



**WARREN FISCHI**

MCGRIFF INSURANCE  
SERVICES

# Cyber Security: Identify and Managing Risks

# Insurance Roundtable

*Cyber Security: Managing and Identifying Risks  
And  
How To Manage Your Cyber Insurance Program*

# Agenda

- 1) Sources and Targets of Cyber Attacks
- 2) How Have You Selected Your Cyber Insurance Policy?
- 3) What Could Be The Impact of a Cyber Attack On You and How Should You Select Coverages?
- 4) What Is A Cyber Breach Response Plan?
- 5) How to Purchase Insurance Effectively

**Preparation and policy language**

# Sources and Targets Of Cyber Attacks?

# Sources and Targets Of Cyber Attacks

- Sources:
  - State sponsored
  - Terrorists
  - Organized Crime Groups
  - Hackers
- Targets
  - **Money – greed driven**
  - Data
  - Terror Mechanism/ Killware/ Political Motivation



How Have You Selected Your Cyber Insurance Policy?

Are you tasked with the responsibility to purchase the cyber insurance to protect your entity?

# How Have You Selected Your Cyber Insurance Policy?

## MOTIVATION

- Protect the entity - late
- Limits
- Lowest premium

## MISSING

- No coverage review
- Limits
- The unverified assumption

# How Have You Selected Your Cyber Insurance Policy?

## MOTIVATION

- Protect the entity
- Limits
- Lowest premium

## MISSING

- No coverage review
- Limits
- The unverified assumption

Which of these factors would be the least important in the event of a claim?



# What Could Be The Impact of a Cyber Attack On You and How Should You Select Coverages?

# What Could Be The Impact of a Cyber Attack On You and How Should You Select Coverages?

## a) Third Party

- i. Network Security and Privacy Liability – failure to protect PII

### ii. Solar Winds Example - liability

## b) First Party Coverage

- i. Reputational Loss and Business Interruption Coverage
- ii. Cyber Extortion and Ransomware Coverage – large threat

### iii. Colonial Pipeline Example – limit?

### iv. Solar Winds Example - Notification and monitoring

## c) Exclusions and Endorsements

- i. Bricking – Merck Example

## d) Read your policies

- i. Commonality but no two policies are created equal
  - i. Example – is profit included or excluded in invoice manipulation example

# What Could Be The Impact of a Cyber Attack On You and How Should You Select Coverages?

## a) Third Party

- i. Network Security and Privacy Liability
- ii. Regulatory Investigations, Fines and Penalties
- iii. Media Liability

### **iv. PCI DSS Assessment Expenses – what's your exposure?**

- v. Breach Management Expenses

## b) First Party Coverage

### **i. Business Interruption – significant exposure**

### **ii. Contingent Business Interruption**

- iii. Digital Asset Destruction, Data Retrieval and System Restoration
- iv. System Failure Coverage
- v. Social Engineering & Cyber Crime Coverage
- vi. Reputational Loss Coverage

### **vii. Cyber Extortion and Ransomware Coverage – large threat – limits and sublimits**

### **viii. Breach Response and Remediation Expenses**

### **ix. Crisis Management Expenses - sublimits**

- x. Court Attendance Costs

## c) Exclusions and Endorsements

- i. War Exclusion and Terrorism Carve Back – discussed later
- ii. Bricking

### **iii. Invoice manipulation – growing trend and wood processing example**

# Additional Coverage Considerations

1. Sublimits and aggregates - your limit may not be what you think it is
  - › Stacked vs Non Stacked Limits – discussed later
2. Deductible selection - motivation
3. Cyber Crime and Treasury – your money – discussed later
4. Insurance and Legal Self Assessment

# Non Stacked and Stacked Limits

## \$3,000,000 AGGREGATE

- \$3M Limit for Breach Event Costs **Inside** the Aggregate
- \$1M limit for Defense - **Inside** the Aggregate.
- \$3M Aggregate - **Inside** the aggregate

## \$5,000,000 AGGREGATE

- \$5M Limit for Breach Event Costs **Outside** the Aggregate
- \$1M limit for Defense - **Outside** the Aggregate
- \$5M Aggregate - **Inside** the aggregate

# Non Stacked and Stacked Limits

## NON STACKED LIMITS

- \$3,000,000 AGGREGATE
  - \$3M Limit for Breach Event Costs **Inside** the Aggregate
  - \$1M limit for Defense - **Inside** the Aggregate.
  - \$3M Aggregate - **Inside** the aggregate

**\$3,000,000 TOTAL  
AVAILABLE LIMIT FOR ONE  
CLAIM**

## STACKED LIMITS

- \$5,000,000 AGGREGATE
  - 5M Limit for Breach Event Costs **Outside** the Aggregate
  - \$1M limit for Defense - **Outside** the Aggregate
  - \$5M Aggregate - **Inside** the aggregate

**\$11,000,000 TOTAL  
AVAILABLE LIMIT FOR ONE  
CLAIM**



# War Exclusion With Cyber Terrorism Carve Back Policy Language

- War Exclusion Cyber Terrorism With Carve back example:

“The Company shall not be liable for any Claim, Damages, Defense Expenses or Loss based upon, arising out of, or in any way attributable to:

**EXCLUDE WAR** - Confiscation, nationalization, requisition, strikes, labor strikes or similar labor actions; war, invasion, or warlike operations, civil war, mutiny, rebellion, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military coup or usurped power.

**INCLUDE TERRORISM** - This exclusion shall not apply to a terrorist event perpetrated by electronic or internet-based applications or means”

- How do you manage this?

# War Exclusion With Cyber Terrorism Carve back

- Policy language and Case Law
  - War exclusions are getting broader
  - Terrorism carve backs
  - Case Law Unsettled territory
  - Case Law Varies by state

# War Exclusion and Terrorism Carve Back Recommendations

- PRE CLAIM
  - Review war exclusion and terrorism carve back
  - Obtain broadest coverage language- no two policies are created equal
- POST CLAIM
  - Do not make assumptions about the source of the cyber attack
  - Review insurance company claim review with qualified legal counsel and an insurance consultant

# What Is A Cyber Breach Response Plan?

# What Is A Cyber Breach Response Plan?

- What partners should be consulted?

# What partners should be consulted for Breach Response?

## UTILITY PROVIDER COMMENT

1. Internal IT
2. External IT vendor
3. Qualified Attorney
4. Insurance Consultant
5. Cyber insurance company
  - › Crisis management coordinator
  - › Their Attorney
6. Accountant
7. Bank treasury



# Half Way Questions



# How To Purchase Insurance Effectively

# How to Purchase Insurance Effectively

- Application Management
  - i. Year long plan
    - i. MFA
    - ii. Data Back Up Plan
    - iii. EDR
- Use Cyber Insurance company scans - below threshold
- Annual Policy Review
- Limit Review
  - Stacked vs non stacked limits
  - Sublimits
- Cyber Crime – next slide
- Cyber Premium and Limit Trends

# Cyber Crime – what is your crime exposure to loss

1. Computer Fraud and Funds Transfer
  2. Social Engineering Fraud
  3. Invoice Manipulation
- Cyber Crime and Commercial Crime policies can overlap

# Cyber Crime – what is your crime exposure to loss

- Computer Fraud and Funds Transfer
  - Maximum cash on hand (\$5,000,000) plus unused line of credit (\$3,000,000) equals \$8,000,000 exposure to loss
- Social Engineering Fraud
  - Largest outgoing payment (\$500,000 exposure to loss)
- Invoice Manipulation
  - Largest outgoing electronic installment (\$350,000 exposure to loss)

End

Questions?