



# Off the Press - October 2009

PENNSYLVANIA ASSOCIATION OF COMMUNITY BANKERS

THE VOICE FOR COMMUNITY BANKING IN PENNSYLVANIA SINCE 1876

## Security Risks to Smaller Financial Institutions

By Justin McIntyre, S.R. Snodgrass, A.C.

Some executives in the financial industry think that their risks are lower because they are located in a small town or have a small asset base or simply because they've avoided problems thus far. Because they think they are low risk, some community banks and other small financial institutions are reluctant to implement or enhance security controls because doing so could increase costs or slightly inconvenience their users.

Unfortunately, "small" doesn't mean low risk—in fact, it may mean the opposite. We have seen an increase in malicious activity in the past few years aimed specifically at community banks and other small financial institutions that thieves believe do not have the defenses of larger firms.

As an example, a Pennsylvania-based community financial institution in a metropolitan suburb has been dealing with hackers and phishing, as is the rest of the banking industry. Over the past few years, company employees have received numerous alerts from customers concerning phishing e-mails. The IT staff has not only become expert at deactivating fraudulent websites, they also search the Internet regularly for imposter websites designed to steal their customers' personal information.

Additionally, in the past year, the institution has noted an increase in customer complaints relating to unsolicited phone calls asking for personal information. The criminals have begun using an "automated voice dialer" system to call a massive number of phone numbers using a recorded message. The message says that personal information has been compromised and leaves a phone number for the unsuspecting customer to call. If the customer calls the number, he or she is asked to "confirm"—and thus give away—personal information. This type of attack appears to be having limited success, since some customers do not realize that even by speaking with someone who appears legitimate, their personal

information is being stolen. This technique of using "voice" to gather non-public personal information is now called "vishing."

This financial institution is not well-known beyond its customer and community base, but it would seem that numerous individuals are intent on doing it harm. This institution has learned that security controls, proactive monitoring, and customer education are all critical.

### SMALL DOESN'T MEAN LOW RISK

Just because an institution is off the national radar does not mean it will escape the attention of thieves, fraudsters, and other online criminals. To take one example, a small Ohio-based community bank with only one branch employed a local third party to host its website and Internet banking login page. As is customary, customer usernames and passwords were securely sent via 128-bit encryption to the outsourced provider for processing. However, a hacker gained entry to the third party's website source code and redirected customers to a fraudulent website first. This website asked customers to verify sensitive information, which could then be used to steal the customer's identity.

The bank was made aware of the problem only when a customer called to ask about the "new" website. Once alerted, the bank was able to terminate the connection to the fake website. But it was not able to determine which customers had entered personal information—login information was not captured because of the redirect.

Thus, the bank was forced to alert all customers to reset Internet banking passwords. The bank also needed to contact each customer to find out who had logged into Internet banking during the course of the fraudulent redirect. Luckily for this bank, with only several thousand accounts and only a small portion using Internet banking, the situation was manageable. But the "fix" was cumbersome and the bank's reputa-



# Off the Press - October 2009

PENNSYLVANIA ASSOCIATION OF COMMUNITY BANKERS

THE VOICE FOR COMMUNITY BANKING IN PENNSYLVANIA SINCE 1876

tion suffered. This community bank had to learn the hard way that being small does not make an institution immune to a hacker with malicious intent.

## LARGE LOSSES FOR A SMALL BANK

Another community bank suffered a large monetary loss and harm to its operations from an online incident again caused by malicious individuals. A large business account chose not to enable dual controls that prohibit one user from having the ability to transfer money outside the institution. When one user's home computer became infected with malware, the username and password were captured, and money was successfully transferred via the ACH system to other financial institutions where it was promptly withdrawn.

Because the infection wasn't discovered right away, and because these transfers were considered "good funds" at the receiving institutions, the bank has not been able to recover the lost money. Again, this is a community bank not known outside its several-county radius that was the victim of an efficient, well-run malware scam that may end up costing them and their insurer several hundred thousand dollars.

Online infections have become increasingly destructive, complicated, and harder to detect and prevent. Moreover, smaller community banks and credit unions are now becoming targets of criminals, with increasing frequency. In fact, criminals appear to view smaller financial institutions as more vulnerable than their larger, more well-staffed counterparts.

All financial institutions, large or small, should actively look for ways to evaluate threats and risks to their organization. Independent third parties can help and implement appropriate controls to prevent them

from suffering bad publicity and needless losses, but customer and internal employee education is essential for preventing and detecting fraud. Both of these parties need to be constantly vigilant when conducting transactions and using electronic systems. Internal review of usage and other security-related logs for mission-critical systems is essential. Additionally, general IT Audits, specialized IT audits, Risk Assessment testing, and Attack and Penetration testing can help detect areas of vulnerability and areas where enhanced controls are necessary.

However, no control is perfect, and technology advances are proving that systems once thought to be bulletproof can be compromised. Without a thorough risk assessment, no threat to an organization should be classified as "low risk" because of overall small asset size, small community size, or lack of national attention. The Internet has shrunk and continues to shrink our world, and, with the click of a mouse, a community financial institution can be a target from hundreds and thousands of miles away.

*Justin McIntyre, CISA is a Supervisor, Senior Technology Services Consultant at S.R. Snodgrass, A.C. His technology audits cover a wide-range of audits, including general Information Technology, Information Security, Gramm-Leach-Bliley Act-related, SAS 70 technology control testing, and SOX-related. Snodgrass is best known for our expertise in the financial services industry, where we currently serve over 175 financial institutions on a national scale. Accordingly, we have extensive industry business experience and sound working relationships with all of the regulatory agencies. Examples of that experience are displayed on our website's Knowledge Bank at [www.srsnodgrass.com](http://www.srsnodgrass.com), where you can view several articles and video presentations on banking-related topics, including a live Attack and Penetration demo.*