



## **BUSINESS INSIGHTS**

# **Managing Cyber Risk at Community Banks**

*The Board's Role in Internet Security*

In association with



# How Boards Can Mitigate Identity Theft Risk

Bank Director spoke to Tracey Vispoli, vice president, Worldwide Financial Fidelity Manager, Chubb Group of Insurance Companies, about trends in cyber risk and the steps boards of directors can take to make sure it understands the risks facing its organization and what the organization is doing to mitigate those risks.

## Has the frequency of identity theft/cyber risk increased in the last year or two?

One of the leading surveys on cyber risk is the Computer Crime and Security Survey, conducted for the last seven years by the Computer Security Institute (CSI) in conjunction with the FBI. The results of this survey show a definite trend is emerging among the organizations surveyed during this timeframe—90% have suffered a security breach. The survey results also show that the number of reported cases of identity theft, as well as the frequency of identity theft and the amount of financial loss resulting from that theft, is growing.

Probably the No. 1 reason community banks are exploring cyber risk products is because they are acutely aware of the trends and of the associated liability. Although consumers would have expected the confidential handling of their records, regardless of state or federal action, Congress has taken action in the form of The Gramm-Leach-Bliley Act, which affirms the responsibility of a financial institution to “respect the privacy of its customers and to protect the seriate and confidentiality of those customers to nonpublic information.”

More than half of the 2004 CSI/FBI survey respondents (56%) said they had been a victim of e-crime and further indicated their company had suffered an actual loss as a result. Nineteen percent of those respondents represent the financial services industry.

As many as one-third to one-half of companies don't track security breaches and related losses and there is a third category—companies that are measuring e-crime, but are afraid to tell the public. So reported numbers just seem to be the tip of the iceberg.

## What should a board do to make sure it understands the problem within its own organization? What questions need to be asked?

As basic corporate governance would dictate, the board first needs to recognize that there is a growing trend in electronic crime. Each institution has a responsibility to mitigate the risk on behalf of its constituents, including customers and shareholders.

One of the first things board members can do is ask if the organization hired a qualified outside party to conduct a third-party evaluation of its security practices. If not, board members need to know why. And, if so, the board should make itself familiar with the type of hazards that the evaluation has identified.

The board should establish a formal procedure requiring data security, internal audit, enterprise risk management, or another qualified respondent within the organization to provide a written response to the findings and explain how the company will comply with the recommendations. Also, the board should understand the makeup of the organization with respect to information technology. Does the organization heavily outsource

technology or does it handle most of it internally? If outsourced, how does the organization select a third-party vendor? What are the criteria? What insurance does the third-party vendor buy?

Regarding information technology, we see the need for a holistic approach to risk management. Technology has been in its own little silo for way too long. Management, mitigation, and identification of cyber risk has always been done by the IT department. We believe that it should not be isolated.

The board should also understand the organization's philosophy and culture to map cyber exposures and mitigate against them. It needs to ask about policies, procedures, and training. How are employees trained to be good users of technology? How does the IT department budget for risk management, and does the budget include funds for physical, software, and information security?

The board of directors cannot possibly understand and know every security defect and every security measure implemented to reduce or eliminate the defect, but the expectation would seem to be that the board has hired those who do.

## Could you explain how identity theft occurs?

Identity theft on a personal level occurs if financial and confidential information is obtained by a third party and that third party fraudulently uses the information to become, in essence, “me.” This thief then racks up thousands of dollars of expenses on my

credit cards, they open up lines of credit that I never authorized to have opened, and they secure bank loans in my name. How does this occur? The information in databases and flowing through the Internet includes account numbers, PINs, passwords, social security numbers, bank relationship information, and credit card numbers.

When a bank transmits or stores information electronically, remote users can gain access to it, particularly if there are not good security measures protecting that information. And when they break into the vault, so to speak, hackers or gangs of hackers can grab hundreds of thousands of pieces of information in one fell swoop.

If you are a bank and information on thousands of customers has gone out the door, your damages due to identity theft are multipronged. You suffer reputational injury, for sure, but from that reputational injury comes financial liability, to customers and possibly shareholders, and the associated administrative and investigative costs that will follow.

theft and disclosure of customer information? That's a big question mark.

### **Explain some of the risk-transfer options available today in terms of coverage for identity theft and other types of cyber risks.**

There is a first-party side and a third-party side to this. First-party side means that if an event occurs, such as a fire, you have a first-party loss—your building burned down and you have to pay to replace it. There are a variety of first-party events that can lead to loss, such as a breach of security and unauthorized access to your systems. Someone can enter the bank systems and steal your money—electronic theft. This is no different than someone walking into your branch wearing a ski mask, toting a gun, and saying, "Give me all the money in your teller drawers." As an example, another first-party event is when somebody "walks" into your system and damages your data or vandalizes your website, rendering you inoperable that day. This latter scenario may also lead to a third-party loss to those customers

All of these situations would impact the organization financially and are considered first-party losses. They should be evaluated for their potential of occurrence, and the ability to recover from them, as well as the ability to transfer some of the identifiable risk to an insurance company. The risk manager of an organization should evaluate its current policies to determine whether or not they cover these exposures, however most of these items are not typically covered by traditional insurance.

