

The New Frontier of Cyber Liability

Presented by | John M. Link, CPCU
July 15, 2014



Cottingham & Butler

Cottingham & Butler
Dubuque, IA 52001 | 800.793.5235
www.CottinghamButler.com

Presenter



John M. Link, Vice President
563-587-5288
jlink@cottinghambutler.com



QUESTIONS

If you have questions following today's presentation, please contact John directly at jlink@cottinghambutler.com.

Target



Target Data Breach by the Numbers

40 million – The number of credit and debit cards thieves stole from Target between Nov. 27 and Dec. 15, 2013.

70 million – The number of records stolen that included the name, address, email address and phone number of Target shoppers.

46 %– The [percentage drop in profits at Target](#) in the fourth quarter of 2013, compared with the year before.

\$200 million – Estimated dollar cost to credit unions and community banks for [reissuing 21.8 million cards](#) — about half of the total stolen in the Target breach.

\$100 million – The number of dollars Target says it will spend upgrading their payment terminals to support Chip-and-PIN enabled cards.

\$1 Billion — The total costs including government fines expected to be paid by Target

What do we need to know?



- As Risk Managers, internet access presents us new and dynamic exposures which we need to properly manager
- As businesses rely more and more on data storage, our responsibility is to protect that data
- In 2013, the average cost incurred by a company due to a data breach was \$188/record....with malicious attack costs running 1.5x higher*
- 40% of all breaches occur in companies with less than 1,000 employees**

*Ponemon 2013 Cost of Data Breach Study** Verizon 2013 Data Breach Investigations Report

What is Cyber Liability?

“Cyber liability” is becoming the common phrase for network & privacy liability that affects all businesses. Also known as “information liability”, it includes:

- Network Liability – unauthorized access / use of an entity’s network. Employees, trusted third parties, or outsiders can steal identity information, critical business information, transmit malicious code, and participate in a denial of service attack – to name a few. The risk includes paper documents and electronic media.

Third Party Liability / Risk – responsibility to others

First Party Liability / Risk - what can happen to you

- Privacy Liability – violation of privacy laws or regulations that permit individuals to control the collection, access, transmission, use, and accuracy of their personally identifiable information. Includes personally identifiable non-public information and confidential corporate data

What are the Threats?

1. Unauthorized Access to or Use of your data or software
2. Computer viruses that damage or impair your data or covered systems
3. Attacks on covered systems resulting in the inability to perform or gain access to e-business activities
4. Libel, slander, disparagement, copyright infringement and public disclosure of private information
5. Theft of money, securities, data, software or computer resources
6. E-business extortion
7. Loss of reputation
8. Loss of Income from operations



What are the Regulations?

Federal Laws

1. Gramm-Leach-Bliley Act
2. HIPAA
3. HITECH (Health Information Technology for Economic and Clinical Health Act)
4. Sarbanes-Oxley Act
5. Fair Credit Reporting Act
6. Children's Online Privacy Protection Act of 1988
7. E-SIGN (Electronic Signatures in Global and National Commerce Act)
8. FISMA (Federal Information Security Management Act of 2002)
9. Homeland Security Act of 2002
10. Privacy Act of 1972

What are the Regulations?

State Laws

1. Forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.
2. 7 states have their own privacy laws
3. 19 have data disposal laws

What are the Regulations?

Reporting Requirements in Event of Data Breach

1. Notification to State Attorneys General of Data Breach
2. Individual State Reporting Requirements
3. Notice to the Secretary of Health & Human Services (HHS)
4. Breach Reporting to the US Secret Service
5. Card Brand Reporting

Claim Examples

Cyber exposures and claims:

1. Conference attendees noticed suspicious charges after staying at a Hotel. Forensic investigation discovered a data breach. 1st party and 3rd party claims.
2. A hospital upgraded IT system for patient tracking system. Data backed up to external hard drive which was stolen from IT vendor. Significant notification expenses which was into six figure costs.
3. Credit card vendor hired by retailer incurred a data breach. Liability of notification passed onto retailer.



