

## Cyber safety: the latest tool in the risk management arsenal – ‘cyber insurance’

by Mark Greisiger

**Traditional insurance such as financial institution bonds, property and professional liability coverage may leave significant gaps in your bank’s insurance program. Here’s why and what to do about it.**

**R**eputation and trustworthiness are key defining attributes of a bank. Customers trust banks as secure places for their most valuable assets, from their life savings to their family diamonds. With the enactment of the Gramm-Leach-Bliley Act (GLBA), banks are now held to a higher standard for the safeguarding of another precious asset: non-public customer information. Yet, increasing dependence on technology, outsourced providers, and Internet-based services makes it virtually impossible to guarantee 100% protection of customer data from malicious or unintentional acts. Managing these cyber risks is one of the most pressing technical challenges for your bank today.

Not as obvious, but of equal importance, cyber risks go well beyond malicious viruses and computer hacks. Service outages, accidental deletion of key data, and privacy policy breaches can all occur without malicious intent. Your institution

may also sustain liability from misappropriation of web site content or employees using e-mail to slander bank customers. Additional risks include sensitive information traversing unencrypted over the Internet or personal account information, credit card numbers, or passwords stored in an unprotected database.

Managing these cyber risks requires the same process as managing any other traditional risk exposure: eliminate the risk where exposure is high and return on investment justified; mitigate other risks to minimize potential effects; accept some residual exposure where risk is minimal and cost of remediation unacceptably high; and finally transfer the risk to an insurance company with the purchase of cyber insurance.

Several insurers, including AIG, Chubb, Lloyds of London, Progressive, St. Paul and Zurich, offer cyber insurance policies to better protect a bank’s computer network. While these policies provide mone-

tary assurance against cyber damages, they do not remove the burden of vigilance from the bank. In fact, underwriters will require the bank to demonstrate that certain security practices and controls are in place for insurability.

In the same way that insurers send in loss-control engineers to check the sprinklers when underwriting a building, underwriters offering cyber insurance may require applicants to undergo an information-security risk assessment. Many cyber insurance underwriters use the ISO 17799 security standard as an assessment framework. This comprehensive standard can help score financial institutions on 10 areas of exposure:

- The bank’s security policy;
- The security organization;
- Information asset classification and control;
- Personnel security;
- Physical and environmental security;
- Computer and network management;
- System access controls;
- System development and maintenance;
- Business continuity planning; and
- Security compliance.

Other assessment areas may include intellectual property infringement and privacy.

---

*Mark Greisiger is the co-founder and President of NetDiligence ([www.netdiligence.com](http://www.netdiligence.com)), a cyber risk assurance and information security services company. Greisiger has spent his career in the cyber risk management business, developing some of the first cyber insurance policies to enter the commercial marketplace, and is now assisting financial institutions with cybersecurity loss-prevention services. Greisiger is a member of Pennsylvania’s Homeland Security Advisory Committee and a frequent author and speaker on cyber risk management and information security. Reprinted with permission from BankNews Publications.*

## Cyber security risk assessment: a high-level explanation

A cyber security risk assessment is a process based on a methodology that seeks to identify critical information assets, potential threat scenarios, and inherent vulnerabilities to determine an organization's level of residual risk exposure. The assessment reviews people, processes and technology to clarify how the business is prepared to address "e-risk" exposures, which can be defined as both malicious (hacking) and non-malicious liability threats. An assessment process grounded in best practices strives to balance business operation needs with the due care security standards and vital loss prevention requirements essential to mitigate and eliminate network exposures, such as human error or software malfunction. Based on risk exposure and business needs, the assessment results include a security protection strategy with recom-

tions, including finance and IT.

**Senior management commitment.** Your executive management team must demonstrate commitment to security and privacy issues and allocate a proper budget to implement effective enterprise-wide network risk management.

### Processes

**Network asset policies.** Establish and enforce effective policies for network security, privacy, document retention and employee use of e-mail and the Internet.

**Legal reviews.** Establish and enforce a legal review process for software development contracts, outsourced service level agreements, and screening of web content for intellectual property infringement.

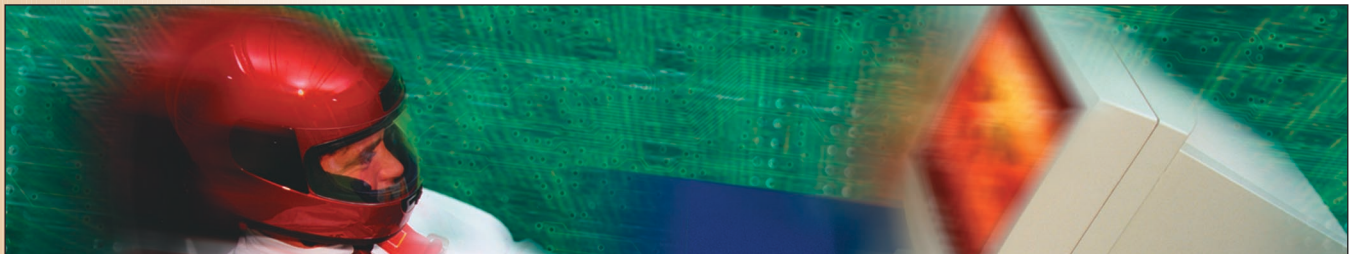
**System change and patch management.** Define processes to recognize known vulnerabilities of all network systems so that proper hardening and configuration can be performed. This includes

Demonstrate the ability to fully restore systems and key data from a backup site and to switch over operations to a standby hot site.

### Technology

**Baseline security controls.** To meet due-care industry accepted standards, implement controls that include: firewall with intrusion detection systems, including personal firewalls on all telecommuters (according to the ICBA survey, only 41% of banks had intrusion detection software); access controls, such as strong, hard-to-guess passwords with input limits; anti-virus software; event and security logs that are reviewed periodically; backup data; and encryption for data in transit and database storage (only 49% of survey respondents had encryption technology).

**Redundant/mirror systems.** Co-locate mission critical systems with redundant fail-over components.



mendations for additional safeguards and countermeasures that may reduce the frequency and severity of residual risk.

The following "top 10" best practices offer guidelines that address people, process and technology issues to help ensure a solid base level of security in a bank.

### People

**Vigilant employees.** Foster a security mentality in employees. Keep them up to date on the latest e-risk threats, network-oriented liability and preventions for the most common vulnerabilities, such as virus-carrying e-mail.

**A prepared internal net-security and privacy team.** Train the team on key safeguard practices, including knowledge of proper systems hardening, patch management and business continuity. Provide education on privacy laws and standards regarding the notice, collection and usage of personal data. Perform background checks for employees in sensitive posi-

---

**“Ultimately, protecting your information assets through vigilant practices and appropriate insurance will help you protect your most important asset — your bank’s reputation.”**

---

receiving security advisories from product vendors and CERT, performing same-day installation of the latest security service packs, changing default server settings and turning off unnecessary services.

**Controlling network privileges.** Ensure that exiting contractors and employees have their access privileges revoked in a timely matter to prevent sabotage.

**Emergency response and business continuity plan.** Implement procedures and test backup plans on an annual basis.

Ultimately, protecting your information assets through vigilant practices and appropriate insurance will help you:

- Reduce financial and liability exposure;
- Reduce concern regarding GLBA compliance issues; and
- Protect your most important asset — your bank's reputation with customers who need to know that their personal information is safeguarded as closely as their savings and family valuables. **BN**