Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

Cyber Liability for Today's Risk Managers

MICHAEL GUZMAN, ARM
ARTHUR J. GALLAGHER & CO.

Today's Agenda

What are we talking about today?

1. Cyber Risk Overview
2. Regulatory Landscape
3. Coverage + Trends
4. Claim Process
5. Recent Breach
6. Recommendations

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

Cyber Risk Overview

Cyber Risk Overview

What is Cyber Risk

The Potential of Economic and Non-Economic Losses arising out of the use of Information Technology Systems

Economic

1. Notification Costs
2. Forensic Costs
3. Data Recovery Costs
4. Business Interruption
5. Legal Expenses
6. Lawsuits

Non-Economic

1. Reputational Damage
2. Supply Chain Relationship Damage

Cyber Risk Overview

Potential Exposures

Cyber Risk

1. Breach of Personal Protected Information (PPI) / Hacker
2. Lost or Stolen Laptop/ Smartphone/ Tablets
3. Employee Negligence/ Human Error/ Rogue Employee
4. Thumb drives / Flash drives
5. Third Party Servers (Dropbox & iCloud)
6. Paper Files
7. Copy Machines

Cyber Risk Overview

Leading Cyber Claims

Top 5 Leading Causes of Cyber Claims
1. Lost employee laptop or other computing devices
2. Malicious acts by a rogue employee or ex-employee
3. Improperly disposed sensitive information
4. Media campaign gone wrong
5. Subcontractor error or omission (including breaches on those subcontracting vendors that are holding your data)

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

Regulatory Landscape

Regulatory Landscape

Complex, Changing, and Challenging

- When a breach occurs, there are many Federal/State and regulatory laws to consider:
  - 47 out of 50 State Laws (Varies from State to State)
  - Health Insurance Portability & Accountability Act (HIPAA)
  - FTC 114: Red Flag Rule
  - Payment Card Industry (PCI) Data Security Standards

Regulatory Landscape

Florida Information Protection Act of 2014

- Gov. Rick Scott signed a bill dramatically changing the State of Florida's data security breach laws.
- The Florida Information Protection Act of 2014 changes the requirements after a data breach and the definition of personal protected information.
- These changes give Florida the broadest and most encompassing breach laws in the nation.

Regulatory Landscape

Florida Information Protection Act of 2014 Summary

FL Definition of Personal Information

1. Social Security Number
2. Driver's License # or FL ID Card #
3. Credit or Debit Card Number
4. Health Insurance Policy or Subscriber #
5. Medical History
6. Financial Information
7. Online User Name or Email Address in combination with their password
8. Online User Names or Email Address in combination with their security question and answer

FL Notification Requirement Changes

1. Provide notification of breach to affected individuals within 30 days.

2. Notice must be provided to the Florida Department of Legal Affairs for any breach affecting 500 or more individuals.

3. Must provide the Florida Attorney General with a copy of an incident or forensic report along with a copy of the company's data breach policies and procedures.

Regulatory Landscape

Sovereign Immunity and Tort Caps

- 1st Party Coverage (Not Covered by Sovereign Immunity)
  - Crisis Management (Notification cost, Credit Monitoring, etc.)
  - Data Recovery
  - Business Interruption
  - Cyber Extortion

