CREATING THE Culture of Security

Cisco Systems Offers **10 Tips** for Building a Business of Pervasive Security

EXECUTIVE SUMMARY:

The threat to information assets has never been so great. Vulnerabilities range from eavesdropping on a phone call to a stolen laptop or even a misconfigured password. Yet, small changes in behavior can have a huge upside for information security. That's why it's every employee's duty – from the executive suite to the production line – to make security a priority. In this piece, Mia Bradway Winter of Cisco Systems offers 10 proven steps to successfully educating employees and affecting security change across the enterprise.

AT CISCO SYSTEMS, the culture of security is built from the top down.

"Security starts with me, the CEO," says John Chambers, Cisco CEO and president. "Right down to the individual contributor… security is mandatory."

Yet, Cisco is a global organization with 48,000 employees and another 27,000 non-employees (contractors, consultants, temps, etc.) spread across offices worldwide. How can even the CEO reach all these individuals with a security message that is compelling enough to change behavior – at every level, in every region?

The answer, says Vice President and CSO John N. Stewart, is to embed security in the company's culture.

"Everyone is responsible for security at Cisco – whether you're designing new protocol, marketing a new product or working on our buildings," Stewart says.

To create this mindset of "security first," it's important to educate employees and build awareness of information

CSO Custom Publishing *Advertising Supplement*

Cisco Systems

security and the growing threat to intellectual property. Vulnerabilities come from everywhere in the organization – from a stolen Palm and over-the-shoulder laptop "eavesdropping" to misconfigured administrative passwords and unsupervised visitors roaming the office.

"There are little things that all of us can do [to increase security]," says Michael Disabato, vice president and service director for Network and Telecom Strategies at The Burton Group. Like taping identification on laptops, locking file cabinets or keeping current on antivirus software. "But security must be unobtrusive and consistent to be successful." Requiring a six-digit alphanumeric password to answer a phone call isn't going to cut it. The best security becomes such an integral part of everyday life that it seems to "disappear," he explains.

Stewart's charter is to shape that change, and security awareness throughout the enterprise is key to meeting that objective.

It's All About Communication

With Chambers' sponsorship and Stewart's direction, Cisco has embarked on a full-scale information security awareness program. "The goal was to deploy a proactive internal security awareness program through positive reinforcement, rewards/incentives, and cross collaboration," says Stewart. "A grassroots effort, if you will, to engage the masses."

In selecting an individual to spearhead the effort, Stewart acknowledged the importance of "marketing" security awareness at every level of the enterprise. Communications skills topped his list of resume prerequisites. He needed someone who could finesse the message and be heard by many different audiences. He also needed someone who could commit an unwavering focus to the job. Like it or not, that "someone" wasn't coming from the security organization or the IT department.

Enter Mia Bradway Winter. She's not an engineer. And she doesn't have a background in IT or security. Winter's expertise lies in communications. She's a 20-year veteran of the public relations industry.

PR? Don't balk. Effective communication is cited as the number one skill necessary for success within the CSO job function in a recent survey by *CSO* Magazine, called *The Role and Influence of the CSO*, in which nearly 500 *CSO* subscribers were polled. [see sidebar]

Reaching the Right Audience

As corporate security programs manager, Winter heads up the information security awareness efforts in the Corporate Security Programs Organization (CSPO) for Cisco. The team's mission: "To drive and reinforce behavior change that protects the confidentiality, integrity and availability of Cisco's intellectual property and information assets through awareness, training and education."

Cisco/*CSO* Magazine Research

The Role of Influence of the CSO

Cisco Systems and CSO Magazine polled CSO subscribers in April 2006 and uncovered some interesting facts:

- When asked to rate the importance of relationships with stakeholders, the majority of respondents led with direct reports (95 percent), the IT department (92 percent) and the CIO (91 percent), following closely respondents cite CEO (89 percent), line of business (86 percent), users (83 percent) and finance (81 percent).
- In regard to interacting with those other functional groups, 85 percent of security professionals indicate that they interact with the IT department, while other departments – such as line of business, direct reports, finance, and executive management – are cited by roughly 60 percent or fewer.
- Perhaps the most intriguing finding: Effective communication is cited as the number one skill necessary for success within the CSO job function.
- Employee error (unintentional) is reported by respondents as the top security threat. Yet the importance of the relationship with users and internal customers is acknowledged by only 83 percent of the respondents.

To meet this mission, the CSPO team set out to create security ambassadors. "It's important to influence the influencers and to hit the masses," Winter says. "I need individuals across the enterprise to say, 'Let's talk about security, let's change our practices.'" The first challenge was identifying the right audiences and customizing security messaging to each audience.

This is where some companies may fall short. According to the *CSO* survey, when it comes to interacting with other functional groups, 85 percent of respondents indicate that they interact with the IT department, while other departments – such as line of business, direct reports, finance, and executive management – are cited by roughly 60 percent or fewer. Winter was determined to beat those odds.

Topping Cisco's list of target audiences was executive management – senior VPs, country managers, directors and even executive administrators who handle sensitive information. These are influencers who set an example in their own behaviors and push security messaging down through the ranks. Winter also hit first-line managers, folks that touch the individual contributors. They have direct impact and can keep employees informed. Marketing and sales, as well as IT and security, were also targeted for obvious reasons.

Once the audiences had been identified, Winter was better able to tailor Stewart's security message. The theme remains constant – pervasive, extensive and unobtrusive security – but the delivery varies based on the department, role, region or even size of the audience.

