Don't Forget the Culture Check

By Marleah Blades, Contributing Columnist

Before implementing new security measures of any type, there are a lot of checks to make. When launching physical security technology, such as a new surveillance system, checks are made on hardware and software, policies and staffing requirements. And when you go live with new network security measures, checks are made on all the connections and rules, and with the support desk to make certain they're ready for calls.

But in any of these instances, do you check the potential impact on the corporate culture? Believe it or not, that may be the most forgotten, and most important, check to make.

Mike Kalac, CISO and VP of information security for Western Union, learned the importance of the corporate culture check when the company decided to move its information security function out from under the IT umbrella. Kalac saw the change as a great opportunity. He welcomed the chance to give information security a stronger business role in the company. He and his colleagues immediately began working on a two-year roadmap for IS based on the projected development of the organization, assets and technology.

After careful planning, Kalac's team chose several new technologies and tools and updated company usage policies to reflect the new security focus. The new solutions would provide a more secure corporate network by, among other things, employing Web filtering to block access to select external sites and to scan downloaded files, and loading a client on PCs that enabled asset tracking, better patch management, and locking down risky applications. IS announced the upcoming changes to employees, and employee response came much more quickly than he expected.

The Backlash

"When we began sending out communications to let employees know what we were doing and how it would impact how they worked, we immediately started getting feedback from employees saying, 'Why are you trying to stop me from doing my job?' and 'You can't just put everyone under lockdown,'" said Kalac.

"When I met with the internal colleagues to talk about filtering, we were discussing what employees would be allowed to run on their PCs, and I made the statement that we won't support programs like iTunes. Feedback based on that comment was that as a company, 'We encourage our employees to use iTunes and also other Internet sites used to balance their personal and work life.'"

The team explained that in many cases, employees are working between 10 to 15 hours per day, so they felt it was important to allow employees the benefit of doing some of their personal business, like online banking, and enjoy some minor luxuries, like listening to their own music, while at the office. Also, the company was trying to reach out to a new generation of potential customers by advertising on social networking sites like Facebook and Myspace.

Kalac left the meeting knowing that IS's new roadmap had done more than irritate a few vocal employees. "I discovered that when we started sending out communications on our plan, we were unwittingly playing with the existing corporate culture. Here we were in the security space, stressing the importance of protecting the company from existing and new threats, and meanwhile the company culture was driving the work-life balance aspect and the need to access non-traditional, non-business Web sites. At the time I didn't realize that our actions would impact the corporate culture as much as they did," Kalac said.

Adapting to the Corporate Culture

IS had always seen the corporation as security-minded, interested above all in information protection for customers both internal and external. Internal colleagues saw it as a business that wanted to show clients and employees that it was keeping stride with the times and technology and allowed some flexibility to employees who worked hard, long hours for the company.

Western Union has a defined corporate culture, however, managing security within a company that is doing business in over 200 countries requires a constant "finger on the pulse" of the company culture versus the security initiatives. "Knowing that security and culture of the company are not static, you must continually re-evaluate your impact on the company," Kalac said.

Kalac confirmed this discovery over and over as he met with other business unit leaders across the organization to talk about IS's new plan. His team considered each group's concerns and priorities, and then adjusted the IS approach to network security where the risk/benefits balance allowed it. One way they shifted their strategy, for instance, was to change their approach to site blocking. While some external sites must remain blocked, others that are important to various business units' cultural and business concerns are instead prefaced by coaching pages – pages that warn users that they may be entering risky sites.

Kalac believes the best way to gauge the cultural impact of a security change is to increase positive communication with colleagues and business leaders across the organization. "An information security leader should be concerned about reaching out to others in the organization to find out what the corporate culture wants to be and how to drive that culture," said Kalac. "This is something information security has to think about before it deploys a plan to secure the company." SECURITY

About the Author

Marleah Blades is senior editor for the Security Executive Council, a member organization for senior security and risk executives from corporations and government agencies responsible for corporate and/or IT security programs. Find out more at www.securityexecutivecouncil.com