

## Success strategies for security awareness

By Ruby Bayan

A corporate security awareness program aims to make all the employees understand and appreciate not only the value of the company's information assets but also the consequences in case these assets are compromised. In theory, the process is straightforward and painless. But as every IT/security manager knows, in real life, an awareness program can be a monstrous headache – especially in a large enterprise.

How do you start with the right foot when implementing a security awareness program? How do you determine what tools will be effective in your organization? And the big question is: How do you make everyone aware? Our security experts offered a number of simple yet often overlooked strategies.

Do your homework

According to Lena L. West, CEO of [xynoMedia Technology](#), before you start drafting a security protocol, you need to know as much as you can about the environment. The two main areas you must look into are:

- How people actually use the systems and for what purposes – "This is the most overlooked area when drafting a security protocol," said West. "If the IT manager does not understand how the company is using the systems and what they use it for, it's hard to determine security levels."
- Who *has* access to what and why, and who *needs* access to what and why – "The two lists should be cross-referenced to determine if the correct individuals have the correct access," West added.

West further stressed, "It's important for the IT manager to know how the company is using the information and she/he must also understand the dynamics of their particular industry...because security measures will not be the same at a financial institution as they would at a construction company."

"Recent [HIPAA](#) and FIPAA legislation demand higher security measures. The IT manager should do due diligence to determine exactly what's required by law and build from there. A healthcare institution may want to implement audit trails on network resources. If a file is missing, copied, or deleted, it would be important in that industry to know who did it and when. This may not be as important at, say, a bakery."

Monique Shivanandan, vice president for IT Strategy, Security & Business Continuity at [BellSouth](#), advised that the security manager must be versed on corporate goals, initiatives, and policies. "The manager must also understand the employee universe – the size, the makeup, the management style, and the corporate culture."

Get it from the top

E. Kelly Hansen is the CEO of [Neohapsis, Inc.](#), an information security consultancy and enterprise product-testing lab. She stressed that executive buy-in is paramount. "Without a corporate leader visibly backing the program, people are not going to be as eager to participate. Training takes time away from people's regular job functions. In a day in which many companies are understaffed, training doesn't seem to be a valuable trade-off. *Tyranny of the urgent* rules most organizations. Without visible executive stewardship, information security awareness programs are doomed to fail."

Likewise, West said, "The IT manager needs to understand that technology is still seen as a necessary evil. If there is no buy-in from the top – c-level and down – there will be no support of the initiative from upper management down to staff."

### Gather your allies

Hansen also emphasized the importance of working with allies. "I've seen several Fortune 1000s team up their IT managers with a counterpart from corporate communications or marketing. The IT security group provides the content, and their marketing counterpart packages it."

A similar approach would be to use internal focus groups, Hansen suggested. "It is always a smart move to run your material by several department heads (e.g., HR, legal, finance, administration) to see how well your message plays. Their feedback can be extremely insightful."

Shivanandan agreed. "It is imperative that the IT manager amass a team of leaders from multiple disciplines throughout the organization to map out a program that addresses the needs of all groups, and [it] will result in the desired level of awareness."

### Watch your language

"Most IT managers fail to realize that they speak a foreign language," explained Hansen. "The language of IT goes over like a lead balloon with most of the corporate community. Oftentimes, people feel like the IT department is purposefully talking over their heads and they actively resent it."

"One of the reoccurring issues we've seen is that security evangelists repeatedly fail to craft a message that inherently appeals to their audience," Hansen added. The key problem is in the analogies they choose.

"We have seen awareness programs wrap themselves around predominately medical and/or military analogies without understanding the impact that language can have. Not to borrow too heavily from [Susan Sontag](#), but there is great power in metaphor. Using the wrong language can ensure that people will stop listening or, worse yet, start viewing security in a negative light – something to be avoided, rather than embraced."

Hansen added that the best security awareness programs are custom in-house projects that essentially "convey your message within the context of your corporate culture." She said that "canned programs sound foreign and will not resonate well – people are more likely to tune out the message."

### Streamline your communication lines

The success of an awareness campaign would essentially hinge on how effective your corporate communication lines are. "Here at BellSouth," Shivanandan explained, "we constantly evaluate and streamline internal communication processes and procedures to leverage what we learn and to make all of our employees aware of what we are doing in the face of a disaster."

"For each initiative, we develop a comprehensive internal communications plan, orchestrated by the PR professionals in our organization. We capitalize on our online capabilities for communications purposes."

"We produce a weekly e-mail newsletter, called NewsSource," said Shivanandan. "This vehicle can also be used for news flashes at any time. We also develop a bimonthly newsletter, available in print and online, and distribute [it] to all employees. In addition, we use our BellSouth Television Network to stream messages to employees on TV monitors located in most BellSouth buildings." BellSouth also utilizes its intricate voice mail system for emergency announcements to employees via telephone. And, depending on the initiative, they use printed posters, ID badge stickers, and key chain affinity cards.

"An example of an awareness initiative that we are currently running is a campaign that involves multiple employee communications vehicles, designed to encourage employees to run a monthly scan

to ensure that all computers within the BellSouth environment are protected from Internet-based security threats."

#### Think fun

West said that another way to make sure your awareness initiatives reach everyone in the organization, call their attention, and elicit cooperation, is to make security a "fun" topic. "Many people are scared of security in general and security professionals in specific. Take the scary aspect away by showing how they are a part of security and get them involved." West suggested setting up a special e-mail or hotline where the employees can report suspicious activity.

"One possible consideration is the use of interactive games or well-placed humor," said Hansen. "A spoonful of sugar helps the security message go down."

#### Tell it like it is

"Also, I think it's important to explain WHY a given policy is in place," Hansen added. "Many people are rebellious by nature. If you say don't touch that red button, too many of us will do just that. By explaining that the red button will shut down power and cause millions in collateral damage, we are less likely to push the red button."

#### Sign off on the same page

"A written policy that staff has to sign speaks volumes," stressed West. "This protects you from frivolous lawsuits, and it protects the staff from the 'I-didn't-know-we-shouldn't-do-this' syndrome." The key to any security initiative is for everyone to be operating from the same page, she said.

According to West, the IT manager should not forget to put everything in writing, issue a copy to all staff, have them sign an acknowledgment form, and keep the forms on record with human resources.

#### Walk your talk

Another important tip came from West: Remain visible and act swiftly. "It's hard for people to respect people/policies that they can't see in action," she said. "If staff sees that security is on the case, they will realize there is no room for error and that cooperation is mandatory. If your written policy says that any employee caught downloading inappropriate material will be terminated, you'd better be able to walk the talk."

#### In a nutshell

Shivanandan wrapped up an effective security awareness strategy in a quick rundown: "First, develop a comprehensive communications plan for each initiative. Use multiple, appropriate communications vehicles to blanket the organization and ensure that the majority of employees, a) receive the message; and b) receive it in a vehicle or manner that they will respond to. Initiatives should be endorsed at the Officer level, with the message cascading throughout the organization. The message should be direct, concise, and meaningful, and the call-to-action must be clear. Managers are engaged and assist with garnering attention and support."