10 STEPS Toward Pervasive Security Awareness

Clearly, there are varying levels of security awareness programs within enterprises across the globe. Based on her experience at Cisco, Winter offers this hard-earned wisdom on how to build security awareness in any enterprise:

1 **Get buy-in from upper management.** Indeed, John Chambers' name and rank carry the necessary clout to open doors at Cisco. When the CEO says security is important and practices what he preaches, those in the trenches take notice. The same goes for all executives and managers down the line.

2 **Appoint the right person(s) to lead the charge.** It's critical to dedicate at least one resource to the job – someone who is excited about security awareness and can focus 110 percent on the task at hand. It's absolutely essential to appoint an individual with exemplary communications skills; someone who knows how to sell, market and build relationships – in Cisco's case, a PR veteran.

3 **Conduct extensive research.** Stewart's team conducted over six months of research before launching Cisco's Internal Security Awareness Program. One must understand the target audiences and the culture of their respective organizations. "You may identify many, many target audiences," Winter says. "But with a complete understanding of each, you can customize your message [for greater retention]."

4 **Build relationships.** A successful security awareness program requires that the security message infiltrate the enterprise. Winter is part of a small team, so she needs all the additional voices she can muster. She gets her support by building strong relationships – engaging influencers and nurturing those connections. She encourages relentless pursuit, but warns that respect for an influencer's time and effort is paramount.

5 **Create security ambassadors.** What Winter cultivates from many of these relationships are security ambassadors. That is, individuals who evangelize security awareness messaging and directly influence behavior change. One such ambassador for Cisco is an employee in the Voice Technology Group who persuaded 800 individuals to take online security awareness training – resulting in a staggering 98 percent completion rate.

6 **Identify the right communications vehicles.** Look for opportunities to tell the security story to the masses. Piggyback on special events (like management summits and global sales meetings) and newsletters that are already in circulation. Don't be afraid to reuse initiatives that have worked in the past. Winter adopted streaming video to get her message across. She "copied" the concept and creative process from an existing program, tailoring it with her own message.

7 **Use credible sources.** When creating messaging for large audiences, it's important to feature

people who are recognized and trusted by the audience. Winter targets her influencers and security ambassadors very carefully, relying on individuals who are more likely to be "heard" by the target audience. It's equally important to use communications vehicles that garner respect, such as a widely read newsletter. Plaques in a meeting room may say more than posters in the cafeteria.

Top 5 Tips for Employees

1. Security is everyone's responsibility.
2. Apply your company's information classification policy to all documents.
3. Do not forward confidential information to outside personal e-mail accounts.
4. Read and comply with your company's internal security policies.
5. Secure your physical and virtual workspace.

8 Keep your messages short and simple. Like any great marketing campaign, it's better to keep things simple. Short messages are easier to retain. Cisco uses pithy lines like "Keeping Cisco secure" or "Be a security champion." Remember, Winter warns, message retention comes from a continuous, sustaining program, so repetition is a must.

9 Use rewards and recognition. The best way to motivate change is by rewarding those who take the challenge to heart. Cisco uses a semiannual Security Champion Awards system, whereby individuals who have gone above and beyond to affect change are rewarded. In addition to a marble plaque and monetary incentives, these individuals are recognized by the CSO at an "all-hands" meeting. And, their managers personally acknowledge them among their peers. Cisco also gives away Security Champion t-shirts and privacy filters.

10 Make training companywide. Security awareness training is only successful if individuals participate and internalize the course work. It's essential to make training available at all levels and encourage participation. There may never be an ideal time to put "real" work aside to take the training, but if the message is strong enough — it happens anyway. And the results can be impressive.

Extra Points for Creativity

No one ever said that building a pervasive security awareness program would be easy. It takes finesse.

Start with the basics. "Security awareness isn't IT's problem, it's the company's problem," says Disabato. To that end, he encourages CSOs to take advantage of existing company-wide communications vehicles – such as newsletters, intranet sites and email. These are inexpensive yet effective ways to reach throughout the enterprise.

At its inception, CSPO didn't have much of a budget, so the team implemented lower-cost tactics – such as annual security awareness training, internal promotions (booths, tent cards and posters), giveaways (Post-it notes with messaging and privacy filters), cascading email campaigns and the CSPO Newsletter.

They secured speaking slots at staff and executive management meetings, including executive management and global team meetings. And, as Disabato suggested, they placed regular columns in numerous Cisco newsletters, including *IT News, Engineering Insider Quarterly, GSD Monthly, Security Marketing* newsletter and others.

Cisco's reigning achievement was an ever-successful Security Champion Awards program, in which shining stars are recognized for their initiative.

With successes under their belt, Winter and her team received additional program funding that allowed them to get even more creative. For example, Winter developed a mini-movie targeting Cisco's Strategic Leadership Offsite, a gathering of executive managers.

"Our message," she says, "was to make sure Cisco leaders understand that there are outsiders that want our intellectual property. And simple things – like a corporate logo on your backpack or traveling on a plane without a privacy filter on your laptop – make you an easy target."

Winter's communications vehicle was a three-minute movie with five vignettes illustrating how individuals can inadvertently expose intellectual property. "We showed how easy it is for outsiders to eavesdrop on a cell phone conversation and steal a laptop from a bathroom stall, among other things," she explains. The program proved to be an overwhelming success.

Above all, Disabato says, "You don't need NASA to tell you what to do." Then he borrows some encouraging words from Nike: "Just do it." ■