PC" stickers that employees used to stick on their computers back in the 80s and 90s? The stickers may not be popular anymore, but the spirit behind them is alive and well; people consider company computers to be their computers.

Computing Is Personal for End Users

By extension, when it comes to learning about security, it's a personal thing for end users. This may not seem like much of an insight, but when was the last time you saw any company approach end user security training from the "What's in it for you" perspective? Remember, to most end users, security measures are usually perceived as impediments to be overcome. End user security training is no different. How many times have you heard the following from an end user or end user's manager: "My computer worked fine before those security measures; now I can't do my job"?

You see, when it comes to end users, their computers, and security, it's very personal. Their ability to work on their computers affects their reputation. By extension, the

information on those computers is their information, not the companies. The end user expects total control over the information in the computer, and expects to be able to use that computer in pretty much the way they want to use it. Anything that even begins to impede that ability appears arbitrary, draconian, and silly.

Don't underestimate how deeply the end user's very work identity is involved with his or her computer. If you, as the security or IT manager, threaten to change end user behavior, you'll experience resistance, because your reasonable changes appear to be tampering to almost everyone else.

Does Management Understand the "Personal" in "Personal Computer"?

For soldiers on the other side of the company-culture cold war — the CIOs and IT employees — that "personal" remains a distraction. Costs are never justified in this way. Neither is training. The following quote from a CIO living in Arizona presents one of the more common reasons for training:

"With Sarbanes-Oxley and HIPAA regulations, it has been much easier to prioritize security and motivate employees to comply with associated policies and procedures."

In other words, we do it because the

government tells us to. I can't think of any less inspiring thought than this. How many people do you know who get excited to learn something new because the government told them to? Other less inspiring motivations include:

- It's the law.
- The company mandates it.
- The company needs protection.

These are legitimate reasons. These are reasons that make sense from a business perspective, in board rooms and server rooms across the world. But at best, the above reasons are boring. At the worst, end users could silently resent having to devote their time helping you do your job.

In short, you have two wildly diverging perspectives. The result? Most CIOs lack faith that employees will comply in significant numbers and see end user security training as a waste of time. Those who actually conduct end user security training fail to realize that end users love their PCs and see them as their own. It's personal with end users. Yet most CIOs and security professionals forget this.

The Key: Make It About Them

If it's true — and I've argued that it is in Part 1 of this series — that almost 75% of the company is full of people who are at



FEATURE

best marginally engaged in achieving the company's goals, then any training based on making the company safer is almost bound to be ignored by the majority of the company. Even those who are truly engaged in the company's goals will see security measures as unnecessary impositions inspired by alpha techno-geeks and bureaucrats.

This is why end users don't like VPNs or no USB device rules. They seem arbitrary, imposed from outside. This is the culture war. Your job is to eliminate this divide by making seemingly arbitrary, artificial impositions appear as changes that are smart, natural, and helpful to them personally. Sometimes, it's better to capitulate to an idea rather than fight it. But you can choose your own terms.

So, instead of saying, "This is what the company requires," position the training as "Here is a way you can communicate securely in a modern work environment." Position the training as portable life skills, rather than as procedures required by some theoretical, bureaucratic set of rules.

End users generally feel that it's their right to continue behaviors that have traditionally allowed them to get their job done and contribute to the company. Your training efforts will at best be seen as interesting adjuncts to their behavior or interesting tidbits about computing, or at worst as proposals for making sure workers never get their work done.

Conclusion

My advice to you is to forget the IT-oriented motivations for justifying end user security and cut to the chase: appeal to the individual. The individual is the key — it's all about me, as they say. I'm convinced that nothing else will give your company the proper security foundation it requires. For Part 3, I'll take a look at specific approaches you can take to motivate not only end users, but also executives and middle management.

Works Cited

Stanger, James. "The Problem with End User Security Training: Part One." *TechieCrossing*, November 2007 (<http://www.techiecrossing.com/article/index.php?id=370125>).

Uchrin, Mike, Chief Operating Officer, Health Choice Arizona, INCNews Release. Personal email correspondence, October 23, 2007.



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.