

10 WAYS TO FOSTER A CULTURE OF SECURITY



As vice president and chief security officer for Diebold, Incorporated, Scott Angelo is responsible for the design, implementation and operations of all areas of Diebold's internal information security program. He also serves as the chairman of Diebold's Risk Council, which is responsible for global risk management infrastructure, monitoring and reporting across the enterprise. A former military intelligence officer, Angelo is a certified information systems security professional (CISSP) and a certified information security manager (CISM) and is a member of the FBI Cyber Executive Advisory Committee and the Chief Security Officer (CSO) Roundtable.

Scott Angelo
VICE PRESIDENT & CHIEF SECURITY OFFICER
Diebold, Incorporated

In the age of advanced security technologies, it's easy for security practitioners to become fixated on the latest shiny objects. And although technology enables us to enhance security like never before, the human element, which helps drive a security culture within an organization, is the most critical component to the success of a security program.

Following is an overview of the 10 ways Diebold believes security practitioners can foster a culture of security within their organizations. Such a culture must be deeply ingrained in the organization and valued by leadership, managers and line staff alike.

Establish Relationships

Many security practitioners mistakenly limit their exposure within their organizations to the security department. But security can and should be a role that transcends departmental boundaries. The only way to create a culture of security is to leave the confines of the security department and become part of the fabric of the organization.

Be a Good Listener

Security has traditionally been a role of telling. Telling organizational leadership about vulnerabilities and threats. Telling employees about policies and procedures. Telling law enforcement when an event has occurred. But in today's business environment, security practitioners must be just as good at listening as they are at telling. Balancing telling with listening helps establish trust in the security function across the enterprise. And it provides insight that can be invaluable in identifying and understanding emerging threats.

Learn to Operate in the Gray Area

When it comes to policies, regulations and compliance, the security function is often black or white. But where security can add real value is in the gray area – the place where protocols aren't as clear and decisions aren't as easy. To

operate in this gray area, security practitioners must have a deep understanding of the business. Reaching this level of competency within the enterprise elevates the security function from an operational role to one of leadership. And it more deeply ingrains security into the organizational culture.

Establish Consistent Policies, Procedures and Practices

Security cannot become a part of an organization's culture if its employees are not involved and invested in it. Security policies, procedures and practices set expectations for the role security should play within the organization. And they also enable employees to understand their stake in keeping the organization secure.

Create Awareness

Security is a team effort, but an individual responsibility. That's why employees should have access to security education. Training programs can help ensure the understanding of the policies, procedures and practices that drive the security agenda, and they can also instill a culture of security that reaches far beyond the security team. A culture in which all employees are security aware and committed to protecting the organization's assets will not only elevate the visibility of the security program, it will help contribute to its success.

Embrace the 80/20 Rule

Despite the vast options in today's security technology, the basic mathematics of security remain the same: At its core, effective security is 80 percent people and process and 20 percent technology. Many security practitioners focus the majority of their resources – be they time, money or people – on technology. This approach overlooks the importance of the human element in securing an enterprise.

Help Your Employees Understand Their Security Role

Like anything else, once employees get involved and understand their role in security, they're more likely to have a vested interest. Tools such as security assessments and performance evaluations can be used to measure their engagement, verifying their compliance with policies, procedures and practices.

Take Security Beyond Compliance

In today's increasingly regulated business environment, many organizations believe compliance is equal to security. But just because an organization is compliant doesn't mean it's secure. In fact, many of the regulations and guidelines with which companies strive to comply represent only the most basic of security needs. That's why a security program must be built around an organization's broad needs, risks and vulnerabilities, and not around the regulation du jour.

Manage Risks and Vulnerabilities

An enterprise that maintains a culture of security can more effectively manage risks and vulnerabilities. This management requires a deep understanding of the business, as well as the capacity to prioritize the organization's security needs.

Comprehending an organization's vulnerabilities requires synthesis and analysis of information from across the enterprise. It entails evaluation of organizational factors, as well as specific assets. Once vulnerabilities are identified, security leaders must assign risk. If an organization has a vulnerability, but there isn't much threat the vulnerability will be exploited, the risk is low. Not every asset can be secured at the same level; a low-risk asset cannot and should not garner the same attention as those that are at great risk. An effective security leader who has created a culture of security will have the trust and relationships needed to build confidence in and support of a security plan that includes ongoing assessment of risks and vulnerabilities.

Find Ways to Say "Yes." The security role often comes with power. And many security professionals choose to exercise that power to serve as a roadblock or barrier to getting things done within an organization. That's no way to foster a culture of security.

Saying, "No," is easy. But it doesn't add much value to the organization. Instead of looking for reasons requests won't pass the security test, security practitioners should find ways to say, "Yes," to the challenges their organizations are facing. The role of the security leader can and should be to enable the enterprise to do what it needs or wants to do in a safe, secure environment that does not leave the company vulnerable.

Technology can help organizations detect and respond to threats. But an organization with a strong security culture can also effectively mitigate risk, minimize vulnerabilities and proactively create a more secure environment – from the inside out. By investing in activities such as listening, relationship building, training and more, security practitioners can expand their influence within their organizations and transcend the traditional boundaries of the security department.

Total Solutions

Hardware
Software
Installation
Service

Diebold, Incorporated
P.O. 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.
Litho in USA. File No. 70-1481