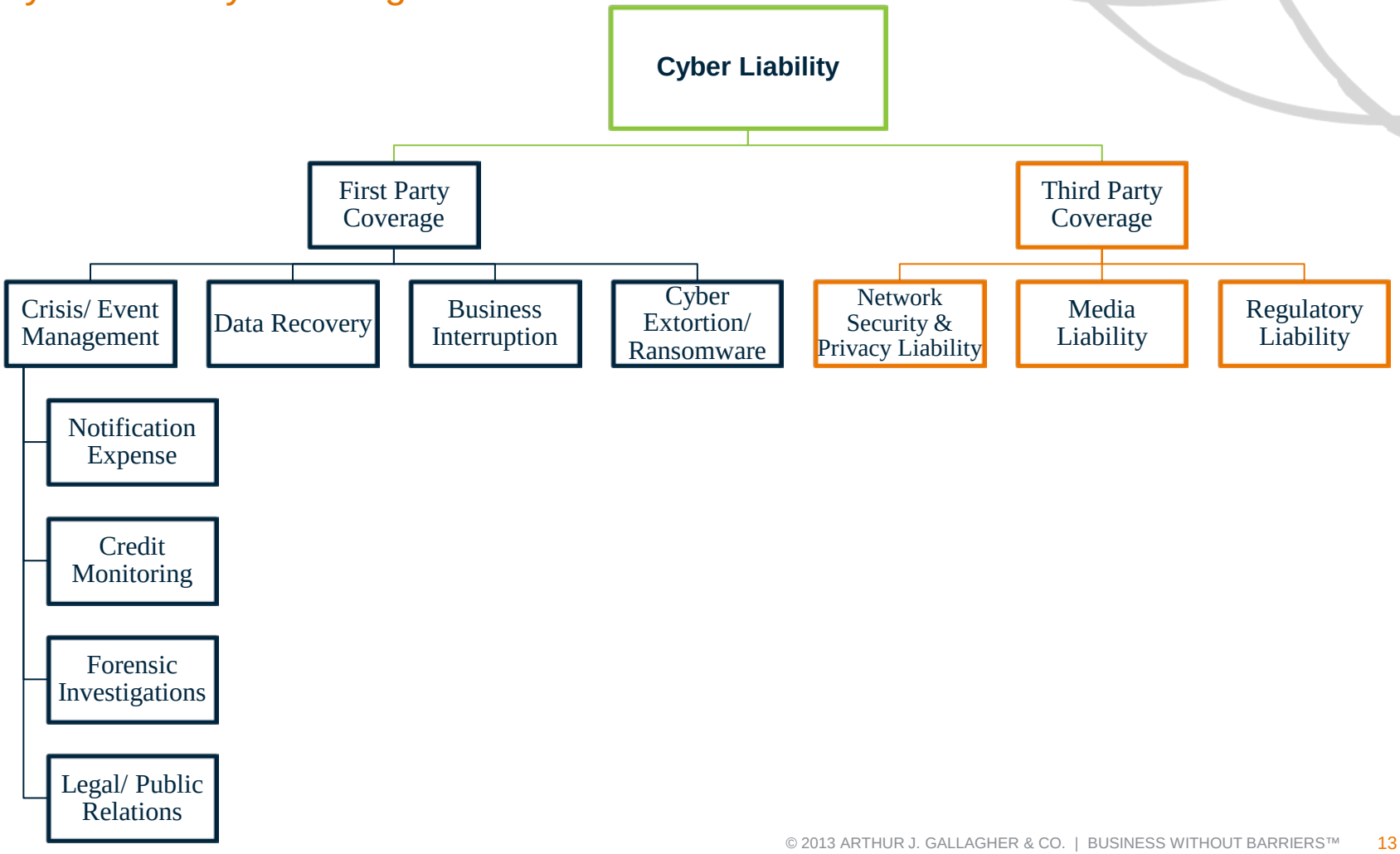
- 3rd Party Coverage (Has yet to be tested)
  - Network & Security Liability
  - Privacy Liability
  - Media Liability
  - Regulatory Liability

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

Cyber Coverage + Trends

Cyber Coverage + Trends

Cyber Liability Coverage



Cyber Liability Coverage

1st Party Coverage

Crisis Management

1. Notification Cost
2. Credit monitoring
3. Call center to handle inquiries
4. Identity fraud expense reimbursement
5. Public relations services to mitigate negative publicity
6. Forensic costs incurred to determine the scope of the network failure and determine whose information was breached
7. Breach Coach and Legal Assistance to handle the event and determine which regulatory bodies need to be notified

Cyber Liability Coverage

1st Party Coverage

Data Recovery

Expenses incurred to restore data lost from an unauthorized access or virus to an information system

Business Interruption

Loss of income and extra expense incurred to restore operations, as result of a computer system disruption caused by a virus or other unauthorized computer attack

Cyber Extortion/ Ransomware

Money paid due to threats made regarding an intent to fraudulently transfer funds, destroy data, introduce a virus or attack on computer system, or disclose electronic data/information

Cyber Liability Coverage

3rd Party Coverage

Network Security & Privacy Liability

Liability coverage for failing to prevent a security breach and protect personal information.

