

10 Ways to Get Users to Follow Security Policy

JANUARY 11, 2007 | It's official: Users are the weakest link in the IT security chain. You can have firewalls, encryption, and NAC up to your ears, but it still won't save you from the guy who gives all of his access information to the members of his fantasy football league.

What does it take to get end users to follow company security policy? How can you ensure they understand the rules and respect them?

There are no easy answers, but after interviewing security pros and our crack team of industry experts, we came up with 10 that are pretty good. Is your organization employing all of these enforcement techniques? Take a look and see if there's more you and your managers can do to make security happen in your organization.

No. 1: Write simple, understandable policies.

When users break policy, it's only natural to blame them for the infraction. But many policy violations are accidental, or committed by end users who didn't make the time to read the fine print. Often, these infractions occur because the policy was confusing, or just too long and detailed, experts say.

"If security policy wasn't always written in the 'Read this 15-page document with footnotes, then sign here and initial that you have read this document that looks suspiciously like an end-user licensing agreement from a certain notoriously vindictive software vendor' format, it might have a better chance of working," says Charles Tuite, operations coordinator at Ball State University. "Too often, our security policies are like the owner's manual in our cars -- unread documents."

Security policies should be clear and easy to read in just a few minutes, experts say. Keep jargon and legal information to a minimum, and don't assume the user knows anything.

No. 2: Ensure that policies don't conflict with everyday processes.

Some security policies are developed in a vacuum, without proper research on how individuals operate within the business. If a policy restricts data that users routinely need to do their jobs, you can be sure the letter of the policy will be violated. If the policy can be easily circumvented, you can be sure the spirit of the policy will be violated.

"If you put metal detectors in the school building and some poor kid gets shot on the playground, then security policy hasn't been very effective," says one security expert.

Seek out potential conflicts between policy and practice and resolve them before the policy is enacted.

No. 3: Make sure end users have read and understood the policies.

In many companies, the standard practice is to distribute the corporate security policy on paper, often as part of an employee handbook. The employee is asked to sign a form which states that he or she has read and understood the policy -- but there is no followup to determine whether the document has indeed been read.

This approach is largely a "legal" defense, which makes it easier to discipline users for breaking policy they should have read. But it doesn't protect your systems and networks from boneheaded user behavior.

In contrast, some companies require their employees to complete a security awareness course. "Our education is a mandatory practice across the enterprise, and those who do not complete it are not allowed to continue working here until they do," says Rafal Los, security architect for a Fortune 100 company. Of course, even forcing users to take a class doesn't guarantee that users will follow policies once they've learned them, he notes.

But such a requirement can make a difference in end-user behavior, experts say. Mandatory classroom hours are more effective than a signed document, and even the most reluctant attendees are likely to retain at least some of what they've learned, according to experts.

No. 4: Get the support of the company's top brass.

Many security professionals feel like voices in the wilderness, issuing policies and security warnings that are largely unheard or unheeded by end users. A chief reason for this isolation is a lack of support from top management, which causes the security department to appear weak or out of touch with the rest of the business.

Getting buy-in -- and active support -- from top managers and line managers can make the difference between end users that only hear and end users who actually listen, experts say.

"Make the C-suite your champions," says Eric Ogren, security analyst at Enterprise Strategy Group, an IT consultancy. "Senior management sets the tone for corporate culture and puts HR processes in place to make sure that users follow policy. IT security officers can't get end users to follow policy, but direct lines of management can."

No. 5: Demonstrate the risks and dangers of policy violation.

Many end users don't take security policies seriously because they've never actually seen the impact of a break-in or insider exploit on an employee or a business. That's why several of our security experts recommend that enterprises flesh out their security training with a sort of "driver's ed" style session, complete with the gory details of actual crashes.

"An ideal way to get folks to listen up is to have someone from outside the organization come in who has suffered the effects of not following a policy, such as someone whose company has been attacked or someone who has been fired for violating policy," says Pamela Howell, CEO and über-geek at Esoteric Resources Inc.

Secure Network Technologies, a penetration testing firm that specializes in social engineering attacks, frequently breaks into companies' physical premises to help demonstrate the flaws in their security plans. Afterward, "some companies have us put together a training session to explain how they fell prey to our effort," says Steve Stasiukonis, vice president and founder of the company. This approach can be a very tangible way of showing employees what can happen when they don't follow security protocol, he says.

No. 6: Keep employees updated.

Another common mistake among security teams is to treat end-user training as a one-time deal, experts say. Often, users are required to sign a document during the week they are hired, and the subject is never raised again -- even when the security policy changes.

"My company has developed a culture concerning these matters, and it is always evolving, through both written and verbal means," says Martin Smith, systems administrator at EVB, a regional bank based in Tappahannock, Va. EVB is constantly evaluating and re-evaluating security practices, he says.

In addition to updating users on changes in policy, security groups should have a process for informing users of new threats, experts say. Email is the most common method of notification, but more serious threats may require group meetings to ensure that end users understand the dangers and how to avoid them.

No. 7: Find ways to speak informally to end users.

Many end users have questions about what they can and can't do with their computers, but they are afraid to ask them in a group setting, for fear of seeming uneducated or unethical. Other users will continue behaving in a dangerous fashion because they don't want to ask questions and call attention to their behaviour.

Several experts recommend that security pros find ways to let users communicate informally -- even anonymously -- about their online behaviour, so they can ask questions or report problems without fear of reprisal.

"We try to have informal, small group meetings, and I'm sometimes amazed at how many questions I get," says one security pro.

No. 8: Don't be afraid to threaten your end users.

A few of the companies we spoke with offer positive incentives for policy compliance -- one company offers "security awareness awards" -- but most security pros agree that when it comes to policy compliance, the stick is much more effective than the carrot. When users believe that their jobs -- or jail time -- are on the line, they tend to follow security rules more readily, experts say.

"Let me use cars as an analogy," says Ira Winkler, author of *The Spies Among Us*. "Seatbelt use didn't become widespread until it became a law, and people were threatened with the stick of tickets and fines. And that is despite the fact that the carrot is the driver's life. Very sadly, policies need to be enforced through sticks -- it's human nature."

Security pros should be clear about the consequences of policy violation and the process for executing them, experts say. "Most IT policies I have seen include the line: 'Non-adherence to this policy can result in disciplinary action, up to and including termination,'" notes Steve Delahunty, an analyst at Booz Allen Hamilton. "That is the true stick."

No. 9: Monitor employees' online behaviour.

Even today, some companies set security policies without having an effective way to find out whether employees are respecting them. But there are many tools on the market today that allow security pros to monitor user behaviour, either through log file analysis or through real-time tracking of end-user activity.

"You should identify for users the mechanisms that IT will use to catch violators," says Robin Wilson, director of software engineering at Precerche Life Sciences LP. "Show users how their Web surfing activities are logged, and how automated scanners flag certain activities. Show them how certain types of email will set off alarms within IT."

Security teams also should inform users when they've identified a violation, Wilson advises. Often, it isn't necessary to discipline employees for breaking the rules -- just let them know you've seen what they're doing, and you'll see it if they do it again, experts say.

No. 10: Enforce your policies.

You can threaten and warn users for a while, but your policy won't be followed if it has no teeth, experts agree. Occasional violators should be warned. Habitual violators should be disciplined. Dangerous violators should be terminated -- and, in some cases, prosecuted, experts agree.

"All of the policies in the world don't accomplish much without the appropriate enforcement from higher up within the company," says EVB's Smith. "The teeth that [Sarbanes-Oxley] brought to the table -- in terms of fines and jail time for senior management -- opened a lot of eyes."