Getting the Message Out

Sandy Sandquist, director of security for General Mills, and the Security Executive Council outline how to improve awareness programs by getting the right information to the right people, at the right time.

By Marleah Blades

A security director at a manufacturing company decides that the company's data protection is not where it should be. He focuses on the need to protect against laptop theft. He writes an e-mail that describes the risks to company information and what employees must do to protect their laptops, and then he sends the e-mail to everyone in the company.

Seventy percent of the company's employees do not have laptops. The e-mail means nothing to them. The security director has unwittingly told 70 percent of the people in the company that he does not understand them or their jobs, and he has compromised his ability to influence them in the future by spamming them with unnecessary e-mail.

Meanwhile, the CEO and the EVPs, who also got the e-mail, do not want to read about the specifics of a laptop security program — they want to know what it will to cost and what the expected results will be. The e-mail implies that the security director would like to employ new technological methods of data protection, and the senior leaders see dollar

signs. It is a bad economy and the company is struggling. This is not the right time.

Even the operations-level staff and laptop users, who would be directly impacted by the new laptop security program, cannot find the information they need in the security director's message. The operations staff needs to know how the new laptop protection program will be implemented so they can train users and prepare laptops, and the laptop users just want to know why it is important for them. The e-mail does not detail any of those things, so it results in more questions and confusion. Several recipients just delete it.

Bob Hayes, managing director of the Security Executive Council, uses this laptop protection example to illustrate what he believes are often the biggest problems in awareness programs: "They're not lined up to get the right information to the right channel at the right time."

Awareness Is Influence

In the process of developing its Security Awareness Program Tool, the Security Executive Council has discussed the elements of successful awareness programs with many of its members and faculty. Their research has shown that awareness is about much more than getting employees to follow policies and procedures. It is an organization-wide endeavor that involves earning senior management support and multi-level buy-in. When it all comes down, awareness is about gaining influence across the company.

A comprehensive awareness program includes targeted communication with people at each level of the organization, and all awareness efforts must be aligned with the business.

Four Elements of Alignment

If you want to help a group improve in any endeavor, you have to start by knowing what the group and its members are doing, and how and why they are doing it. If you play baseball and you want to improve your team's chances, for example, you have to first know a lot about baseball. You have to know the rules, who plays which position and how they play, the team record and stats, and what the team dynamic is like. If you try to talk to your team without that information, they are going to look at you like you are an idiot.

In the same way, understanding the business is key to getting the right message to the right people at the right time.

Awareness is about much more than getting employees to follow policies and procedures. It is an organization-wide endeavor that involves earning senior management support and multi-level buy-in.

The ideal strategic landscape: Security is in alignment.

As the above graphic shows, there are several elements of business alignment. Security programs — about which you are trying to raise awareness — must be appropriate to the risks, business culture, strategy and direction, and economic situation of the organization. Sometimes aligning across these elements means dropping some projects you personally would like to implement because they do not match the risk appetite of the organization. Sometimes, it means finding less expensive ways to accomplish an important goal. And sometimes it means changing the way you think.

"If a security director comes out of government knowing how to operate through policies, procedures, rules and guidelines, he or she will usually try to do that same thing in a new company," Hayes says. "Well, what if the corporate culture is such that they don't run on policy and guidelines, they run on process and procedures? This security director is trying to sell a program to the company in the wrong format. His influence is hugely diminished because he doesn't have an understanding of the company."

If you try to talk to your business team — senior management, mid-level management, staff — without first building your own awareness of the company, they may not look at you like you are an idiot, but they probably will not listen to you any more than if you were one.

Target Your Message

Once you have ensured that the program for which you want to drive awareness is appropriately aligned with the business, you have to consider how to push your message to each level of the organization.

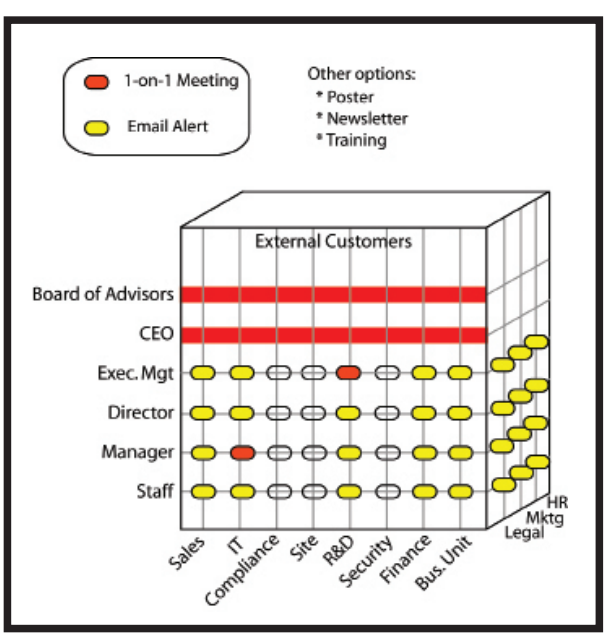
Dave Kent, vice president of Global Risk and Business Resources for Genzyme Corp., and a member of the Security Executive Council, believes targeted messaging is crucial to improving awareness at all levels. "You have to understand the business of the people you are talking to," he says. "If it is the CEO, you have to understand the business in his or her terms, what his or her level of interest is, and what level of abstraction around the issues he or she can tolerate. If it is a business unit leader or product line manager, you have to be able to understand their work almost at the level of a general manager, so you know what their markets are, what the products are, where they are on their prime maturity line, their profitability, and the finances, so you can use language that interests that person. That way, they can immediately translate the value in their own language."