Media Liability

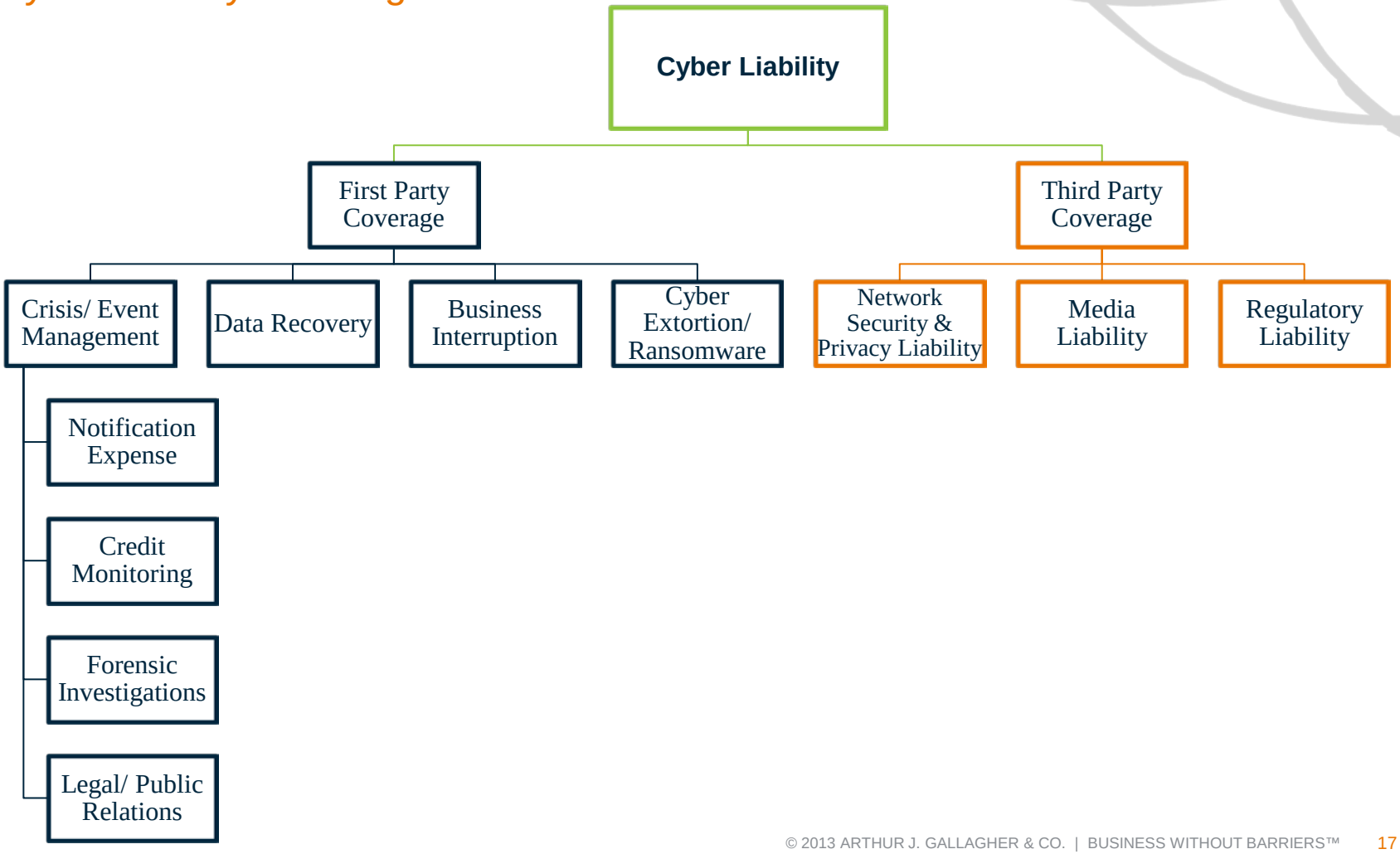
Intellectual Property and Personal Injury liability from an error or omission in content (website, electronic publishing, etc.)

