

## The Human Factor in Compliance: Best Practices from the Trenches

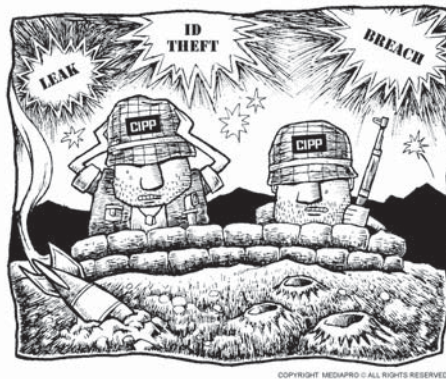
*This article is the first in a series contributed by MediaPro, Inc., in which privacy and data protection thought leaders from leading organizations share best practices for addressing the human factor in compliance and data protection programs and implementing a successful privacy and data security awareness and training initiative.*

**H**ow important is the human factor in data security and privacy? More than 88 percent of data breaches studied involve human error or negligence, according to this year's Ponemon Institute Annual Cost of a Data Breach study. Ironically, organizations invest heavily in IT tools to protect data but invest very little on training and awareness for their employees.

"And that's a problem," says Richard Purcell, CEO of Corporate Privacy Group. "Information privacy is assured primarily by the way people act on the job. Not so much by technologies and by other more tangible factors, but rather by the behaviors of the individuals. It's the employee who leaves the company laptop in his car—not the overseas computer hacker—who's a greater threat to most organizations. Most of the privacy challenges we observe have been caused by people at the very edges of the organization—staff-level employees," says Purcell. "It is those people who actually have a very strong ability to cause a significant data breach."

Michael Jernigan, the compliance training manager for Microsoft's Office of Legal Compliance, agrees, stating,

*It's the employee who leaves the company laptop in his car—not the overseas computer hacker—who's a greater threat to most organizations.*



"We've got somewhere in the neighborhood of 100,000 full-time employees and probably that many contingent staff. And it only takes one employee to do something really foolish to significantly impact the entire company legally and financially. The fact that the 'foolish' act is most likely unintentional, and/or due to being uninformed, emphasizes the need for training at all levels of the company."

### **For us, the human factor is everything**

Like Microsoft, The Procter and Gamble Company sees data security as a foundation for a solid global privacy program. With buy-in from the highest levels of management, the company has implemented a comprehensive, enterprise-wide training program to address the human factor in data

protection. Sandra Hughes, CIPP, the executive in charge of global ethics, compliance, and privacy at P&G, says, "For us, the human factor is everything. We can have the best systems and processes and standards in the world, but unless people are following them, it isn't going to mean anything."

Hughes continues, "You're always going to have those mistakes that happen inadvertently—and that's where your systems and processes have to come in. When employees are thoroughly trained in solid data protection practices, you're able to quickly fix those unintentional breaches, adjust or create new processes, and then communicate this new knowledge with effective training so that it doesn't happen again."

Robert Posch, senior director of global compliance training for the Schering-Plough Corporation, believes that companies must "influence the individual colleague at the company so they understand not just that PII (personally identifiable information) is important, but how it applies to what they do and how they do their job, so that they buy into the value of doing it right." Individual employees have to understand that security and privacy breaches can not only impact the company as a whole but also their own career success and job security, according to ***The Human Factor***, page 2

## The Human Factor

*continued from page 1*

ing to Posch. “They have to see a long-term payoff” for data security compliance, he says.

### **Leaving basic elements such as training and education out of the equation is foolish**

Larry Ponemon, the Ponemon Institute’s chairman and founder, says, “Ultimately, people are the ones who use and manage the data, so leaving basic elements such as training and education out of the equation is foolish.” And yet the Ponemon Institute’s study revealed that only 57 percent of respondents were addressing data protection with employee training and education.

So why do so many organizations have lax—or non-existent—data privacy and security training? “I don’t think people really understand the huge risk that they’re taking,” Jernigan says. Although some data breaches have led to expensive class action settlements, the Ponemon Institute reports the most negative and significant cost impact results from lost confidence and trust in the company, which translates directly into customer turnover—and in the case of a severe breach, potential loss of brand equity.

Jernigan believes that is why it’s incumbent on company management and executives “to really understand the risk and do whatever needs to be done in order to mitigate those kinds of potential occurrences.”

Getting buy-in from the organization’s executive team is a critical step, says Zoe Strickland, vice president and chief privacy officer for Wal-Mart Stores, Inc. “Once the company executives decide they want a privacy program that includes training and awareness, they’ve made a commitment and expect to see results. But too many times they simply don’t know how to get it done.” Strickland credits

executive teams that recognize the bottom-line value of training, but admits, “They don’t know what that means to the people who have to implement it. What’s the best channel to give training and to whom? What are the key messages? You’ve got a lot of work to do to help them understand the process for employee education and the ongoing support they will need to provide.”

John Block, MediaPro’s director of compliance curriculum, agrees with Strickland’s assessment. “The challenge for most privacy and security professionals is that training and awareness are not normally on their resume. So when they’re asked to plan, create, and implement a company-wide data protection program, they have no idea where to start. As a compliance officer, you may know everything about data privacy and security regulations, but nothing about best practices in adult education that will really lead to a positive change in employee behavior.”

### **The quality of the message reflects on you and the organization**

While MediaPro works with many Fortune 1000 companies, Block is still surprised by the number of companies that forego formal training in favor of a halfhearted or cobbled-together internal program, or even no training at all. “Training may be the most visible and important item of communication an employee receives to understand your message. You really need to get it right. The quality of the message reflects on you and the organization. If it’s a halfhearted approach, employees may not take the message seriously.”

He continues, “There is a widespread perception on the part of privacy and security professionals that if training is engaging and effective, then it must be beyond their budget. The reality is that high-quality online

training is quite affordable, especially when compared to the cost of data breach recovery.”

Block says that “By applying even a few time-tested training best practices, organizations can reap the benefits of a focused and successful implementation strategy. The ultimate goal is to provide training and awareness that enables an informed workforce to reduce security and privacy risks and forge strong customer relationships.”

Richard Purcell agrees. “Ultimately, you have to educate employees on good DP practices and to understand the consequences of misbehavior. It becomes a lot easier to get things done at that point.”

---

*MediaPro would like to thank **Richard Purcell, Michael Jernigan, Sandra Hughes, Robert Posch, Larry Ponemon, and Zoe Strickland** for their contributions to this article. **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).*

#### **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.***

*“We can have the best systems and processes and standards in the world, but unless people are following them, it isn’t going to mean anything.”*