5 BEST PRACTICES TO MAKE SECURITY EVERYONE'S BUSINESS

Employees are one of your greatest risks to information security. Use these five proven techniques to strengthen your security strategy and protect your business.

"When policies are developed collaboratively across the company, and security awareness is woven into the culture, violations are infrequent."

— STAN BLACK
CHIEF INFORMATION SECURITY OFFICER
CITRIX

Menaced by an ever-expanding array of increasingly potent threats, today's highly mobile employees are front-line participants in the struggle to secure the enterprise. So while solid security strategies must include smart policies, rigorous enforcement, and deep monitoring/reporting, they must also reflect the needs and habits of the company's users.

"End users are ultimately where security succeeds or fails," says Kurt Roemer, chief security strategist at Citrix.

Unfortunately, keeping employees both safe and satisfied isn't easy. Employees want anywhere, anytime access to information from any device without cumbersome security protections slowing them down. Business managers want to safeguard important information without inhibiting growth, innovation, and competitiveness. IT departments want to keep everyone productive while recognizing that employees and their devices are often the weak links in the security chain.

To balance those competing interests, security leaders should follow these best practices:

1. Educate users

An informed, security-conscious workforce is every company's first line of defense against security threats, so teaching people how to work safely from any location on any device must be a top priority.

Simply preaching best practices is a recipe for failure. Take the time to understand who your users are, what they do, and what they need. Then explain your company's security policies to them in terms that are easily understood and relevant to their role.

"Relevance is key," Roemer says. "Everything you present should be specific to a person's function rather than one-size-fits-all."

It should also be personal, Stan Black, chief information security officer at Citrix adds. For example, in addition to work-related security training, Citrix gives its employees advice on topics like securing a home wireless network and helping their kids use the Internet safely.

"We try to tie all our education efforts to the full lifecycle of

security, not just what people do at the office," Black says. That makes security training more valuable for employees while also protecting sensitive data from poorly secured personal hardware.

2. Engage with line-of-business organizations

Close working relationships between IT executives and line-of-business managers are an essential ingredient for effective security. Meeting regularly with business decision makers empowers security leaders to build appropriate safeguards into new business initiatives right from the beginning. It also gives them an indispensable, up-close perspective on a business group's unique risks and requirements.

"You'll learn more about operational processes and potential dangers that you'd never know about otherwise," Black says. "You can then incorporate those insights into your security plans and make them even richer."

3. Take a modern and mobile look at security policies

As critical as it is, training alone doesn't ensure strong security. Many of the devices, networks, and storage systems employees rely on these days are outside of IT control.

"IT needs to update traditional security policies for the new mobile and cloud services reality," Roemer observes.

Start by thinking through how strictly you want to limit access to your company's data based on where an employee is located and what kind of device they're using. Most companies adopt graduated policies that protect sensitive information more carefully than public information and provide less access from consumer-grade and "bring your own devices" (BYOD) than from more thoroughly "locked down" enterprise-grade devices.

Then revise your security policies to reflect risks like storing business data on personally owned devices, posting passwords on a computer monitor, or using a USB storage device you found on the floor.

4. Enforce policies fairly and consistently

Security policies can lose value over time if users don't believe violating them has consequences—or worse yet, if they believe bypassing them improves productivity. Policies must be maintained and kept current with the business. Security leaders must therefore enforce policies fairly and consistently.

"When policies are developed collaboratively across the company, and security awareness is woven into the culture, violations are infrequent," Black says.

5. Automate security seamlessly

To further reduce policy violations, use security software to automate policy enforcement. For example, many security solutions can implement desired behaviors—like encrypting business data on mobile devices—by default. They can also build tighter security into core elements of the user experience by automatically preventing employees from running unauthorized apps over the company network or limiting which apps people can open email attachments with, for example. Other solutions provide logging and reporting functionality that can help you prove to auditors that you've applied appropriate policies scrupulously.

Even so, software is ultimately just one piece of the security puzzle.

"To really protect the company you have to get to know your line-of-business groups and your end users," Roemer says.

Ultimately, the best security strategies are as much about people as technology. ■

HOW CITRIX CAN HELP

Securing the enterprise takes close engagement with employees and line-of-business groups. Security and compliance solutions from Citrix offer powerful help by ensuring security and compliance for critical business information while empowering your workforce to work anywhere, anytime, on any device.

Citrix XenDesktop allows companies to publish Windows apps and desktops in the data center, where IT can maintain centralized data protection, compliance, access control, and user administration. Citrix XenMobile provides rich enterprise mobility management capabilities, including identity-based provisioning and control of apps, data, and devices. Citrix ShareFile enables employees to share data securely with anyone and sync data across all of their devices. Citrix NetScaler adds a unified management framework that lets IT secure, control, and optimize access to apps, desktops, and services on any device.

Citrix solutions are "secure by design" systems carefully architected to minimize vulnerabilities and are complemented by state-of-the-art offerings from industry-leading security partners. The end result is comprehensive protection that enables business units and employees alike to observe company security policies without compromising productivity or profitability in the process.

To find out more, please visit www.citrix.com/secure