Regulatory Liability

Coverage for lawsuits or investigations by Federal, State, or Foreign regulators relating to Privacy Laws

Cyber Coverage + Trends

Cyber Liability Coverage



Cyber Coverage + Trends

Carrier Vendor Benefits

Crisis/ Event Management

1. Notification & Call Centers
2. Credit Monitoring Vendor
3. Forensic Investigator
4. Legal/ Breach Coach
5. Public Relations Firm

Approved Vendor Panel

Pre - Negotiated Rates

Cyber Coverage + Trends

Cost of a Data Breach

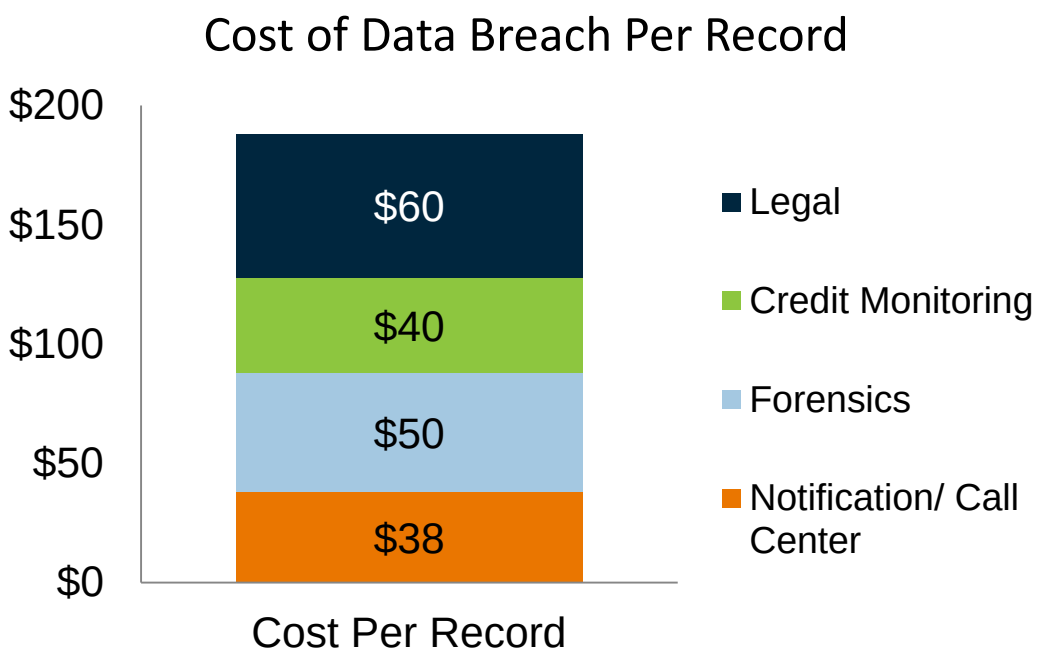
- Ponemon Institute, LLC conducted a study on the cost of a data breach.

What could a cyber breach cost you?

$188 - $194
Average cost per record (includes response costs, credit monitoring, forensics, and breach coach).

$5.4 Million
Average total cost per breach.

