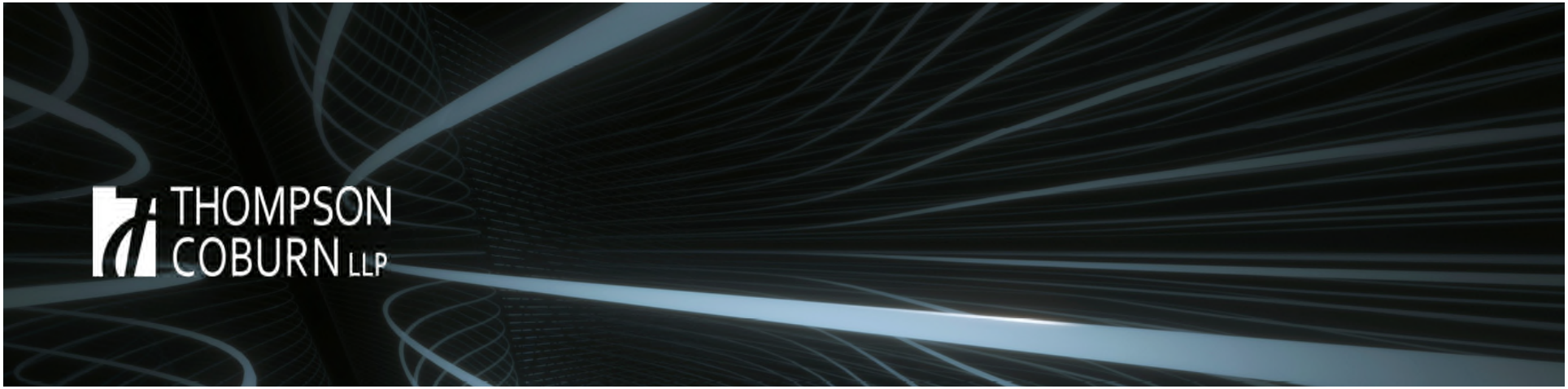
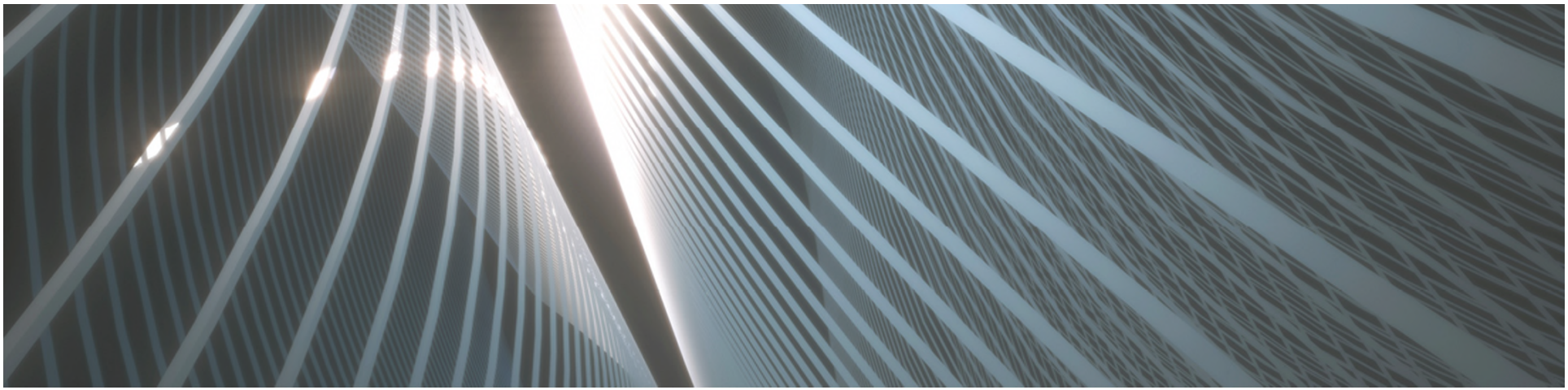


Are You Protected?
Insurance Coverage for Cyber Risks

Presented by:
Matt Darrough and Brandi Burke



A Security Breach Is Inevitable

"There are only two types of companies: those that have been hacked and those that will be. Even that is merging into one category: those that have been hacked and will be again."

Robert Mueller, III,
FBI Director, 2012

THOMPSON COBURN LLP

Are You Susceptible?

