SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Seven Steps to Information Security Compliance

Lou Magnotti

Originally Published in Security InfoWatch

October 2008

Seven Steps to Information Security Compliance

Cyber communications technology is continually advancing. E-mail is already the most used form of communication, and the use of radio frequencies and satellite relays will soon facilitate wireless communication from anywhere on the planet. The affordability of computers coupled with the world's level of information dependency creates a critical problem for the security and privacy of data. Many organizations need to comply with a myriad of standards and rules such as FISMA, HIPAA, SOX, ISO 17799, and GLBA, to name a few.

Information security policies and standards can provide an organization with an accurate security baseline and the tools to strengthen its security posture. To achieve compliance, any organization must master the “Big Four”—perimeter defenses, system certifications, auditing, and user involvement. Without the implementation of these four safeguards, costs associated with non-compliance will eventually usurp security efforts. Surveys have already revealed that businesses prefer speed and capacity over the security and privacy of data. The security “sell” will continue to be an uphill battle.

There are seven steps chief information security officers can take to launch their organizations in the direction of InfoSec compliance, regardless of their available resources.

- Identify current or potential vulnerabilities. The acknowledgement of auditing agency findings and the CISO's own observations and records may be good resources.
- Apply objective values to issues requiring attention. Usually objective measurements coincide with cost.
- Establish a priority list. The philosophy that “ Rome was not built in a day” may apply here. The cost of security hardware and software is ever-increasing, and the demands on most budgets are great—so choose carefully.

- Start complying. Any progress is progress! Without taking that first step, success can never be realized. Just get in the game.
- Create a comprehensive security, education and awareness program. This is the first line of defense for information assurance in business, government and military enterprises. Users are often eager to assist and comply when they know the rationale behind such efforts. Make them well aware of the threat. While CISOs may desire to keep successful or attempted attacks confidential, it may be important to share such information with users. Theoretical security incidents or scenarios do not have the same impact as real facts. That said, users must not be allowed to independently or unilaterally decide whether to adopt necessary safeguards. Without mandated compliance to InfoSec policies, the system is no stronger its weakest user.
- Market success. Sell your security and compliance program to upper management by illustrating real dollar savings. Everyone loves a winner! Success will be rewarded with dollars to further enhance compliance.
- Always seek to increase budgets. Never miss an opportunity to ask for a budget increase to better safeguard information and enhance the company's bottom line.

Lou Magnotti is the Chief Information Security Officer for the U.S. House of Representatives. Mr. Magnotti is a recognized security professional with more than 26 years of government and industry experience. He provides information assurance counsel to multiple federal agencies, is a member of the (ISC)? Government Advisory Board for Cyber Security and a Security Executive Council Tier 1 Stakeholder.

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