SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Make Awareness Programs Count

Eric Cowperthwaite

Originally Published in SecuritySolutions.com

August 2007

MAKE AWARENESS PROGRAMS COUNT

A security training and awareness program should be more than a mark on the regulatory compliance checklist or a way to satisfy the auditors. It is, fundamentally, an ethical obligation of the company leadership, part of the commitment between employees and the company.

We hold employees responsible to adhere to policies and standards and other governance controls, and we apply sanctions when an employee fails to meet those obligations. That creates a dilemma if we are not investing in a true training and awareness program.

When an employee breaks a rule and claims to have done so unintentionally, it is easy to argue that it is his or her responsibility to know what the policies are. But since employees may be put on “performance plans” or even lose their jobs because of unintentional policy violations, and since the damage to the company is the same regardless of the employee's intent, let's not be so quick to dismiss the issue.

Over the years I've been involved with a number of cases in which post-incident claims of inadequate training or awareness programs compounded problems for the company, the employee or both. There was the employee who had postponed the installation of mandatory encryption on an assigned laptop three times. Consequently, when that laptop - holding the confidential data of 22,000 people - was stolen from the trunk of the employee's car, it was unencrypted, and it was also unattended. These were two violations of formal, explicit policies, and yet, although the cost of the loss was more than 1,000 times the cost of the laptop itself, the employee was only counseled. Why? Because the employee had not had appropriate training and was not aware of the policy requirements or the need to apply specific controls to the laptop and the data it contained.

Another case: An employee was using a company-owned computer to download and view pornographic videos from the Internet. The employee was fired. When the employee challenged the termination in court, the court found that the organization had not adequately trained the employee.

It is our ethical responsibility to provide good training and awareness programs rather than "check the box" programs — the kind that actually help our employees to do the right thing, for the protection of both our organization and our employees. Such a program will also reduce the risk to our customers, employees, data and assets. Doing the right thing is good business.

Eric Cowperthwaite *is the chief security officer of Providence Health & Services, which has 29 hospitals and more than 50,000 employees located in five Western states. He is a member of the Security Executive Council www.securityexecutivecouncil.com.*

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com