Risk Management and Internet Banking: What Every Banker Needs to Know

By Barbara Stafford

ACB's risk management alliance partner, the St. Paul Company, is just as interested in current developments in information security as community bankers are. At ACB's annual Directors' Conference in Seattle, St. Paul offered a timely presentation on this topic.

Internet banking is one of today's hottest topics among bankers, and it's being driven by growing consumer demand, peer pressure and pressure to improve profits.

With regard to consumer demand, there are an estimated 72.4 million computers connected to the Internet. About 37 million U.S. households have Internet access. Of the approximately 93 million U.S. households with a banking relationship, approximately 9 million households use online banking, with significant growth expected in the next few years.

Peer pressure is evident in the increase in the number of banking Web sites, which more than doubled from 1,500 in 1997 to 3,500 in 1999. Approximately 1,100 of these sites are transactional. Banks that are offering Internet banking have experienced more than a doubling of the number of customers using Internet banking from mid-1998 through the end of 1999.

Profitability pressures are real, too, and a recent OCC study concluded that institutions with Internet banking outperformed non-Internet banks in terms of profitability. The exception to this involved small de novo banks where the non-Internet de novos outperformed those de novos with Internet capabilities. There is also some truth that greater reliance on Internet banking may allow banks to reduce expenditures on "bricks and mortar," thereby generating lower expenses.

The banking industry has been at the forefront of change fueled by technology. It wasn't that long ago that we first experienced the convenience of drive-up teller windows, or first used an ATM, or signed up for electronic deposit of our paychecks. Certainly many banking customers have enjoyed the convenience of supermarket banking, and many have enjoyed the convenience of phone banking and the more extensive home banking.

Internet banking is a very natural "next" step for the banking industry to take along the e-commerce path, and banks that are thinking and acting on today's reality will survive and prosper tomorrow.

When thinking about the growth and profitability goals of the organization, it is important to understand how the Internet may support these goals. Question whether the management team at your bank is more inclined to find safety in standing still or if they are a group that embraces change. Any organization today that stands still may not be a long-term survivor.

Make sure your Internet banking vision is both compelling and well understood throughout the organization. Also important is a well thought-out capital allocation plan that supports the development of your Internet banking initiative. Assess your bank's existing competencies to determine if they will enable or hinder your Internet banking initiative. You may have to build or hire talent with specific competencies in mind. And of course, this will be true across staffing, technology platforms and, most importantly, security.

Another important point is that vulnerabilities associated with the Internet are not well understood, and may not be given the same degree of high priority by outside vendors, developers or consumers. Security that has been appropriate for mainframe computers and small, well-defined networks inside an organization is not effective for the Internet, which was designed to be open and approachable, with control and trust resting with the users.

With the digital nature of the Internet, there are no physical or geographic locations or boundaries. This means that traditional or time-honored physical security is no longer relevant in an environment with no boundaries. The Internet calls for new knowledge and a new point of view in order to understand its workings and vulnerabilities. Remember, your customer's privacy, the safety of your bank's assets and your reputation is at stake.

The growth in electronic commerce and the momentous growth in Internet users have brought an alarming increase in the number of knowledgeable intruders or criminals who now, through the Internet,

have at their disposal a large number of targets of opportunity. Every Web site that exists is a target.

Computer intrusion and theft is a very serious problem yet many decision-makers are either unaware of or unconvinced of the level of risk. There is a fairly reasonable level of knowledge and awareness of such risks among technical people. The problem has been that these people have had difficulty communicating the degree of risk to the corporate decision-makers—those that make the investments in security. A decision-maker that is working to maximize profits and is unaware or unconvinced of the level of risk will not see the payoff from security expenditures.

Part of the problem is that people have been lulled into a false sense of security. Today's intrusions are kept very close to the vest—people are not talking about them and consequently not learning from them. According to several studies, privacy and security are the most important issues that consumers have. It's important to keep this in perspective and to secure the bank accordingly.

The following is intended to help increase the understanding of exposure to intrusion. The recently announced results of the fifth annual "Computer Crime and Security Survey" conducted by the Computer Security Institute indicate some disturbing trends among the 273 organizations surveyed:

- Ninety percent of the respondents detected computer security breaches within the last 12 months;
- Seventy percent reported a variety of serious computer security breaches including theft of proprietary information, financial fraud, system penetration from outsiders, denial of service attacks and sabotage of data or networks;
- Seventy-four percent acknowledged financial losses due to computer breaches;
- Forty-two percent were willing and/or able to quantify their financial losses. The losses from these 273 respondents totaled $265,589,940, up from the average annual total over the last three years of $120,240,180; and
- Fifty-nine percent cited their Internet connection as a frequent point of attack.

As another means of measuring the increase in computer intrusion, you only have to consider the number of security incidents reported to the CERT Coordination Center. CERT/CC is a part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University. In their first full year of operation back in 1989, the center responded to 132 computer security incidents. By 1999, its staff responded to more than 8,000 incidents, and these numbers are expected to grow.

The exposures connected to e-commerce and Internet banking are indisputable. On a daily basis, you face exposure to lost revenues, business interruption, theft of proprietary software or customer information, damage to your data or covered systems due to viruses, loss of performance or the ability to access your systems due to attacks, data or system integrity problems, denial of service liability losses and, most importantly, loss of reputation, all because of unauthorized access.

There is certainly risk associated with any new effort. How this risk is managed and controlled is important and this is largely a function of solid leadership, a vision and strategy, adequate funding, education and awareness, appropriate security, competent staff and careful scrutiny of outside resources.

Managing and controlling risk should also include risk transfer, and insurance is a useful risk transfer tool. Several markets are offering insurance protection of certain e-commerce exposures, either through separate e-commerce policies or by endorsing e-commerce coverage solutions to existing property and casualty coverages. Other coverages are also important, such as Directors and officers liability, a financial institution bond with respect to exposure to fraud from unauthorized employee intrusions and, certainly computer theft coverage for the hacker exposure. As part of your risk management plan, make a point of having your local agent or broker conduct a coverage review with an eye to e-commerce exposures.

An effective risk management plan should also include the engagement of an outside firm to conduct ongoing assessments and monitoring of your institution's system vulnerabilities through intrusion testing and intrusion detection. You'll want to use every tool available to foil any hacker's attempts. If you believe it's important to lock the safes and vaults, set all the alarms, and close and lock the premise doors at the end of each business day, wouldn't you also want to make sure that your systems are locked down too?

There is no question that computer intrusion and theft is a very serious problem today and the Internet plays a very significant role in this regard. The Internet calls for new knowledge and a new point of view in order to understand its workings and to protect against vulnerabilities. In maintaining customer confidence and privacy, the protection of bank assets, and the protection of your bank's reputation, there will be no substitute for solid awareness, careful planning and execution, and effective risk management.

Barbara J. Stafford is an assistant vice president at St. Paul Fire & Marine Insurance Company of St. Paul, Minn., an ACB Partners Inc. endorsed carrier since 1993. For more information, visit St. Paul at www.acbpartners.com*, or call 1-800-356-4098, ext. 0-7150.*