

## More Than “Checking the Box” in Information Protection Training and Awareness

*This article is the second in an ongoing series in which leading organizations share best practices on addressing the human factor in compliance and information protection programs and implementing a successful privacy and information security awareness and training initiative.*

**I**n these challenging economic times, some organizations may be tempted to cut corners on information security and privacy training for their employees. Instead of going “above and beyond” to protect sensitive data, some companies may settle for “checking the box” when it comes to providing employees with the critical knowledge they need.

Well, “checking the box” is better than doing nothing, right?

Richard Purcell begs to differ. “To say ‘we comply with all laws as they are presented to us’ is a little bit like saying, ‘yeah, I stop at red lights.’ Well come on. You’ve got to do a little more than just obey the law. If somebody is crossing the street outside of a marked crosswalk or intersection, it’s still not right to just run them over.” The CEO of Corporate Privacy Group, Purcell cautions information security professionals against “all too common” advice from legal departments who see compliance as a black and white issue.

“A lot of lawyers will say, ‘Don’t sweat it. It’s not something we need to train people about.’ And I think that that’s a huge mistake. It isn’t just compliance. There’s also signaling to the marketplace a sense that you’re a respected corporation,” says Purcell.

*It is just as vital for every company to implement a high-quality training initiative as it is to evaluate its information collection, use, and management practices.*



### **A reflection of your company values**

Sandra Hughes, global ethics, compliance, and privacy executive for The Procter and Gamble Company, agrees that the way your employees handle and protect sensitive information is actually a reflection of your company values—and can have a bottom-line impact on the organization. “It really is part of how your company operates and what your corporate culture is. Your consumers are driving the bus and if privacy is important to them, it’s going to be important to you, whether or not it’s the law.”

Hughes adds, “By training our people well, by going beyond just the minimum, we are clearly signaling to them that good information management and good information privacy practices are really one of the best ways we can maintain the trust in our organization and our long-term finan-

cial success.”

“It is just as vital for every company to implement a high-quality training initiative as it is to evaluate its information collection, use, and management practices,” says Larry Ponemon, chairman and founder of the Ponemon Institute. “We emphasize the point that regulations are not the goal, but a starting point. A number of companies have been victimized by high-profile breaches even though they felt they had ‘trained’ their employees,” he notes. “A checkbox approach to compliance training becomes a meaningless exercise when your customers are receiving a breach notification letter and learn that they’ve been put at risk.”

It’s also meaningless when it comes to the PR, investor relations, and even legal damage a serious breach can cause. “It only takes one employee to do something really foolish to significantly impact the entire company negatively,” says Michael Jernigan, Microsoft’s compliance training manager for the software company’s Office of Legal Compliance. “A Bing search will turn up dozens—perhaps hundreds—of negative news stories after a high-profile breach.”

So what should a good information security and privacy training program include? How does a company design an effective program that goes beyond

See, **More Than**, page 2

**More Than “Checking the Box”***continued from page 1*

“checking the box”?

**The tone at the top is absolutely essential**

With more than 100,000 full-time employees, Microsoft’s commitment to information security training has to be company-wide. “The tone at the top is absolutely critical,” says Jernigan. “We actually have the executives from the different business groups launch the training. They send out launch communications to the employees in their group, and then we communicate with those groups through their executives on a regular basis, letting them know how their business group is doing. The best measure that this approach has a positive impact? We achieve a better than 99.5 percent completion rate on our legal compliance training annually.”

Robert Posch, senior director of global compliance training for the Schering-Plough Corporation, agrees that both the content of your information security training and the way it’s delivered are important to the success of your program. “It’s not just about how you roll out your privacy initiative. When people receive the training they need to feel comfortable that they’re getting training that applies to what they do, that has some practical value. It’s not just someone sending out training to say ‘I’ve trained everyone’ and then checking a box.” Posch says. “It is delivering training that has an innate value and influences the way that someone does his or her work or informs his or her work flow.”

“A one-time training course may help you ‘check the box,’ but may do little to actually protect your organization’s sensitive information,” says John Block, director of compliance curriculum for MediaPro, Inc., an information security and privacy training company. “If you do have a security breach, regulators may want to examine your training.”

A poorly produced and implemented

training program may help you comply with the letter of the law, but investigators aren’t easily fooled. This could be a red flag that says your company wasn’t serious about information security and was just going through the motions. “Effective training involves quality design and thoughtful implementation,” says Block. “Achieving your objectives will require more than good training; it also involves strong management support, connection to organizational strategies, and ongoing awareness and reinforcement.”

**It doesn’t have to be expensive, or time-consuming**

“Training that goes beyond just ‘checking the box’ doesn’t have to be complex, expensive, or time-consuming,” Block adds. “Examples can include hanging eye-catching posters that reinforce the training message, sending an e-mail message from a senior manager positioning how the training supports key business objectives, and providing knowledge reinforcement in the form of a simple online game which will engage the learner while achieving your training goals.”

When it comes to information security and privacy training, “You’ve got to develop an implementation plan for awareness and training that involves senior managers and other stakeholders. You’ve also got to think about what’s realistic and actionable for your particular company,” says Zoe Strickland, vice president and chief privacy officer for Wal-Mart Stores, Inc. “It’s best if you integrate it into the normal processes with which employees are familiar, into the environment with which they are familiar. This may mean a combination of e-learning, classroom sessions, and supervisory led shift-starters.”

Schering-Plough’s Robert Posch

notes that compliance training, as challenging as it may be to plan and implement, is worth the investment of time and dollars. “It’s always so much easier to deal with something proactively versus being in a crisis stage when it comes to maintaining the company’s reputation. Investment in effective training is usually very small compared to the cost of recovering from a breach!”

The information security and privacy experts we interviewed agreed that aiming for minimal compliance wasn’t enough for their organizations. With their companies’ reputations and bottom lines at stake, each has gone beyond just “checking the box.”

---

**John Block** has worked in the training industry for close to 30 years and directs the development of compliance courses at MediaPro, Inc. He can be reached at [johnb@mediapro.com](mailto:johnb@mediapro.com). The author would like to thank **Richard Purcell, Michael Jernigan, Sandra Hughes, Robert Posch, Larry Ponemon, and Zoe Strickland** for their contributions to this article.

**Contributors:**

**Richard Purcell**, CEO, **Corporate Privacy Group**

**Michael Jernigan**, Compliance Training Manager, Office of Legal Compliance,

**Microsoft Corporation**

**Sandra Hughes**, Global Ethics, Compliance & Privacy, **The Procter & Gamble**

**Company**

**Robert Posch**, Senior Director, Global Compliance Training, **Schering-Plough**

**Corporation**

**Larry Ponemon**, Chairman and Founder, **Ponemon Institute**

**Zoe Strickland**, Vice President, Chief Privacy Officer, **Wal-Mart Stores, Inc.**

**John Block**, Director, Compliance Curriculum, **MediaPro, Inc.**

*A poorly produced and implemented training program may help you comply with the letter of the law, but investigators aren't easily fooled.*