

The top 5 mistakes of privacy awareness programs

Despite good intentions, companies often make these five mistakes when educating employees about data protection. By Jay Cline

February 8, 2010 ([Computerworld](#))

The [Health Insurance Portability and Accountability Act](#) requires it. The [Payment Card Industry Data Security Standard](#) requires it. The [ISO 27001](#) standard requires it. In fact, every regulation that mandates that reasonable measures be taken to protect information implicitly requires companies to set up training programs to help employees understand what those measures are.

But what does *training* actually mean?

Many corporations have adopted a check-box approach toward compliance with this obligation. Here are five shortcuts I see them taking instead of using the opportunity to ensure that employees really know how to protect information.

1. Doing separate training for privacy, security, records management and ethics. Do you get one message from your [chief privacy officer](#), one from your chief information security officer, and an annual sign-off on the code of ethics from your legal department? You're not alone. In large companies, the people responsible for specific functions don't want to dilute their messages by mixing them with related topics. So they each go their own way with training and awareness. The result is confused employees who just want one place to go to learn the do's and don'ts of information management.

2. Equating *campaign* with *program*. When executives get money to spend on "soft" projects like privacy training, the natural first step is to launch an awareness campaign. Some deploy computer-based training modules. Once they do that, they might think that they have a program in

place. But there's a difference between hitting employees with one or two messages a year and surrounding them with reminders that the policies are real, have teeth and are baked into the culture. A true training program has an annually refreshed calendar of messages and training for different employee groups throughout the year.

3. Equating *awareness* with *training*. Does your company post some PowerPoint presentations to an intranet, send out some e-mails, put up some posters and say it has a privacy and security training program? An effective information-risk training program will certainly include awareness campaigns, but it will also include role-based training to educate smaller groups about what they should be doing to implement those policy objectives.

By the Numbers

More than 88% of data breaches involve insider negligence.

Source: [Ponemon Institute LLC](#), February 2009

4. Using only one or two communication channels. Let's face it: We live in a multimedia world. Our employees are used to big-screen TVs, sophisticated visual effects, podcasts, chat and more. Yet how many of our awareness campaigns are limited to a few e-mails and a couple of PowerPoint presentations? Consider incorporating sound, moving pictures and interactive content into your training program.

5. Failing to measure. Security experts often say that [insiders are the biggest threat to corporate information](#), and the list of breaches maintained by the Privacy Rights Clearinghouse is dotted with incidents resulting from employee mistakes. Employee training is probably the most important component of an information risk management process. Yet few companies actually measure the effectiveness of their privacy training programs. Consequently, the budgets for these "soft" initiatives are prime targets when it's time to cut costs.

I still remember the most effective training session I ever had, over 10 years ago. The trainer walked us past the data center, gathered us in a conference room and drew a big circle on the board. She paused, looked us in the eyes, and said, "Everything you do here will fall somewhere on this board." Some of our choices, she said, would be deemed wrong by everyone and would fall outside the circle. Some would fall into a gray area on the edge of the circle. But at this company, she said, putting a dot on the board, our choices had to be at the center of the circle.

That told me everything I needed to know about that company's policies and ethics. Will employees remember as much about your privacy training and awareness program 10 years from now?

Cline, a former chief privacy officer at a Fortune 500 company, is president of Minnesota Privacy Consultants and a Computerworld.com columnist. You can contact him at cwprivacy@computerworld.com.