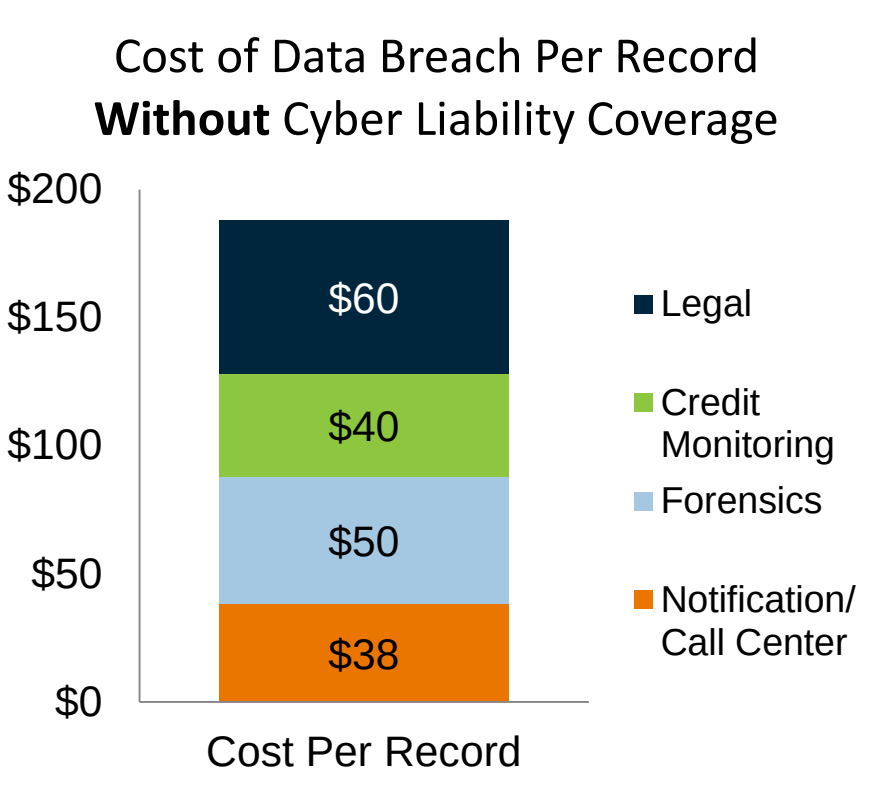
**2013 Annual Study: U.S. Cost of Data Breach—by The Ponemon Institute, LLC; Sponsored by Symantec*

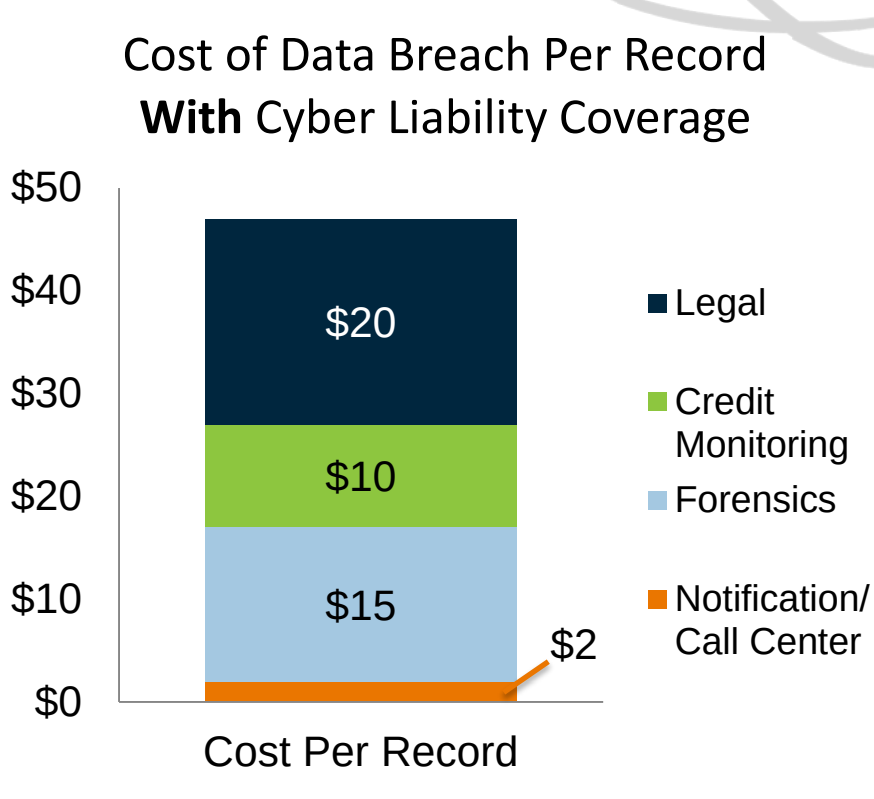


*Cost can vary depending on vendor.