Kent continues that the nature of your approach should also vary depending on the group you are reaching out to and its circumstances. "One business unit might have a higher tolerance or more resources for a certain program at a certain time, but that might not be uniformly distributed throughout an organization. You may have to push your message to that unit and throttle back on another one. Maybe one group is pushing the company into a high-risk arena and you've got to jump in there and make some demands. It's a very tailored approach — always premised on a good, solid understanding of the business," he says.

Had the security director in our laptop protection example followed this advice, he would have likely found more support. He would have communicated to the operations staff and laptop users separately what each of them needed to know and why the program would be important to them. He would have avoided spamming the majority of the business' population. He would have had a one-on-one meeting with senior managers — rather than copying them on a broad e-mail — to discuss the risks he saw and present mitigation options that were economically appropriate in the current business climate.

Tying It All Together

How you position yourself to gain influence across the company will depend on your corporate structure and the level of support and knowledge you already have. Sandy Sandquist, a member of the Security Executive Council, has had a great deal of success in the influence and awareness arena as director of Global Security for General Mills for the last 10-plus years.



Delivery methodology

"I have a small department, but we have more than 30,000 employees across the world — of which nearly 50 percent work outside the United States," he says. "You cannot (raise awareness in) a $15 billion company with that many employees with a small staff unless you are creative. And the way we become creative is by using many vehicles, not just one."

One way Sandquist maintains business alignment and influence is through what he calls the Security Board of Directors, an internal set of senior leaders that meets annually to discuss security successes and to direct strategy. "I ask them to consult with us on focusing our strategy on what the business is looking to achieve," he says. "This helps us to ensure that our program is going in the direction they need it to go, and that we are not just dictating what risks are there and what mitigating strategies may be available. It is reaching out to the various businesses and putting them in charge of what our strategy is."

This process keeps Sandquist in regular contact with business unit leaders, puts them in the driver's seat to ensure alignment, and makes them aware of security's strategy and programs. Sandquist also sits on the company's Enterprise Risk Management Committee, which is another forum that enables him to better align his program and provide bi-directional support to the business.

"You cannot (raise awareness in) a $15 billion company with that many employees with a small staff unless you are creative," Sandquist says. "And the way we become creative is by using many vehicles, not just one."

"In addition to that, we use brochures to train employees and raise awareness on our core mitigation programs, such as our food defense program and our respect in the workplace program, and we use these in multiple languages across the world," Sandquist says. "It is very important that we get the right information to people, so we use specifically targeted brochures. We provide a weekly intelligence report about events going on around the world in areas where we are located. We provide that information to senior leaders and also to those who regularly travel to those areas."

Again, Sandquist emphasizes, awareness is not about creating a pamphlet or marching in saying "I'm security and I'm here to help." It is just one part of an overarching strategy to improve business, and it ties in with alignment and risk management.

"It's not one thing — it is tying these many things together and making sure they have a singular focus or strategy in creating that awareness, and that tends to flow upward," Sandquist says. "We are trying to influence our entire population — not just management or employees — and reinforcing the fact that they all play a role in security.

"If you are out there truly attempting to help business leaders meet their forward-thinking objectives five years out and helping them with solutions on risk, you become part of the solution, and from that comes the credibility that allows you to continue with the process of creating awareness across the entire employee population," he concludes. "It tends to tumble over and grow itself." ▮

What If You Don't Have Access?

Dave Kent, vice president of Global Risk and Business Resources for Genzyme Corp., and a member of the Security Executive Council, has learned over his career that having the ear of senior management is a crucial element of awareness and many other facets of successful security. But it is not always easy to gain access to those upper echelons. Here are some tips he has to offer:

"In any organization, you have your management group and then your informal gatekeepers who may not be part of the formal power structure. You have to work your way through the channels in your organization. You have to identify people who are critical to your success.

"If we are talking about driving awareness, the first step is to have the program you are interested in pushing to the organization, or the message, service or system, then identify the key audiences and scale them. How much do those people support security and how much influence do they have? That can help you select a target audience to get leverage.

"If you have high influencers and strong supporters, work on them first because they will become disciples who can help you spread your message. You have to know your organization well enough to know your audience, and know who can help you push a message forward. Typically those folks are in different functional places, and you need to tailor your message to them so they can then take it to their own team.

It is not just boilerplate security awareness, it is a tailored message that shows you know and care about the elements of their success."

Marleah Blades is senior editor for the Security Executive Council, a problem-solving research and services organization that involves a wide range of risk management decision makers. Its community includes forward-thinking practitioners, agencies, universities, NGOs, innovative solution providers, media companies and industry groups. Backed by a Faculty of more than 100 successful current and former security executives, the Council creates groundbreaking Collective Knowledge™ research, which is used as an essential foundation for its deliverables. For more information about the Council, visit www.securityexecutivecouncil.com/?sourceCode=std.