Filling the Information Security Officer Role within Community Banks

By, ***John J. DeMauro***, President, Practical Security Solutions, LLC and
Thomas W. Grottke, President, NEBSG, LLC

Banking has been significantly impacted by technology. Maybe more than any other business, but that may be an insular view. Technologies that came to the industry during the 1960s through most of the 90s emphasized and impacted operations and financial systems. Technologies impacting banking today and for the past decade have transitioned to those that connect a financial institution's operations with customers or other third-parties. In other words, such technologies have had an outside orientation.

This absolutely revolutionary orientation has increased dependency on technology and also reliance on technology for operating procedures that we used to rely on heavily to be performed by our human resources.

These new technology changes coupled with the ever increasing power and use of the Internet has changed the nature of major aspects of the business of banking. Most of us believe we are only at the tipping point in this transformation and some of our clients are preparing for nearly complete transformation to this automated business model. Technology, once relegated to the backroom is now a focus of the boardroom as evidenced by comments from some of our CEO and their directors, "…people don't want to come into the branch anymore…", "...the next generation won't even know what a bank is.." or "there are not enough deposits available here (in our branch markets) and we can't afford to open new branches so we must use the Internet to gather deposits…".

This growth and expected continued growth of technology based products, services and front and back-office automation may be why regulators stopped just short of requiring that banks appoint an Information Security Officer (ISO) as they drafted the GLBA data protection provisions back in 2001 and 2002. But, by 2003, the FFIEC issued guidance that states: "Senior management should designate one or more individuals as information security officers."[1]. For some time, we have seen regulatory examinations strongly recommend to their banks that are in excess of $1 billion in assets that they established the ISO position and see regular comments where it has been established on the quality and structure of the position. With increasing regularity we are seeing similar regulatory commentary at smaller banks.

This is a costly and, we have witnessed firsthand with a number of banks, politically charged position that the regulatory agencies are requiring all banks to address. Now certainly it is not a full-time job, in our experience, not even at a bank with an in-house core data processing system with over $2 billion in assets.

1 http://www.ffiec.gov/ffiecinfobase/booklets/information_security/01_security_process.htm

Before options are discussed it is important to consider the responsibilities that make up the ISO role. First and foremost the ISO should be responsible and accountable for the administration of the information security program. At a minimum, they should directly manage or oversee the information technology (IT) risk assessment process, development of IT security policies, standards, and procedures, testing, and the information security reporting processes.

To ensure appropriate segregation of duties, the information security officer should report directly to the board or to a senior officer with sufficient independence to perform their assigned tasks. It is not uncommon or completely out of the question for the position to report to the CIO. However, such a circumstance can raise questions with regards to adequate levels of independence. Typically, security officers should be risk managers and not a resource assigned operational responsibilities within the information technology (IT) department. They should have sufficient knowledge, background, and training, as well as a level of authority that enables them to adequately and effectively perform their assigned tasks.

With these points in mind the following options are worthy of your consideration:

1. Hire an individual that has the necessary blended background in technology, information security, banking and risk management. This person should also have the capability to understand the business implications of this responsibility. You need someone who understands technology and information security risks and can clearly articulate such risks to management and the Board. They need to be able to convert complicated technical issues into plain language and help others to understand its potential impact on the business.

The main potential issue with this option is that these resources are in short supply and typically command salaries that will likely burden most financial institutions. ‘

2. Assign the responsibility to an existing bank employee. It is important that this person have many of the skills described above and that they are given sufficient time outside their normal set of responsibilities to effectively carry the additional ISO responsibilities.

The main potential issue here is that the likelihood that a person with such skills exists within most banks is remote. If such a resource does exist they probably work in the IT Department and therefore lack the independence necessary to act as ISO. It is very likely that a resource selected from the existing ranks would result in compromised effectives of the position.

3. Outsource this role to a qualified professional. Hiring a full-time staff position as described in option 1 can be capital intensive. Outsourcing can provide you the same type of resource but at a significant cost savings. This option may be the most cost effective for many small to midsize community banks.

The main potential issue with this option is vendor management, scope of services and ability to understand banking.

In all three scenarios, cost and skill are key issues. Clearly option 2 is the lowest cost, as the bank is basically taking on opportunity cost assuming they do not add an FTE to the person's unit who is acting as the ISO. Out-sourcing certainly will add hard dollar expense, but outside of cost there are other benefits related to this option. One is that the outside entity is completely independent of IT operations. Another is that an outsourced ISO role can be made to be flexible and may be tailored to meet specific business requirements of your organization. In addition, using an out-side ISO can reduce the annual IT audit costs.

Other issues to keep in mind when considering outsourcing the ISO role:

- Outsourced professionals should have deep technical, IT security and banking industry experience.

- Consider the importance of IT security certifications such as CISM (Certified Information Security Manager), CISSP (Certified Information Systems Security Professional) or CISA (Certified Information Systems Auditor).

- Outsourced service options should be consistent with FFIEC guidance.

Banks should consider their options in filling this increasingly critical role whether they are being forced to by examiners or auditors. 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.

January 2, 2008

John DeMauro can be reached at 508-614-0719, or at JDemauro@.practicalsecuritysolutions.com and Tom Grottke can be reached at 860-798-7107 or tgrottke@nebsg.com