

## Outrunning the Regulators

by Joni Bessler, Debra Banning, and Roman Regelman

02/05/07

a strategy+business exclusive

# Outrunning the Regulators

Staying ahead of security rules can create competitive advantages.

by Joni Bessler, Debra Banning, and Roman Regelman

**T**he password to your bank account is about to be invalidated,” reads the e-mail. “To prevent this, please click on the following link and enter all your security information.”

The hapless individual who follows instructions, of course, risks giving away access to one or more bank accounts to cyberthieves. And as such devious practices become more sophisticated, regulators tend to get nervous. In fact, that anxiety has led the Federal Financial Institutions Examination Council (FFIEC) to add another layer of rules to those governing the banking industry, already among the most regulated business sectors in the United States. Under the new requirements drafted by the FFIEC, which was created in 1979 to establish uniform principles in federal bodies’ oversight of the industry, financial institutions must put more stringent controls on their electronic security by the end of 2006. Specifically, they must examine the ways in which they communicate electronically with customers, whether those interactions are on Web sites or interactive phone systems; they must determine what security threats exist on those systems, establish a process for assessing future risk, and formally educate their customers about security risks.

Banks don’t have much more time to meet the FFIEC’s demands and, unfortunately, many will make

the minimum effort necessary to comply with the requirements, sigh in relief, and consider the task finished — thus leaving themselves unprepared for the FFIEC’s next set of guidelines.

This attitude does not just open the door to future noncompliance. It sets in place a debilitating cycle of increasing vulnerability. Given the constantly evolving state of security in financial services, banks that take a desultory approach to security are positioning themselves as the weakest members of the herd, and thus the most vulnerable to sophisticated “phishing” and “pharming” schemes, in which attackers gain access to customers’ accounts and personal data through e-mail fraud or Web traffic redirection. The FBI estimates that every incident of a Trojan virus attack costs banks at least \$38,000 in revenue loss and employee hours — and that figure doesn’t take into account the harm to a company’s reputation and loss of customer confidence, which can be more damaging than the actual attack.

Companies in heavily regulated industries, a group that includes pharmaceuticals, health care, and utilities, often act as though the regulations that besiege them are irritating trivialities. However, new requirements can offer companies an opportunity to escape the cycle. For instance, instead of maintaining an ad hoc approach to foiling invasions and complying with regulations, banks

**Joni Bessler**

(bessler\_joni@bah.com) is a vice president with Booz Allen Hamilton in San Francisco. She specializes in strategy and operational effectiveness for financial-services companies.

**Debra Banning**

(banning\_debra@bah.com) is a principal with Booz Allen Hamilton in McLean, Va. She specializes in information assurance with a focus on IT security compliance, information-related risk management, and security program development.

**Roman Regelman**

(regelman\_roman@bah.com) is a principal with Booz Allen Hamilton in New York. He specializes in growth, strategic operations, and technology for financial-services companies.

should craft an overall public-facing security strategy. Although it can be difficult to persuade senior management to invest in long-range plans, there's no better time to do it than when they are in the shadow of an imminent regulatory deadline — especially one that is disrupting the entire organization as the company marshals its resources to deal with it.

For example, in aiming to go beyond regulatory compliance and achieve security excellence, banks can institute a mechanism for self-analysis and self-improvement that allows them to anticipate their future security needs. In doing so, they will meet their current burden of compliance, lessen the impact of any future regulatory guidance, reduce their risk exposure, and address customers' concerns about the security of online banking.

Instituting such a robust risk-mitigation program involves three elements. The first is to determine the most appropriate technical solution, which can be the biggest hurdle for many companies: They may not know how many Web sites they operate, security across the systems may be inconsistent, and key applications and services may reside on poorly secured systems. Therefore, banks, for example, should assess their current level of risk exposure and determine risk-mitigation strategies that will balance compliance, business objectives, and customer satisfaction. In implementing technical solutions, banks must avoid overly complex approaches, which may have higher-than-expected direct and indirect costs.

The second element is an effective organizational structure to manage the initiative. A common roadblock to implementing new security standards is a decentralized company, which can lead to inconsistent approach-

es to IT security across the enterprise, along with incomplete monitoring and accountability. However, piecemeal fixes will not work. Grafting a centralized security program onto a decentralized organization often results in the corporate equivalent of organ rejection.

How might banks address this issue? They can create a hybrid centralized-decentralized model, in which critical compliance activities and governance oversight are centrally managed, while less critical functions remain with the business units. Alternatively, banks can construct enforcement mechanisms that shift the burden of compliance to the heads of the business units, rather than keep it centralized at corporate headquarters. Regardless of the specific solution, banks can manage risk exposure and regulatory compliance in a uniform fashion only if they have the requisite organizational structures in place.

The final element of a robust risk-mitigation program, customer awareness, can be a key component of a company's defense against fraud and identity theft. A well-educated bank customer can more easily spot phony come-ons, like phishing e-mails, and avoid being deceived. In fact, many banks are finding that educated consumers are their front line of defense in reporting phishing and other fraud attempts. One basic but effective measure is to advise customers to always type the bank's Web address into their Internet browser rather than click on a link in an e-mail, because the e-mail may be fraudulent.

Furthermore, making customers aware of enhanced online security is a key differentiator in the marketplace. In a 2005 survey by Deutsche Bank Research, "security offering" was far and away the most important feature to prospective online banking customers, with 87 percent

calling it their top priority. A well-publicized security program could prove a significant lure to new customers in the highly competitive banking environment.

Any highly regulated industry will face similar vicious cycles of its own and should be thinking about approaches for leaping ahead of regulatory requirements. The common thread is that simply responding to regulatory guidance will never be enough. Anticipatory thinking is the only way to avoid being caught in the middle of an endless series of provocation and regulation. +

strategy+business magazine  
is published by Booz Allen Hamilton.  
To subscribe, visit [www.strategy-business.com](http://www.strategy-business.com)  
or call 1-877-829-9108