

“The Changing Role of the Bank’s Security Officer.”

By Paul Reymann

With the changing scenario of banking due to infusion of information technology, what would be the role of Bank’s Security Officer and challenges ahead?

You are correct; the scenario of banking is significantly affected by increased dependency and use of technology. The power of the Internet and new technology changes our traditional understanding of strategic planning and risk. Technology has moved from the backroom to the boardroom. It is no longer a back-office operation that can be viewed as a single cost center or line item on the budget, and it is no longer an area that falls solely on the shoulders of information technology personnel. Financial modernization, the Internet, and new technology are changing the landscape. Banking has entered a new paradigm.

This is why the regulators debated whether to require a bank to appoint information security officer, as they drafted the GLBA Data Protection Provisions. As you know, the existing physical security regulations require the appointment of a Security Officer. Therefore, I assume you are referring to the Bank’s Security Officer that is charged with establishing, maintaining and reporting on the “physical” security program of the bank. The new “information” security regulation, however, provides you flexibility in addressing this management responsibility. Therefore, although your Security Officer might take on these new responsibilities, there are other options. Generally, I see four options for how to fill this new role:

- 1.) Increase the role of the existing Security Officer to include the information security responsibilities called out in the new regulation. If your Security Officer has a technology & information security background and can wear this additional hat – great. However, you may find that this individual is great at physical security matters, but not the best resource for technology and information security challenges.
- 2.) Hire an individual that has the necessary blended background in technology and information security along with the business acumen to also understand the business implications of this responsibility. For example, a real challenge is to bridge the communication gap between Sr. Management and the technology issues. As the influence of technology changes your institution’s risk profile, guess who understands the new risk best? The techies! You need someone who understands your technology and information security risk and can clearly articulate such risks to management and the Board. They need to be able to convert the techi-talk to plain language and help others to understand its impact on the business.
- 3.) Form a committee that includes key participation from several business units (compliance, technology, legal, operations, physical security officer, etc.). Since technology and information security is blended and woven through your organization, this frequently presents a viable alternative and helps everyone to understand its impact on the organization.
- 4.) Outsource this role to a high-caliber professional knowledge expert. Hiring a full-time staff position to accomplish the tasks described in option 2 can be capital intensive. Outsourcing can provide you the same resource but at a significant savings. This frequently works best in conjunction with the internal committee structure described in option 3.

Whichever option works best for your institution, you need to ensure that this new role has a direct line of reporting to the Board or its delegated executive committee.

I hope you find these points helpful.