

THE PRIVACY ADVISOR

The Official Newsletter of the International Association of Privacy Professionals

iapp

Editor, Kirk J. Nahra, CIPP

June 2010 • Volume 10 • Number 5

Winning support from senior management and others

This article is the third 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.

As a security and privacy professional, you understand the critical importance of solid, enterprise-wide compliance. And you're sold on the value of comprehensive training. But how do you get buy-in from the C-suite on down? That's the question we asked privacy and security leaders.

Bottom-line business case

Larry Ponemon, CIPP, chairman and founder of the Ponemon Institute, suggests that privacy and security professionals start the discussion with senior management by making the bottom-line business case for compliance. Ponemon notes that the average total cost of a data breach is \$6.65 million, according to the institute's research. But much more may be lost in terms of damaged reputation, negative publicity, and lost customer goodwill in the event of data theft or a privacy scandal.

Pointing to a study conducted by the Royal Bank of Canada, Richard Purcell, CIPP, CEO of Corporate Privacy Group, says the data supports the bottom-line business case for privacy and security training. The study demonstrated that a certain percentage of the bank's profitability and customer loyalty was due specifically to data protection practices. "Get your management to understand that investing \$50,000 a year in privacy training helps reduce the chances you'll face a million dollar judgment from your regulator," says Purcell. "Produce metrics that help management understand that there is a profit factor in establishing loyalty and depth of service with your customer base," he adds. "Compliance, then insurance, then profit. That's the wise way to do it."

The right thing to do

"What we emphasized with our leadership—especially in a company where we're so focused on customers—is the importance of the brand," says Gregory Maher, director of privacy for U.S. Cellular. His strategy is shared by Sandra Hughes, CIPP, the executive in charge of global ethics, compliance, and privacy for The Procter & Gamble Company. "We did do some research and focus groups with consumers early on to see how they felt about privacy," Hughes reports. She and her team showed the company leadership that consumers were strongly concerned about privacy and security issues. Maintaining privacy and security "is just the right thing to do," says Hughes. "We have to build that trust with our customers, and we have to build that trust with our employees."

Zoe Strickland, vice president and chief privacy officer of Wal-Mart Stores, Inc. says, "I don't think you get the same support for privacy and security training unless leadership understands how training fits into your corporate mission and culture and that it reflects your goals and values."

Significantly increasing training success

Once a compliance officer identifies the legitimate business case for privacy and security training, industry leaders we interviewed emphasized the importance of cultivating leadership buy-in. John Block, director of compliance curriculum at MediaPro, Inc. says that "engaging the support for the training initiative from managers and stakeholders is one of the most important tasks for an information security professional. It will have more influence on the success (or lack of success) of training than any other factor." Block adds that "Management support can range from endorsing training, which is passive support, to actively participating in the planning and implementation of training. The odds of your training being successful increase significantly the more active managers are in the process."

"Our research consistently shows that C-level executive buy-in is vital to an organization's willingness to allocate sufficient resources for the implementation of effective security training," says Larry Ponemon. "If the executive suite fails to appreciate the risks, and their role in setting a strong example from the corner office, the information security team has a steep, uphill battle."

This doesn't appear to be a problem at Microsoft, notes Michael Jernigan, Microsoft's compliance training manager in the Office of Legal Compliance. "The impetus behind the training requirement is actually coming from our board of directors. They have said, 'You will do this as a company, and this is important.' And they've given us a specific amount of time for compliance training that we can do annually." Jernigan continues, "The fact that Microsoft CEO Steve Ballmer is supporting it by providing the introductions to the training in a video clip...the fact that the executives are involved, either on video or through training launch communications...the fact that the executives talk about the importance of compliance...that's what establishes the importance of completing the training as far as our employees are concerned."

Building your team

So, how do you build your team of "white knights" within the leadership structure? How do you identify stakeholder team members? "I think you identify two, three, four, five key stakeholders and they become your core team—and that would include subject matter experts for each of the topics and your technical support people," says Microsoft's Jernigan. "You have to know who your core stakeholders are, who the key players are. I think one mistake that a lot of people make is they try to involve too many people. And when you do that, you start making training decisions by committee, and pretty soon things start falling apart."

Wal-Mart's Zoe Strickland has built an eclectic team. "As an example, I have a team member who has a law degree and knows a lot about emerging laws, emerging technology, emerging standards, and things of that nature. And another team member has a lot of store experience. He can really understand how the stores operate and manage data. You want to think about a blend of skill sets. For Wal-Mart it was important to get a blend of different people; some who'd been here many years and others who brought new blood."

Your elevator speech

When approaching leaders to get their buy-in, "have your elevator speech ready," advises Cara Gorsuch, who is responsible for Enterprise Information Security Policies and Awareness at Supervalu.

“Management is going to ask, ‘Why is this important?’ It is critical that they understand the value that training and awareness would add to the organization. Going in unprepared when meeting with executive or senior management means you are wasting their time. So do your homework and get to know who your audience is...that’s part of what you have to do to win support. What are their concerns? What are their objectives? Tell them how your plan helps them meet their objectives, and come prepared with answers to their likely concerns.”

And once you do identify the executives and managers you want to recruit to your leadership team, it's important to speak to them in their “native tongue,” says Karen Sutherland of the Sacramento Municipal Utility District's QA and IT Training Group. “If I’m talking to accounting,” she says, “I’m talking in numbers. If I’m talking to customer service, I’m talking in ‘customer-service-speak.’ If I’m talking to business technology, I’m talking ‘techie’...it doesn’t do any good to go in with ‘training speak,’ and talk about blended learning styles and role development and storyboards; none of that rings true to them.” Sutherland continues, “What you need to say to them is, very succinctly: ‘At the end of the day you want to have your folks do X, Y, and Z to protect information, and here’s how we’re going to help you do that. We owe it to our customers to maintain their information in a safe and secure manner. It is imperative. We also owe it to our employees. How do we minimize their risk? What do they need to do? And, of course, why is it critical to the organization?’”

They really want to pitch in

“One of the things we’ve learned from winning involvement and support from managers and stakeholders is that once we get them onboard, once we have a win-win relationship with them, they really want to pitch in!” says Sutherland.

“Having designed privacy and security training for dozens of enterprises, we’ve seen how important management and stakeholder support is to the process,” says John Block “The odds of training being successful increases significantly. And support is important before, during, and after the training. Unless managers reinforce the knowledge and the expected behavior changes, then the impact of the training will be short-lived.”

*MediaPro would like to thank **Richard Purcell, Karen Sutherland, Larry Ponemon, Gregory Maher, Sandra Hughes, Michael Jernigan, Cara Gorsuch, 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.*