The Ins and Outs of Cyber Insurance

March 31, 2016
Speakers

**Mike Read**  
Marketing and Sales Manager  
ABA Insurance Services

**Peter Hilbert**  
Senior Attorney  
ABA Insurance Services

**Doug Johnson, Moderator**  
Senior Vice President  
American Bankers Association
Agenda

• Current Trends in Cyber
• Cyber Insurance Coverage Components
• Financial Institution Bond Coverage
• Buying Cyber Insurance
Current Trends in Cyber

Global Changes
- Increasing regulatory involvement
- Industry cooperation (the ISACs)
- Increased pressure on service providers
- Standardization in security protocols

Insurance Changes
- More stringent underwriting standards
- Clarifying policy language
- Increased focus on liability coverage
- Risk assessment requirements
Anatomy of a Data Breach – Claims by the Numbers

- Median claim payout = $144,000; average claim payout = $733,109
- Median cost per record = $20; average cost per record = $956
- Median cost per breach response expense = $110,594; average cost for breach response services = $366,484
- Median cost for legal defense = $283,300; average cost for legal defense = $698,797
- Median cost for legal settlement = $150,000; average cost for legal settlement = $588,520
- Median number of records lost = 3,500; average number of records lost was 2.4 million
- Personally Identifiable Information was the most frequently exposed data
- Hackers were the most frequent cause of data loss, followed by employee mistakes
- Insiders were involved in 32% of claims submitted

Source: NetDiligence 2014 Claims Study
Survey of 2013 claims filed with major cyber insurers across all industries
Cyber Insurance Coverage Components

Third Party
- Privacy Liability (data security)
- Systems Security (virus transmission, access issues, spam)
- Web Based Media Liability (libel, slander)
- Funds Transfer Fraud (not all policies include coverage)
- Regulatory Actions (many policies are defense only)

First Party
- Breach Response Expenses
- Business Interruption
- Cyber Extortion
Privacy Liability

Exposure Addressed
- Risk of exposed data from system hacks, mal-ware, bank targeted phishing scams, and employee error.

Description
- Provides liability coverage for privacy violations resulting in the unauthorized access of either 1) confidential customer information or 2) confidential information. The unauthorized access may come from a breach of the Bank’s systems, a breach of a Service Provider’s system, or other errors or omissions on the part of the Bank.

Claims Examples
- A demand is made against the bank alleging unfair trade practices due to the disclosure of a commercial loan customer’s plan to make a bid on a competitor’s business via a breach of the bank’s operating systems.
- The bank’s systems are hacked resulting in the unauthorized exposure of customer personal information. Bank’s customers sue the bank for lack of adequate security measures.
System Security Liability

Exposure Addressed
• Risk of denial of services and web application attacks, bank targeted phishing scams and virus transmission.

Description
• Provides liability coverage for:
  – failure to provide system access (standard);
  – the transmission of electronic viruses (standard);
  – other causes of action (broad).

Claims Examples
• Demands are made against the bank for loss of business opportunity due to the loss of account access while the bank’s on-line banking systems were under a DDOS attack.
• The bank is sued by a customer who claims it’s system was damaged by a virus it received though the bank’s on-line banking website.
Web Based Media Liability

Exposure Addressed
• Risk of wrongful publishing acts via web and social based media.

Description
• Provides liability coverage for electronically displayed or disseminated information through the Bank’s:
  – Website (standard); or
  – social networking accounts (broad).
• This includes coverage for allegations of copyright infringement, misappropriation of ideas, defamation, and advertising injury.

Claims Examples
• The bank unknowingly uses copyrighted art on its website. The American Society of Artists sues the bank for copyright infringement.
• Someone posts on the bank’s Facebook page that the bank is the best because it never charges ATM fees. However, in reality, the bank does charge fees but reimburses those customer accounts which meet certain criteria. The bank does not respond by posting correct information nor does it remove the message. Relying on the false information posted, a customer files a lawsuit for reimbursement for all the ATM fees she has paid on her account to date as well as for punitive damages.
Funds Transfer Fraud Liability

Exposure Addressed
• Responds to risk of funds transfer fraud.

Description
• Provides third party coverage for wrongful acts committed in connection with the transfer of customer funds. This may be restricted to on-line transfers or may include fax, email, and phone initiated transfers.

Claims Examples
• Funds from a customer deposit account are wired to a third party bank based upon fraudulent authorization utilizing the stolen credentials of an authorized employee. The customer demands restitution.
• Funds from several customer accounts are wired overseas utilizing customer account information stolen from the bank’s systems. The customers sue the bank attempting to recover the funds.
Regulatory Actions

Exposure Addressed
• Risk of regulatory action stemming from a privacy breach.

Description
• Provides coverage for Defense Costs (and in some cases, settlement costs) for a demand brought by a Regulatory Agency in connection with privacy breaches.

Claims Example
• In the wake of a system breach resulting in the exposure of confidential customer information, the bank’s regulators make allegations that the bank had inadequate security controls. In addition, the FTC alleges the bank committed several law violations designed to protect the privacy of customer information.
Breach Response Expense

Exposure Addressed
• Expense to remediate a system breach. First Party Coverage.

Description
• Provides first party coverage for reasonable and necessary expenses incurred in connection with a data breach.
• Coverage includes forensic investigations, privacy attorney consultations, costs of issuing notifications and credit/identity monitoring services.
• Public relations expense coverage may be within the rider or a separate insuring agreement.
• Does not cover costs to remediate (patches, new software/equipment).
Business Interruption

Exposure Addressed
• Bank operations are interrupted due to the failure of its systems due to malicious activity.

Description
• The bank is indemnified for loss arising from such interruptions. Coverage usually includes loss from business income and extra expense incurred to continue operations in absence of its system access.

Claims Example
• A hacker shuts down the bank’s on-line banking platform. The website is down for 48 hours as programmers rewrite, test and elevate new code. In the interim, the bank extends hours at it branches to accommodate those who normally bank on-line in the evenings.
Cyber Extortion

Exposure Addressed
• Threats are made to damage or compromise the bank’s systems.

Description
• The bank is indemnified for loss of property surrendered as a result of such threats.

Claims Example
• A bank decides to not extend credit to a business customer. In retaliation, the customer announces it has access to the bank’s systems and threatens to initiate a Denial of Service Attack unless the bank transfers a large sum of money to its Cayman Islands accounts.
Financial Institution Bond

- Employee Dishonesty
- Extortion
  - Covers payment necessary to protect Insured and/or pay ransom for credible threats of loss or damage to the Network, Confidential Information, Money, Securities, Intangible Property or defacement of Insured’s website.
- Computer Crime Rider
  - Destruction of Data or Programs by Virus
  - Destruction of Data or Programs by Hacker
  - Funds Transfer Fraud
Reasons to Consider Cyber Insurance

• Insurance places a dollar value on an organization’s cyber risk.
• The underwriting process can help organizations identify cybersecurity gaps and opportunities for improvement.
• Many cyber insurance policies bring supplemental value through the inclusion of risk mitigation tools as well as significant incident response assistance following a cyber incident.
Categories of Information Insurers Need to Underwrite Cyber

- Dedicated Information Security Resources
- Information Security Policies and Procedures
- Employee Education
- Incident Response Planning
- Security Measures: Vendor Management
- Board Oversight
Shore up your risk management process.

This will enable you to provide better responses on insurance applications (which can lower your premiums) and will also help you identify key risk areas. Specific areas of focus should include:

- the amount and type of data stored;
- the strength of the bank’s technology infrastructure;
- the use of remote devices (for both employees and customers);
- the number and strength of third party service providers with access to sensitive information.

Assess the bank’s ability to respond to a breach – both systemically and financially.

- The bank may have sufficient staff to respond to a wide-scale system breach, but if not, insurance policies can help fill the gap with Breach Response coverage. Considerations of how to integrate insurance coverage tools into the bank’s internal response processes can help the bank make decisions on the coverage features it needs.

- Additionally, the bank should evaluate the costs it may incur to cover system downtime, forensics investigations, legal fees, notification expenses, and liability obligations in the event of a breach. This will help guide decisions on retentions and limits.
Things to do when Buying Cyber Insurance

Evaluate Policy Options

- Once risk assessments are performed and financial concerns are identified, look for policies that offer coverage and policy limits for your key risk areas. A knowledgeable broker or insurance underwriter should be able to help guide you to the right policy.

- Specific questions to ask:
  - Are breaches at your Service Provider covered if they impact your customers?
  - Are you required to use the insurance carrier’s breach response vendors, or can you choose your own?
  - Is Funds Transfer Fraud covered? What are the restrictions or requirements?
  - Are lost and remote devices (laptops, flash drives, phones) covered?
  - Is social media activity covered?
  - Is cloud based storage covered?
  - What type of data are covered? (Some policies only cover “personal” information, leaving your corporate customers exposed.)
  - What type of pre-claim and post-claim services are provided? This includes loss control tools and breach response services.
  - What type of security violations are covered? Some policies only cover lawsuits that allege violations of specific privacy laws – leaving general lapses in security policies uncovered.
  - Do I have overlapping coverage?
Questions and Answers
Thanks for your participation.

Contact information:

mread@abais.com
216-220-1319

philbert@abais.com
216-220-1342

djohnson@aba.com
202-663-5059