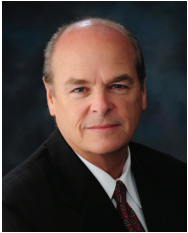


FIVE WAYS TO HELP END USERS BOLSTER SECURITY IN 2010



As vice president, Diebold Security, Bradley J. Stephenson is responsible for leading the organization to provide integrated security solutions that help protect end users from criminal activity and critical loss while enabling business in a safe, secure and efficient environment. Stephenson earned a bachelor's degree in computer information systems from Aquinas College in Grand Rapids, Mich., and has spent nearly 40 years in the security industry.

Bradley J. Stephenson
VICE PRESIDENT
 Diebold Security

The following Diebold column was originally published in the Today's Systems *Integrator* e-newsletter on January 12, 2010.

From one end of the globe to another, criminals are getting smarter. As their attempts to steal assets become more informed and more sophisticated, the need to stay one step ahead of them is even more critical.

At the same time, organizations have more priorities than ever before, and security may not be top of mind. Security integrators must help them remain focused on the protection of their assets. In 2010, we can help end users bolster their security by understanding risk, leveraging physical and logical security, working toward convergence and fostering trust.

Help End Users Understand Risk

As security experts, we can help our customers mitigate their organizations' vulnerabilities. That's why the effort to help customers identify and understand their risks should be a top priority for security integrators. Awareness of the threat environment and how it could potentially impact assets is critical to creating an effective security strategy.

Leverage Physical Security as the First Line of Defense

In today's world of identity theft, cyber crime and data loss, physical security remains the most fundamental form of protecting assets. While data security is getting much-deserved attention, we must not let our customers underestimate the value of a proactive physical security strategy.

The key to building a proactive physical security strategy is to help end users think like criminals. How might criminals try to infiltrate a facility? What might they do to make assets vulnerable? What gaps might they find in protection measures? A physical security plan should answer these questions, and it should enable end users to stop would-be criminals at all points. To do this, an effective physical security program should incorporate perimeter surveillance, interior hardening, access control, intrusion detection and a UL-certified central station.

Give Logical Security the Attention it Deserves

Threats have changed in character. Gone are the days when the most dangerous threat was posed by a criminal coming through the door with a weapon. As technology has evolved, threats to data – hackers, viruses, insider sabotage and more – have become more prevalent.

Logical security breaches can be more expensive and more damaging to a company's brand than any threat previously faced. The impact of

the theft of consumer information, for example, is often far-reaching and long lasting. Direct costs are high, and indirect costs such as damage to a company's brand can be immeasurable. A firewall is no longer enough to protect an organization's information assets. As security integrators, we must help our customers deploy a logical security plan that protects sensitive data and the infrastructure on which it resides.

Work Toward Convergence

Physical and logical security shouldn't be mutually exclusive. Bringing both functions under a single umbrella can foster better synchronization and collaboration. End users can derive a multitude of benefits – lower staffing costs, reduced duplication of efforts, streamlined operating procedures and fewer turf battles, to name a few – by partnering with a security integrator that can help them achieve convergence.

Remember, It's About More Than Money

In the current business environment, it can be a challenge to keep end users focused on their security needs. Investments in security – of both human and financial resources – can seem too costly during a time when some businesses are struggling to survive.

Organizations must continue to protect assets and prevent loss, even amidst the most challenging of business environments. Effective security programs can prevent the loss of monetary, physical and digital assets. But that's only part of the equation. For companies to thrive, they must remain diligent in preventing the loss of one other important asset – consumer trust.

Without trust, organizations risk alienating their customers. Without trust, millions and millions of dollars invested in new technology will have been wasted. Without trust, organizations can lose customers, employees and their reputations. By helping end users maintain their focus on and investment in security, integrators can play a vital role in the preservation of vital business assets, especially the asset of consumer trust.

The criminal community is becoming more sophisticated. And consumers are becoming keenly aware of security threats. As security integrators, let's make 2010 a year in which we become invaluable partners in creating programs that help our customers detect and deter crime, protect consumers and employees and maintain the all-important foundation of trust.



Diebold, Incorporated
 Post Office Box 3077, Dept. 9-B-16, North Canton, Ohio 44720-8077
 800.999.3600 USA | 888.545.9444 Canada | 330.490.4000 International
 productinfo@diebold.com | www.diebold.com

Diebold is a registered trademark of Diebold, Incorporated. Copyright Diebold, Incorporated, 2010. All rights reserved. Lithos in USA. File No. 70-1479.