FARELLA BRAUN + MARTEL LLP

AUGUST 25, 2015

Cyber Insurance:

Protect Your Wine Business Against Data Security Breaches and Other Cyber Risks

Tyler Gerking, *Partner*

David B. Smith, *CPCU, ARM, Insurance & Risk Management Consultant*

What is “Cyber” Insurance?

- “Cyber” insurance protects companies against losses and claims arising from data breaches.

- The cyber insurance market is growing in light of:
  - recent high-profile data security breaches (e.g., Target, Neiman Marcus, Home Depot, Sony, JP Morgan Chase, Anthem, Ashley Madison);
  - BUT not limited to high-profile or large companies;
  - a New York Supreme Court decision finding no coverage under traditional general liability policies (Zurich American Insurance Co., et al. vs. Sony Corp. of America, No. 651982/2011 (N.Y. Sup. Ct. New York City); and
  - The insurance industry’s modification of commercial general liability policies to exclude coverage for data security breaches

- The coverage is relatively new, so its scope varies among policies.

FARELLA BRAUN + MARTEL LLP

What Kinds of Information are at Risk?

Consumer Information

- Credit Cards, Debit Cards, and other payment information
- Social Security Numbers, ITIN's, and other taxpayer records
- Customer Transaction Information, like order history, account numbers, etc.
- Protected Healthcare Information (PHI), including medical records, test results, appointment history
- Personally Identifiable Information (PII), like Drivers License and Passport details
- Financial information, like account balances, loan history, and credit reports
- Non-PII, like email addresses, phone lists, and home address that may not be independently sensitive, but may be more sensitive with one or more of the above

Employee Information

- Employers have at least some of the above information on all of their employees

Business Partners

- Vendors and business partners may provide some of the above information, particularly for Sub-contractors and Independent Contractors
- All of the above types of information may also be received from commercial clients as a part of commercial transactions or services
- In addition, B2B exposures like projections, forecasts, M&A activity, and trade secrets

Many people think that without credit cards or PHI, they don't have a data breach risk. But can you think of any business *without* any of the above kinds of information?

FARELLA BRAUN + MARTEL LLP

Potential Causes of Data Breach

- Data breach—theft/disclosure/alteration of private or proprietary information
- Insertion of computer viruses/malware
- Denial of service attacks
- Human error – programming errors, faxing/mailing errors, carelessness in handling sensitive information
- Misuse/misappropriation of information
- Cyber extortion
- Left/loss of computers or unencrypted portable devices (laptops, back-up tapes)

FARELLA BRAUN + MARTEL LLP

Data Shows Widespread Losses

- Average total cost to a company of a data security breach in 2013 was $5.9 million, which is 15% higher than the prior year and about $200 per record (*See* 2014 Cost of Data Breach Study: Global Analysis by Ponemon Institute)

- Nearly half (44%) of all data security breaches were caused by malicious or criminal attacks; the rest resulted from human error or system glitches (*Id*.)

Potentially Covered Losses and Liabilities

- First-party losses
  - Response expenses
    - Crisis management/PR
    - Forensic investigation
    - Legal advice regarding notification req’ts and liability exposures
    - Breach notification
    - Credit monitoring
    - Call center
    - Data restoration
  - Business interruption / reputational harm

FARELLA BRAUN + MARTEL LLP

Potentially Covered Losses and Liabilities (cont.)

- Defense costs and liability in third-party actions (e.g., consumers class actions, corporate customer claims)
- Regulatory scrutiny / investigation / fines and penalties (OCR, HHS, FTC, state AG, SEC)
- Limits available:
  - Primary: up to $25 million
  - Excess: up to $150+ million
  - First party expenses often sub-limited

Key Issues

- Buying cyber insurance:
  - What is the market like now?
  - What is the application process?
- Latent intrusions before policy inception – are they covered?
- What is the value of first-party coverage?
- Can you insure against the loss or theft of intellectual property?
- Breaches of third-party systems – are you covered against related losses?
- Indemnity agreements with third-party vendors

FARELLA BRAUN + MARTEL LLP

Key Issues (cont.)

- Unencrypted mobile devices
- Coverage territory and location of security failure
- Trigger
  - First-party coverage (intrusion vs. data loss)
  - Third-party coverage (claims vs. suit)
- Bodily injury / property damage resulting from a data security breach
- Cloud providers' special considerations
- PCI compliance
- Insurer-selected service providers

FARELLA BRAUN + MARTEL LLP

Contact Information

Tyler Gerking
415.954.4968
tgerking@fbm.com

David Smith
415.954.4435
dsmith@fbm.com