@ISACA
RELEVANT, TIMELY NEWS
Volume 10, 9 May 2012

Five Ways to Create a Risk-conscious and Security-aware Culture

By John P. Pironti, CISA, CISM, CGEIT, CISSP, CRISC, ISSAP, ISSMP

Adversaries and the threats they pose to information are more advanced and daunting than ever and show no sign of becoming less concerning in the future. Creating a risk-conscious and security-aware culture within an enterprise can provide more protection for an enterprise's information infrastructure and associated data assets than any technology or information-security-related control that currently exists. This kind of capability can be a game-changing force multiplier if leveraged effectively.

Here are five things that you can do to help create this kind of culture in your enterprise:

1. **Use risk management to remove the fear of security**—Consider the psychology associated with the words "security" and "risk." When a businessperson thinks of the word "security," the first thoughts that come to mind are often prevention, disablement and disempowerment. This is a fundamental result of experiences that he/she has often had when interacting with security, and it negatively drives his/her perception of the functions and capabilities security provides. When that same individual hears the word "risk," what typically comes to mind is understanding, management, control and empowerment. Therefore, alignment with risk at the onset often leads to greater acceptance than does security—in both terminology and approach.
2. **Work with business leaders and stakeholders to develop a business and information risk profile**—It is important to implement tools that enable business leaders and stakeholders to understand their risk appetite and their risk management requirements, as well as the parameters needed to align and manage their business activities in relation to risk. A key tool that can be used to create a risk-conscious and security-aware culture is the business and information risk profile. This profile establishes the bounds of acceptable loss, compromise, disruption or disablement of key and material business functions, individuals, activities, information and processes for an enterprise. An enterprise's business and information risk profile also provides a framework and limits for the information risk management and security team to align their own activities to ensure that business expectations are met.

3. **Follow an embrace-and-educate approach**—The adoption and use of an embrace-and-educate approach to new ideas, concepts, technologies and solutions can help change the mind-set and culture; it involves positive feelings of the information risk management and security elements of an enterprise. In this model, the risk management and security elements of enterprises recognize and acknowledge the immediate value of the capabilities the business intends to use. At the same time, this model provides education to the user population regarding the identified risk and expectations of use to ensure that appropriate levels of security exist to align with the enterprise's risk profile. The key to success with this method is to use education and awareness techniques that can be easily understood and internalized by the intended audience. This often means the use of simple and easily understood terms, case studies, and examples that are readily identified as being applicable to the enterprise's business activities.
4. **Provide personal benefits**—If individuals can derive personal benefit and value from the knowledge, insights and guidance provided to them about risk and security there is a high likelihood they will change their behaviors in both their personal and professional lives to be more risk conscious and security aware. An example of this can be a change in behavior regarding the use of social networking solutions. These capabilities are often used by individuals for personal activities, but increasingly have business benefits as well. If you can effectively educate users on the risk associated with these solutions, as well as on safe and effective ways to continue to use them, they will most likely appreciate and be more open to your insights and ideas in the future. They will also most likely begin to adopt the safer use techniques in all environments, without even realizing they are doing so.
5. **Employ effective reinforcement methods**—Changing the mind-set and culture of an enterprise requires the use of effective and consistent reinforcement of the desired state. In doing so. it is important to identify the learning style, values and interests of the intended audience. The use of various methods and techniques to deliver messaging is essential to reach a diverse audience. This messaging can include in-person training and seminars, computer-based training and messaging (i.e., screen savers), visually stimulating and thought-provoking strategically placed signage, and positive messaging that demonstrates how the adoption of this new mind-set can promote success and benefit the enterprise as well as the individual.

This tips column draws from a volume 2, 2012, *ISACA Journal* article on the same topic. Learn more about this subject or other tips by reading "**Changing the Mind-set: Creating a Risk-conscious and Security-aware Culture**."

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC.