

Data Breaches: Avoiding Hard & Soft Costs

Historically, among the most serious things a director or senior executive at a community bank feared hearing was “We’ve had a robbery” or “We’ve had a fire.” It is now time to add “We’ve had a data breach” among the worst-case scenarios. Bank robberies and property damage have long been familiar perils; and most banks consider themselves well-prepared for such first-party threats. However, these “brick and mortar” risks are being eclipsed by e-commerce liabilities. Today’s community banks are increasingly dependent on a wide variety of cyber activities for conducting everyday business. With this change in the way banks operate comes a new risk. Cyber liability was recently named by a leading insurance blog as the “Stealth Risk” facing community banks in 2010.¹ In these tough economic times, when every dollar counts, a data breach could result in significant regulatory, financial and reputational costs. Bank directors need to consider ways to protect themselves and their companies.

Customer data is one of a bank’s most important assets, and bank directors and managers have a custodial responsibility to protect “any and all” private and confidential information (including that of employees) in their possession. Since someone other than the bank incurs the harm in a data breach, it is often referred to as a “third-party” risk. A bank could damage a third-party through employee negligence, a malicious virus, a hacking incident, or copyright infringement. As a general rule, long-established insurance coverages, such as the Banker’s Blanket Bond or a property policy, were designed to cover “tangible” property such as money or securities from named perils such as theft or fire. Customer data would be considered “intangible” and typically would be excluded from those old-school coverages.

It would be a mistake to assume data breaches are only “big bank” problems. Last year, a \$160M bank in Colorado compromised 1,325 customers’ data by e-mailing an attachment containing their names, Social Security Numbers, and account details to the wrong Google address.² In November 2009, over a six-day period, hackers stole log-in credentials for more than 8,378 accounts at a \$1.7B Long Island, NY bank.¹ The theft of payment card information from national merchant card processor Heartland Payment Systems, Inc. in early 2009 is thought to involve at least 660 community banks nationallyⁱⁱ, but the real number could include hundreds more. Many community banks had to bear the costs of that third-party breach themselves – a bank in Massachusetts had to pay \$50,000 for its 3,300 debit cards that were comprised.ⁱⁱⁱ

Regulatory Climate: Increased Attention on Cyber Protection

Both federal and state regulators have been progressively tightening customer security requirements. The Gramm-Leach-Bliley Act of 1999 requires a bank to “respect the privacy of its customers and to protect the security and confidentiality of those customers to nonpublic information.”^{iv} The Sarbanes-Oxley Act (SOX) of 2002 requires management to personally attest to a controlled environment. Forty-four states now have a patchwork of privacy and consumer notification laws in place (importantly, it is the residence of the customer, not the institution, that matters; so a bank in Oregon might have to abide by the more stringent notification laws in Massachusetts).

In a regulatory push to get bank boards even more involved in data security, the four-time delayed Red Flag Rules are to finally come into effect June 1st, 2010. The Federal Trade Commission’s (FTC) Red Flags Rules are designed to identify, detect and respond to “red flags”, or suspicious patterns, of identity theft.^v As community banks become more stable financially, the regulatory pendulum is expected to swing away from focusing on safety and soundness and towards consumer protection. Showing the importance of information management, the FDIC issued 11 C&D orders in 2009 for inadequate IT oversight.^{vi}

Hard Costs: Considerable Unbudgeted Expense

Regulatory compliance, however, does not guarantee security. As shown by Heartland, the financial costs of data breaches are significant. A 2009 report by the Ponemon Institute, a respected privacy and information management research firm, sampled a variety of industries and found that in the U.S. the “per victim cost” of a data breach was \$204.^{vii} Much of that cost is due to regulatory notification obligations and potential litigation. Customers who feel victimized could file lawsuits to seek retribution. At the least, such lawsuits would require defense costs.^{viii} So, even for a breach of several hundred accounts, the unbudgeted expenses can be substantial.

Soft Costs: Protect the Brand

While not traditional balance sheet entries, soft costs such as the bank’s reputation and customers’ loyalty are critical assets. Banking is a relationship business based on trust. Customers expect the businesses to handle their personal information with care. While the bank may believe it was the “victim” of the breach, customers and regulators will not be as sympathetic. They may view the bank as partially responsible for not preventing the breach. Recovering existing customers’ confidence, convincing potential customers the bank is trustworthy, and rebuilding the company’s reputation, could all be very expensive and long-lasting propositions.

Data Breaches: Avoiding Hard & Soft Costs

Cyber Insurance: Mitigate the Risk

A board has a fiduciary responsibility on behalf of its customers, employees, and shareholders to mitigate the company's overall risk. A board should try to reduce the cost burden of a breach by implementing "best practices", such as regularly reviewing and updating internal controls and hiring third-party consultants to evaluate the bank's security procedures. But, in the end, directors only have two options regarding cyber vulnerability: reserve against contingency or transfer some risk by purchasing a cyber liability policy. Cyber insurance provides peace of mind, even when the bank might be adequately managing its cyber risk. A cyber policy should be considered an integral part of the bank's holistic risk management program. It is a budgeted item for an unexpected, often considerable, expense. Cyber policies vary greatly with respect to coverage, limits, exclusions and definitions. When contemplating a cyber liability policy, buyers should consider the following:

- Customer relationships are paramount. Banks have a custodial duty to protect their customers' confidential information. Look for a policy that covers privacy injury resulting from unauthorized use or disclosure of all private information in the bank's custody. There should be coverage not only for e-commerce and the bank's web site, but also for customer information stored off-line on the bank's network.
- Make sure the policy covers privacy resulting from the theft or loss of removable media such as bank-owned laptops, PDAs, or other forms of portable storage. Mistakes happen.
- With its website, the bank's internal systems are "borderless" and claims can originate from anywhere in the world. Be sure the cyber policy covers third-party claims that can occur worldwide.
- As noted above, a data breach entails significant financial and reputational costs. Cyber policies should cover voluntary notification costs as well as those compelled by "duty to notify" laws, usually with no or low deductibles. Your policy should also cover the costs of hiring a public relations firm to recover the bank's hard-earned reputation and to provide credit monitoring services for affected customers.
- Defense of privacy regulatory actions is expensive and time-consuming; the policy should include a full policy limit for regulatory defense coverage for actions brought by regulators. "Duty to defend" policies are desirable because cyber-insurers are typically experienced in privacy regulation and computer forensics.
- Since 40% of breaches result from a third-party to which a company entrusts its information,^{ix} a cyber policy that protects against third-party liability exposure is preferable. Also, the bank should have "hold-harmless agreements" in place with their third party provider.

If a board is uncertain about the adequacy of its coverage against data security risks, it should consult an insurance advisor for a review of policies and coverages to identify potentially costly gaps in the bank's overall risk management and insurance program.

1 "Data Privacy and Security: The "Stealth Issue" of 2010?", *The D&O Diary*, March 16, 2010

2 "Data Breaches in 2009 – A Year in Review", Assassin's Blog,

3 "22 Banking Breaches So Far in 2010", www.bankinfosecurity.com, March 23, 2010

4 "Heartland Breach: The Latest Updates on the Biggest Breach Ever Reported", www.bankinfosecurity.com,

5 "Hacker Costs Keep Growing", *The Boston Globe*, August 22, 2009

6 "Managing Cyber Risk at Community Banks: The Board's Role in Internet Security", *Bank Director Magazine – Business Insights*, First Quarter 2005

7 "The Evolving Landscape of Data Privacy", *LTN Law Technology News*, March 12, 2010

8 "New Exam Focus? Well-Capitalized Banks Hit with C&Ds Over IT Issues", www.FinCriAdivor.com November 15, 2009

9 "The Cost of Data Breaches: It Ain't Cheap!", *Technologist: The FindLaw Legal Technology Blog*, April 27, 2010

10 "Costs of a Data Breach – Dr. Larry Ponemon", www.bankinfosecurity.com, Feb. 2, 2010

11 "Taking Cover: Directors and Officers Respond to the Growing Threat of Cyber Attacks", *Best's Review*, July 2008

For additional information on CNA's Community Banks Program, please contact Mark Tomlinson, Underwriting Director, at mark.tomlinson@cna.com or 312-822-4831.

The purpose of this article is to provide information, rather than advice or opinion. It is accurate to the best of the author's knowledge as of the date of the article. Accordingly, this article should not be viewed as a substitute for the guidance and recommendations of a retained professional. In addition, CNA does not endorse any coverages, systems, processes or protocols addressed herein unless they are produced or created by CNA. Any references to non-CNA Web sites are provided solely for convenience, and CNA disclaims any responsibility with respect to such Web sites.

To the extent this article contains any examples, please note that they are for illustrative purposes only and any similarity to actual individuals, entities, places or situations is unintentional and purely coincidental. In addition, any examples are not intended to establish any standards of care, to serve as legal advice appropriate for any particular factual situations, or to provide an acknowledgement that any given factual situation is covered under any CNA insurance policy. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All CNA products and services may not be available in all states and may be subject to change without notice. CNA is a registered trademark of CNA Financial Corporation. Copyright © 2010 CNA. All rights reserved.