Cyber Coverage + Trends

Cost of a Data Breach with Cyber Liability Coverage





*Please note these are estimated numbers and will vary depending on each carrier.

Arthur J. Gallagher & Co.

BUSINESS WITHOUT BARRIERS™

Claim Process

Cyber Claim Process

How would coverage respond in the event of a breach

#1
- Notify the Cyber Liability carrier once your organization is made aware of a possible breach

#2
- The carrier will assign a Breach Coach to your organization who will help you select the proper breach counsel and forensic team.

#3
- The Breach Coach and your organization will select a notification service provider to notify the affected individuals ensuring all regulatory requirements are met.

#4
- Your organization will approve the notification letters to be mailed to the affected individuals.

#5
- The Breach Coach will contract a call center service provider to handle any questions on your organization's behalf.

#6
- Affected individuals receive their notification letters and may enroll in the credit monitoring service.

#7
- Your organization will receive reports on the progress of the notification letters and credit monitoring enrollment for continuous monitoring of the event.

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

Recent Cyber Breach

Recent Cyber Breach

Anthem Breach

- On February 5th, 2015 the second largest health insurer, Anthem, announced hackers gained access to their servers on 1/27/2015
- Up to 80 million individuals affected across all Anthem product lines
- Credit Monitoring is being offered to all affected individuals

Recent Cyber Breach

Anthem Breach. What it means for affected employers

Organizations Potential Affected by Anthem

1. Involve key personnel and legal counsel to determine if your organization was affected.
    - Please note the age of the breached information is currently unknown. Older data exchanged with Anthem could be involved.
2. If potential affected, speak with Anthem to provide guidance and determine who is responsible to notify the affected individuals.
3. Monitor the situation closely and actively communicate any progress with employees.
    - Direct employees to athemfacts.com for any questions, clarification, and to enroll in credit monitoring

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

Cyber Recommendations

Cyber Recommendations

Additional Insured

- Named Additional Insureds
  - Will vary depending on the client and carrier
  - Majority of Cyber carriers will not add additional insureds
- Ensure Vicarious Liability Coverage
  - Vendors legally responsible for information on behalf of your organization

Cyber Recommendations

Vendor Requirements

Recommended Cyber Liability Vendor Requirements

Vendors should provide evidence of the following requirements, via Certificate(s) of Insurance, prior to commencement of awarded contract.

1. Vicarious Liability
2. Network Security / Privacy Liability –$1M Minimum Aggregate Limit
3. Breach Response Sublimit - At least 50% of the aggregate
4. Technology Products E&O (If Applicable) - $1M Minimum Aggregate Limit
5. Claims-made policies must be in place for a period of at least 12 months after the contract completion/ termination date.
6. Carrier A.M. Best rating of at A- VI or better

Cyber Recommendations

Gallagher Cyber Liability Recommendations

Personal Identifiable Information Definition

Any nonpublic personal information defined in Privacy Regulations including foreign, state, local, or foreign statue or regulations. Such as:

1. HIPAA or HITECH
2. Gramm-Leach-Bliley Act
3. Federal, State, Local data breach regulations
4. Identity Theft Red Flags under FACTA
5. Federal Fair Credit Reporting Act
6. Privacy Protection Regulations or laws adopted by countries outside the United States.