- You have to be correct 100% of the time; cybercriminals need to be correct once.
- New and developing threats are not going to stop.
- Technology is changing and criminals are adapting.
- Human error is a certainty.
- No company is immune.
- It's not a matter of if, but when.

Abundant Threats Exist

External Threats

- ✓ State Sponsored
- ✓ Criminal Attacks
- ✓ Hacktivists/Activists
- ✓ Social Engineering
- ✓ Extortion/Ransom Threats
- ✓ Malware/Viruses

Internal Threats

- ✓ Malicious Employees
- ✓ Carelessness
- ✓ Willful Ignorance
- ✓ Leavers
- ✓ System Failures

THOMPSON COBURN LLP

Risk Transference Generally

While risk avoidance is of great importance, response planning and risk transference are required if we assume that a security breach is likely to occur.

- Risk transference typically takes two forms:
  - Indemnification in contracts with others, such as service providers;
  - Insurance
    - Purchased
    - Additional Insured Status on Vendor's Required Insurance

THOMPSON COBURN LLP

Cybercriminals

- Around the globe.
- Seeking political, military, or economic advantage.
- Usually steal money or information that can be monetized in some way (credit card numbers, health records, personal identification information, tax returns, etc.)
- Breaches intended to secure any advantage can result in an impact beyond the targeted information.
- Yahoo, Target, Home Depot, LinkedIn, Verizon, Wendy's, Cottage Health System, Sony, Neiman Marcus, just a few in recent years.
  - Symantec 2016 Internet Security Threat Report – increased targeting of small and mid-sized companies over past five years (in 2015, 65 percent of phishing attacks directed to small and mid-sized companies).
  - As large companies dedicate more resources to cybersecurity, small and mid-sized companies become easier targets.

THOMPSON COBURN LLP

Gaps in Traditional Coverages

- Property Coverage:
  - Not Insured Peril
  - Not Insured Property
- Commercial General Liability:
  - Not damage to tangible property
  - Not personal or advertising injury
  - Not first party coverage

- Errors and Omissions Liability:
  - Not first party coverage
  - Does not arise out of professional services
- Directors' & Officers' Liability:
  - Not first party coverage
  - Exclusions
- Crime:
  - Covers loss of tangible property, money, securities
  - No third-party protections

THOMPSON COBURN LLP

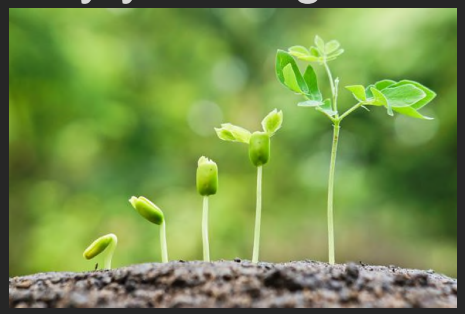
Cyber Risk Insurance Was Historically Difficult to Underwrite

- As a demand began to develop for cyber risk insurance products to fill in gaps, insurers struggled to underwrite the risk.
- The risk was difficult to quantify due in large part to a lack of actuarial data.
- To further complicate the assessment, the risks were unpredictable and always evolving.
- Insurers necessarily relied on qualitative assessments of a prospective insured's business, culture, systems, and procedures.
- The insurance was often customized and therefore, more expensive.

THOMPSON COBURN LLP

Growth of Cyber Risk Insurance

- Products started to appear on the market about twenty years ago.
- Interest has grown rapidly in the recent past with:
  - Enactment of privacy breach notice laws;
  - Increased reliance on electronic information;
  - Use of Internet;
  - Storage of valuable information;
  - High-profile hacking scandals/increased risk awareness.



- Current premium in excess of $3 billion, with estimated tripling in the next several years.
- Some speculate that the global market for cyber risk premium could ultimately be in excess of $80 billion.
- Markets now provide a multitude of insurers offering various cyber risk products.
  - U.S. and European (not uniform).
  - Increased competition results in better pricing and expanded coverage.

Valuing Your Assets

- In recent surveys, responding organizations valued their cyber assets above their tangible property (plant, property, and equipment).
- Sixty-five percent expected increased risk of cyber risk exposure in the next 2 years.
- Yet, a majority of the surveyed companies placed about 4 times more insurance on property than cyber risk exposures.