Claim Response:

Needs Related to An Event:

- ✓ Investigation/Forensics (Do you have a network security team?)
- ✓ Defense and Coverage Counsel expenses
- ✓ Determine Compliance with all relevant jurisdiction (State, Federal, Tribal)
- ✓ Notification and credit monitoring where necessary
- ✓ Public Relations
- ✓ Possible recovery of data
- ✓ Monitoring of data/investigation assistance
- ✓ Financial impact

And On...and On...and On

Addressing the Threats



1. Design and set up proper platforms
2. Work with experts on the technology needed
3. Hire the right people with the right experience to manage the systems
4. Have a sound infrastructure in place for financial transactions
5. Develop appropriate contracts with liability transfer and hold harmless provisions – outsourcing does not necessarily eliminate all risk.
6. Transfer risk with your insurance policy

Outsourcing

No Worries – We are Outsourcing!

Business Insurance Survey, 2013:

Data breaches were more likely to occur when the data has been outsourced, according to 70% of the surveyed businesses. At least 85% of the companies responding to the survey reported that they share customer and employee records with third parties by providing billing, payroll, employee benefits, Web hosting, or other information technology services.

Despite this outsourcing exposure, 62% of the surveyed businesses do not require third parties to cover costs associated with a data breach in their contracts.

Insurance

We should consider risk transfer through insurance...

What do I need to know?

Insurance Market

Insurance Market is running amok with new Cyber Liability insurance policies



And more and more coming out with these policies every day.

Other Policies for Protection

Is there protection in other insurance policies we currently have in place?

1. **General Liability** – definition of “personal injury”; careful on exclusion for “customers of insured organization”
2. **Employment Practices Liability(EPL)** – could extend to “employment related” breach of privacy; further could extend to 3rd Party provisions

Other Policies for Protection

Is there protection in other insurance policies we currently have in place?

3. **Fiduciary Liability** – be certain HIPAA civil money penalties are covered and no HITECH exclusions exist
4. **Crime Insurance** – typically for “tangible” loss; provisions for “computer fraud” and “funds transfer fraud”

Key Elements of Cyber Insurance Coverage

- **3rd Party - Liability**

- ❖ Privacy Injury – privacy rights violations
- ❖ Privacy Regulatory Proceeding – cost to notify others of breach
- ❖ Network Security Liability – theft of other's information, infection of third-party, damage to other's network, other's inability to access your network
- ❖ Content Injury or Broad Form Media – advertising materials, trademark infringement, copyright infringement
- ❖ Cyber Terrorism – computer attacks that are acts of terrorism

- **1st Party - Liability**

- ❖ Network Extortion – payment for extortionist's demand to prevent network loss or implementation of a threat
- ❖ Network loss/damage – cost to recreate or restore to pre-loss condition
- ❖ Business Interruption & Extra Expense – loss of income and extra expense
- ❖ Event Management – cost to retain public relations services
- ❖ Electronic Theft – loss of money, goods, security, trade secrets, intangible property

Key Elements of Cyber Insurance Coverage

1. Buy 1st and 3rd party coverage
2. Breadth of Coverage...the internet has NO boundaries
3. Consider whether your Cyber Liability policy protects info on unencrypted devices
4. Is there coverage for Business Income/Extra Expense/Dependent Business Income?
5. Protect info in the care, protection or control of 3rd parties
6. Consider data restoration costs in your coverage
7. Consider whether your policy covers regulatory actions
8. Consider whether injuries to a company's corporate clients are covered, not just injuries to natural persons
9. Consider whether the insurance policy covers data transmittals that take place outside of the company's offices
10. If your business accepts payment by credit cards, consider if your policy provides for payment card industry liabilities
11. Provides coverage for identity theft resolution services?
12. Consider including loss control services in your coverage
13. Is there coverage for Property Damage and Bodily Injury?

How do I know??

First - Work with a competent insurance broker/advisor who understands the true difference of insurance for your business.

Second - Conduct a formal review of all your insurance policies.

Example: At Cottingham & Butler, client and prospective client policies are put through our Risk Management Analysis to determine risk exposures...This becomes a working, breathing document to which is reviewed with management – Thus, offering a level of additional protection showing due diligence was done

Third - You could actually read the policy...

Fourth - You'll know what you have when you have a breach...which is the worst time to find out!

Summary

1. There is a need for cyber liability protection
2. Transferring risk through insurance is a small cost – “what if” is very expensive
3. Insurance policies are not equal – Review them!
4. Risks continue to evolve and change and the courts continue to evaluate this exposure

QUESTIONS?



John M. Link, Vice President
O: 563-587-5288 C: 563-590--0428
jlink@cottinghambutler.com