Cyber Recommendations

Gallagher Cyber Liability Recommendations

Named Insured/ Employee Definition

1. Any past, present or future principal, partner, officer, director, trustee, employee, leased employee, or temporary employee

2. Independent Contractors – only to the duties on behalf of your organization

3. Volunteers (crucial for public entities)

Cyber Recommendations

Gallagher Cyber Liability Recommendations

Portable Media

1. Ensure Portable Media is included under the computer system definition – Laptops, Cell Phones, Flash Drives, etc.

2. Remove Unencrypted Portable Media Exclusion – Excludes losses involving any unencrypted portable media device (i.e. Flash Drives)

Cyber Recommendations

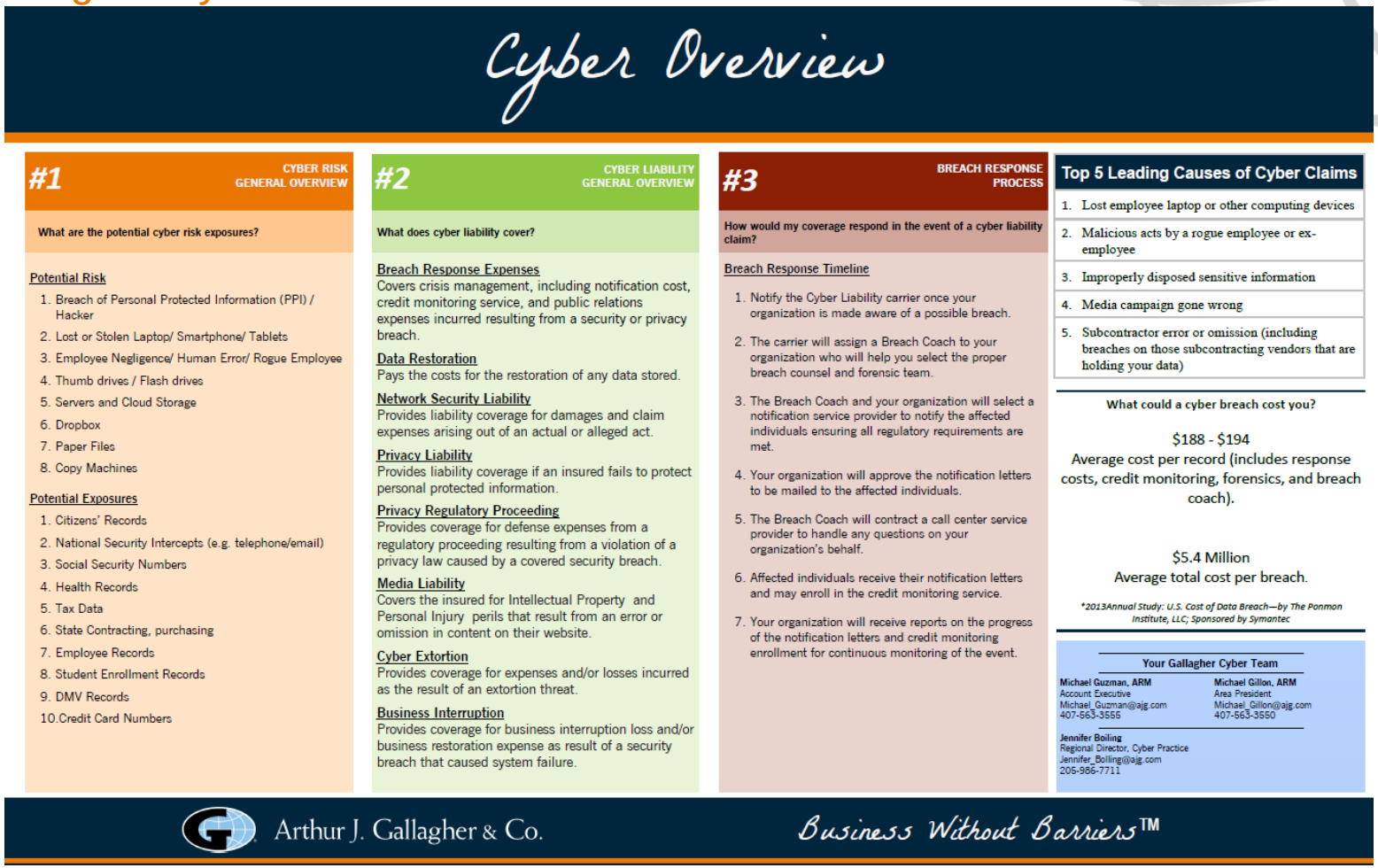
Gallagher Cyber Liability Recommendations

Participate in the Carrier On-Boarding Call

1. How coverage is triggered
2. How to report a claim
3. Explanation of the claim process
4. Carrier Vendor Panel Discussion
5. Vendor Responsibilities
6. Other Q&A you may have

Cyber Recommendations

Gallagher Cyber Handouts



Cyber Overview

#1 CYBER RISK GENERAL OVERVIEW

What are the potential cyber risk exposures?