2017 Cyber Risk Transfer Comparison Global Report, Ponemon Institute

THOMPSON COBURN LLP

Overview of Data Breach

1. Discovery - Theft, loss, or unauthorized disclosure of non-public information in care, custody, and control of insured or a third-party for whom the insured is legally liable.
2. Evaluation – Forensic investigation and legal review.
3. Management – Handling of short-term crisis, including notification, monitoring, public relations.
4. Handling – Losses in income, lawsuits, regulatory fines, reputation damage.

Costs – 2016 Ponemon Cost of a Data Breach Study determined average consolidated total cost of a data breach is $4 million, with an average cost per record lost or stolen of $158

THOMPSON COBURN LLP

Cyber Risk Insurance Generally

- First Party Coverages
  - Event Response
    - Legal Costs
    - Forensic Costs
    - Remediation Costs
    - Public Relations
  - System Restoration
  - Notification Costs
  - Credit Monitoring
  - Business Interruption
  - Cyber Extortion

- Third Party Coverages
  - Network Security Liability
    - Defense of claims arising from breach in security or transmission of malware/viruses
    - Indemnification
  - Privacy Liability
    - Defense of claims arising from mishandling of private or confidential information
    - Indemnification
  - Regulatory
    - Defense
    - Fines/Penalties

THOMPSON COBURN LLP

First Party Coverage Specifics

Exposures	Coverage Description
Legal Expense (Breach Response)	Legal expense associated with reviewing and determining responsibilities under Privacy Breach Laws
Forensic Investigation (Breach Response)	Expense for investigation of intrusion into the insured computer system and to restore the system
Notification Expense (Breach Response)	Expenses to comply with the notification requirements imposed by applicable Privacy Breach Laws
Credit Monitoring (Breach Response)	Credit monitoring costs for third parties that had private information potentially disclosed
Public Relations (Breach Response)	Expenses required for a public relations firm
Data Recovery	Expense to recover data damaged on an insured computer system as a result of a security failure
Business Interruption	Lost income from interruption to an insured system as a result of a security failure
Cyber Extortion	Payments made to party threatening to attack system or required to restore system

Third Party Coverage Specifics

Exposures	Coverage Description
Network Security Liability	Defense and indemnification from third-party claims arising from failure of system to prevent a security or privacy breach
Privacy Liability	Defense and indemnification from third-party claims arising from failure to protect private information in care, custody, or control
Regulatory Liability	Defense and indemnification from actions by Federal, State, or Foreign regulators relating to violation of privacy laws
PCI Assessments	Contractual assessments, fines and penalties owed under terms of Merchant Services Agreement due to non-compliance with Payment Card Industry Data Security Standard (PCI-DSS)
Media Liability	Defense and indemnification from intellectual property and personal injury perils that result from dissemination of content (patent and trade secrets may not be covered)
Errors & Omissions	Defense and indemnification for wrongful acts committed by or on behalf of insured in providing services

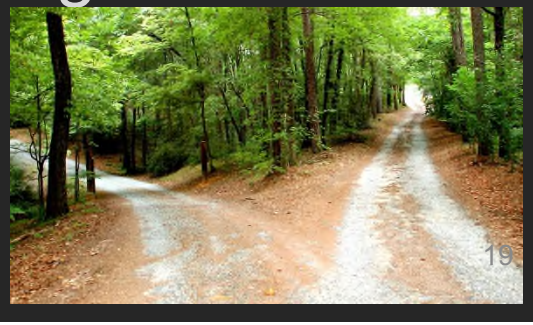
Risk Assessment

- In developing an insurance strategy, a company needs to consider its risk profile, risk appetite, and the availability of cash reserves to respond to a loss.
- If there is a level of comfort with carrying some risk, higher limits may be available for the same premium by purchasing coverage with a substantial retention or deductible.
- Assessment of current insurance portfolio and cyber risks should provide a guide to the requisite cyber risk coverage.
- Work with broker, risk manager, IT, and counsel in identifying needed coverage, approaching the markets, and comparing offerings.

THOMPSON COBURN LLP

Current Market

- At least 31 insurers issuing some form of cyber coverage currently. 2016 Betterly Report.
  - Different brokers may have access to different insurers.
- Capacity differs greatly among insurers.
- Many insurers underwrite both primary and excess coverages.
- Companies are placing coverage through US insurers and in the London Market.
- Availability and pricing could differ depending on sector - financial, healthcare, and large retail companies face greater exposure.