When a third party is injured or harmed and your organization is responsible, a third-party lawsuit will likely be filed against you as an organization. This can include such exposures as identity theft or the invasion of your customers' privacy. Another area of exposure banks increasingly are looking at is website content and the infringement of a third party's intellectual property, or what I call advertising injury perils, such as the infringement of one's copyright or one's trademark. Perhaps someone uses your website to access another website, information you don't own. There is also the promise that your website will be up and running 24/7. What happens when it's shut down for several days because of a security breach? Another situation is what I call a conduit injury where you're the middle man. A hacker accesses your system, grabs your e-mail database and vendor/customer list, and uses your system to send out damaging malicious code, such as a virus, worm, or Trojan horse.

### **"Community banks are not immune to cyber risk just because they are small; in fact, they might be more of a target."**

What will it cost to patch the security weakness and investigate the crime? How will it impact your company financially to restore customers' account numbers and reissue credit cards? And last, what is the liability you assume as a result of the third-party

whose reliance on your system is key to their livelihood. Finally, one of the perils is extortion... someone telephones or e-mails you and says they are holding your customer information hostage until you release ransom money.

### **Do insurance companies have different philosophies when it comes to cyber risk product offerings?**

There are three approaches to cyber risk insurance product offerings. Some insurers simply do not provide specialized coverage for these unique exposures. The next category follows a band-aid approach by providing endorsements to traditional policies, such as property, fidelity, and bankers professional liability insurance. The last approach is to provide stand-alone cyber solutions, which is what Chubb and others have done. And that approach is two-pronged. Some insurers choose to provide a solution for first-party exposures and separately provide a third-party liability exposure in a different contract. Other insurers blend them together into one contract.

### **Do bank directors need to get involved with the development of their organization's cyber policy?**

Yes, because the FDIC and other banking examiners are now asking financial institutions if they purchase cyber insurance. The board doesn't need to look at the actual policies, but it should at least ask if the bank's risk manager has evaluated the insurance programs that the company has purchased and determined that these perils have been addressed.

Bank Director *also spoke with Jeffrey J. Brown, assistant vice president, DFI ForeFront Product Manager, Chubb Group of Insurance Companies, about how cyber risk affects community banks.*

### **Are community banks as much at risk as larger banks to the threat of cyber-liability?**

Absolutely. Once you have an Internet presence, you are exposed to the world. Community banks are not immune to cyber risk just because they are small; in fact, they might be more of a target. Most of them have websites and PC banking, and even if they don't have PC banking their websites are often transactional, with services such as bill-pay. They offer these services to compete with large institutions and to retain customers. Community banks' mission is to provide superior service to local clientele so they're definitely in the ring with cyber exposure. And legislation demands they look at cyber risk. FDIC examiners are also looking at how financial institutions are mitigating cyber risk and from a reputational point of view, banks need to be concerned about protecting their customers' information. We've entered a whole new age, the information age, and anyone who is involved in it has to step up to the plate.

### **How can small community banks deal with cyber risk if they don't have a full-time chief risk officer?**

Because community banks typically do not have a full-time risk manager, this duty usually falls to one of the senior officers. Furthermore, the board, either at the audit committee or executive committee level, also should be evaluating it. First the board needs to be aware of the potential risks associated with the broadened use of technology. And it needs to get a sense of what technology the bank is using and whether or not that technology is outsourced. Most community banks

outsource their IT services through a third-party vendor, but they can't outsource the liability. They will still be held responsible. The board also needs to ask bank management how third-party vendors are chosen and understand the bank's due-diligence process for the selection of those vendors, and they should request that these vendors prepare reports on their security measures, software, and other technologies they use.

### **Are there any advantages to being a smaller bank when it comes to mitigating cyber risk?**

I don't think so. Only if a community bank has no Web-based operations can they say that they are totally out of the realm of exposure. Once you have a transactional website, you are vulnerable to hackers looking for weak targets. Hackers run programs that hit sites and look for vulnerabilities or missing software patches. Part of keeping security updated is keeping up with maintenance on your software. As software companies discover holes in their security, they release patches. And they usually discover these glitches because a company fell victim to some sort of intrusion. Therefore, if your vendor isn't keeping up with installing all of these patches in a timely manner, you've got an issue. So, being small does not reduce the risk. In fact, the same dollar amount loss is a much larger threat to a community bank's balance sheet than it is to a regional or money center bank, not to mention that community banks trade on superior service and reputation.