SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Compliance Scorecard – Is Your Security Awareness Program All It Can Be?

Kathleen Kotwica

Originally Published in Security InfoWatch

October 2008

Compliance Scorecard – Is Your Security Awareness Program All It Can Be?

Your organization may have to (or, in the case of standards, feel compelled to) comply with any number of regulations, such as HIPAA, C-TPAT, PCI, NERC Cyber Assets, Title 18 (sentencing guidelines) or ISO 17799. What do all these regulations have in common? Security awareness and training program requirements. If you feel your department is adequately addressing these requirements by conducting a few training sessions a year, slapping up some posters or sending out some e-mails, you may run the risk of security awareness failures.

To test the basic robustness of your security awareness and training program, ask yourself if it appropriately addresses each of the following questions.

What: *What risks impact your organization?* **Countermeasures:** What measures are in place to mitigate the most potentially damaging risks, as defined by you and senior management?

Who *needs to be made aware of your organizational risks, and to what degree?* **Roles and responsibilities:** Security is everyone's responsibility; as the expert, you can assist others in defining their roles. You may need to provide varying levels of advice or training to different groups of employees based on their functions and titles.

When: *How often do you engage people in awareness activities?*

How: *How do you satisfy awareness and training requirements?* **Delivery:** You may deliver your awareness

and training messages in a number of ways, including e-mail reminders, posters, meetings, exercises/drills, newsletters, and intranet resources. The frequency and intensity of training may depend on your risks (What) and the responsibilities of individual employees (Who).

After you have developed your program around these questions, how do you know it is working? You need to develop your measures and metrics program to include awareness program effectiveness. Do not forget to tie your work into the areas of risk to which the board responds, so they can identify with your efforts.

Kathleen Kotwica is SVP and Chief Knowledge Strategist for the Security Executive Council. Prior to joining the council, she held a wide range of leadership positions including information architecture consultant at a New England consulting firm, director of online research at CIO *and* CSO *magazines, and research associate at Children's Hospital in Boston.*

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