Potential Risk

1. Breach of Personal Protected Information (PPI) / Hacker
2. Lost or Stolen Laptop/ Smartphone/ Tablets
3. Employee Negligence/ Human Error/ Rogue Employee
4. Thumb drives / Flash drives
5. Servers and Cloud Storage
6. Dropbox
7. Paper Files
8. Copy Machines

Potential Exposures

1. Citizens' Records
2. National Security Intercepts (e.g. telephone/email)
3. Social Security Numbers
4. Health Records
5. Tax Data
6. State Contracting, purchasing
7. Employee Records
8. Student Enrollment Records
9. DMV Records
10. Credit Card Numbers

#2 CYBER LIABILITY GENERAL OVERVIEW

What does cyber liability cover?

Breach Response Expenses
Covers crisis management, including notification cost, credit monitoring service, and public relations expenses incurred resulting from a security or privacy breach.

Data Restoration
Pays the costs for the restoration of any data stored.

Network Security Liability
Provides liability coverage for damages and claim expenses arising out of an actual or alleged act.

Privacy Liability
Provides liability coverage if an insured fails to protect personal protected information.

Privacy Regulatory Proceeding
Provides coverage for defense expenses from a regulatory proceeding resulting from a violation of a privacy law caused by a covered security breach.

Media Liability
Covers the insured for Intellectual Property and Personal Injury perils that result from an error or omission in content on their website.

Cyber Extortion
Provides coverage for expenses and/or losses incurred as the result of an extortion threat.

Business Interruption
Provides coverage for business interruption loss and/or business restoration expense as result of a security breach that caused system failure.

#3 BREACH RESPONSE PROCESS

How would my coverage respond in the event of a cyber liability claim?

Breach Response Timeline

1. Notify the Cyber Liability carrier once your organization is made aware of a possible breach.
2. The carrier will assign a Breach Coach to your organization who will help you select the proper breach counsel and forensic team.
3. The Breach Coach and your organization will select a notification service provider to notify the affected individuals ensuring all regulatory requirements are met.
4. Your organization will approve the notification letters to be mailed to the affected individuals.
5. The Breach Coach will contract a call center service provider to handle any questions on your organization's behalf.
6. Affected individuals receive their notification letters and may enroll in the credit monitoring service.
7. Your organization will receive reports on the progress of the notification letters and credit monitoring enrollment for continuous monitoring of the event.

Top 5 Leading Causes of Cyber Claims

1. Lost employee laptop or other computing devices
2. Malicious acts by a rogue employee or ex-employee
3. Improperly disposed sensitive information
4. Media campaign gone wrong
5. Subcontractor error or omission (including breaches on those subcontracting vendors that are holding your data)

What could a cyber breach cost you?

$188 - $194
Average cost per record (includes response costs, credit monitoring, forensics, and breach coach).

$5.4 Million
Average total cost per breach.

**2013Annual Study: U.S. Cost of Data Breach—by The Ponmon Institute, LLC; Sponsored by Symantec*

Your Gallagher Cyber Team

Michael Guzman, ARM
Account Executive
Michael_Guzman@ajg.com
407-563-3555

Michael Gillon, ARM
Area President
Michael_Gillon@ajg.com
407-563-3550

Jennifer Boiling
Regional Director, Cyber Practice
Jennifer_Boiling@ajg.com
205-986-7711

Arthur J. Gallagher & Co.

Business Without Barriers™

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

Thank You

Michael Guzman, ARM
Arthur J. Gallagher Risk Management Services, Inc.
200 South Orange Avenue | Suite 1350
Orlando | FL | 32801