THOMPSON COBURN LLP

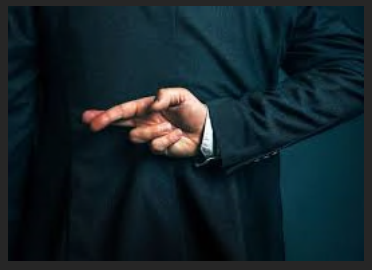
The Application Process

- Because of the qualitative assessment performed by the underwriter, the process of placing coverage is necessarily cooperative.
- Risk management department may lack detail required to provide requested information, requiring involvement of IT.
- The application is important. Insurers can seek to rescind or void coverage based on misrepresentation at a later date. The application is usually incorporated into a purchased policy.
- Insurers will examine systems, policies, procedures, and claims experience.
- The insurers rely on the application in making decisions concerning offerings, issuance, pricing, limits, and retention.
- Error on the side of overinclusion with supplements.

THOMPSON COBURN LLP

Devil Is in the Details

- The policy forms are not uniform.
- In addition to comparing quotes, it is essential to compare offered policy forms.
- Policies are a labyrinth of insuring clauses, definitions, exclusions, exceptions to exclusions, and conditions with interplay among the various provisions.
- Proposed endorsements modify the base policy form.



THOMPSON COBURN LLP

Some Concerning Provisions

- There should be coverage for breaches resulting from negligence:
  - Exclusion for failure to continuously implement the procedures and risk controls identified in the Application.
  - Exclusion for failure to take reasonable steps to use, design, maintain, and upgrade security.
  - Exclusion for mechanical failure, error in design, or deterioration.
  - Exclusion for loss caused by employee.
  - Exclusion for errors in programming.
  - Exclusion for interruption or failure of Internet or utilities.
- Third party networks and vendors, including cloud usage:
  - How define system and direct control.
  - How handle indemnification agreements in vendor contracts.
- Implications of a “war”, foreign enemies, and terrorism exclusions.
- What coverages for regulatory (which regulators, defense only, fines/penalties, PCI-DSS)?
- Derivative suits for insecurity. Compare to D&O liability coverage.
- What type of first party coverage provided to fill gaps.

Social Engineering Fraud

- Social Engineering Fraud is a significant risk.
- What is it? Employee of company is tricked into transferring funds to a fraudster. Fraudster typically impersonates a vendor, client, or supervisor in an email requesting a wire transfer.
- Are you covered? Many assume incorrectly under either cyber risk or crime coverage.
  - May not be covered under cyber risk policy because no first party coverage for such loss.
  - May not be covered under a crime policy as there is no entry into the system, not direct loss, or voluntary parting/cyber/social engineering exclusions.
- What to check with respect to coverages:
  - Does it fall within the insuring grants?
  - If so, is it excluded?
  - Is it covered, but with a sublimit?
  - What conditions imposed on recovery?
  - Insurers are starting to provide offerings as demand increases.

THOMPSON COBURN LLP

Indemnification and Additional Insured Status

- Can transfer risk through contractual provisions with providers whether you have your own insurance or not.
- Belt (Indemnification) and Suspenders (Additional Insured).
- Proper contractual language required.
- For additional insured status, insurance specified and written on a primary and non-contributory basis with waiver of subrogation.
- Not advised to rely on certificates alone.

THOMPSON COBURN LLP

Using Your Coverage

- First Party Coverage
  - Policy Trigger – loss or discovery within the policy period (suspected or confirmed)
  - Satisfying Conditions
    - Notice
    - Proof
  - Cooperation
  - Vendor Selection
  - Timing
  - Other Insurance
  - Subrogation, including indemnification claims
- Third Party Coverage
  - Policy Trigger - differences in a claims-made form.
    - Is a Suit required? What about a demand?
  - Notice
    - Timely and Proper
  - Cooperation and Defense
    - Reserved Rights
  - Resolution
  - Other Insurance
  - Subrogation, including indemnification claims

Questions

Matt Darrough
(314)552-6552
mdarrough@thompsoncoburn.com

Brandi Burke
(314)552-6598
bburke@thompsoncoburn.com

Thompson Coburn
One US Bank Plaza
St. Louis, Missouri 63101
www.thompsoncoburn.com

THOMPSON COBURN LLP