The Ever-changing Landscape of Cyber Risk

Prepared by Matt Gullickson | Senior Account Executive – Cyber Liability Practice

We would like to emphasize that this document is only provided for educational purposes and does not constitute legal advice. We highly recommend that you seek the advice of legal counsel in order to become fully apprised of the legal implications related to these issues.

Gallagher

Insurance | Risk Management | Consulting

Meeting Agenda

Gallagher
Insurance | Risk Management | Consulting

- Cyber Risk; what is it and why is it a concern?
- Claim and Loss Trends
- Information Security Best Practices
- Cyber Liability Insurance Policy Overview
- Coverage Considerations

Define Protected Information

Challenge = identifying information that is held to a higher standard of care

– Information protected by law (i.e. personally identifiable or protected health information)

- Examples:
  - State Privacy and Consumer Protection Laws
  - Federal Trade Commission Act
  - HIPAA/HITECH
  - Gramm-Leach Bliley, etc.
  - European Union General Data Protection Rule

- Information required to be kept confidential by contract (i.e. corporate confidential information)
  - Examples:
    - Non-Disclosure Agreements
    - Merchant Services Agreements

The Legal Landscape

Understanding why Cyber-Risk exists

Current Regulations

- **All 50 States have Privacy Laws**
  - State Attorney Generals have been very active in bringing action against affected organizations
- Federal regulators are also **heavily involved**
  - Examples: FTC, Office of Civil Rights, etc.
- **Contractual obligations** can also apply
  - Merchant Service Agreements, Non-Disclosure Agreements, Etc.
- New regulations are **always in the works**
  - EU General Data Protection Regulation
    - Effective as of May 25th, 2018
    - Applies to any organization that collects, processes or stores the information of EU residents
      - Broad Definition of Protected Information ; Simply having an EU-facing website can put an organization in the scope of GDPR
      - Includes strict data management and breach prevention requirements
    - Allows for penalties to be assessed against non-compliant organizations up to the greater of 20,000,000 or 4% of global annual "turnover" (re: gross income)
    - Action can be brought for failure to comply, regardless of if data has been affected.

Items of Note

- **Multiple laws can apply at the same time** and the organization is expected to comply with each applicable regulation
  - The application of laws is often times **dependent upon the residency of the affected individual**
- Many laws establish that transfer of information to a 3rd party **does not constitute the transfer of liability**
  - The "originating" organization is considered the "Data Owner" and therefore responsible for notification if compromised while in the care of a 3rd party (e.g. cloud storage, payroll administrator, etc.)
- There are **numerous inconsistencies** among Privacy Laws
  - Differences in **defining** "protected information"
    - **Typically** includes a Name + social security number, state ID or Driver's License number, and financial account number with access code
    - Some states **are broader** than others and include biometric information, health insurance and medical information, and e-mail addresses/usernames with passwords
  - Reporting requirements **vary**
    - Example: Some states require the Attorney General be notified, others don't have this stipulations

Gallagher
Insurance | Risk Management | Consulting

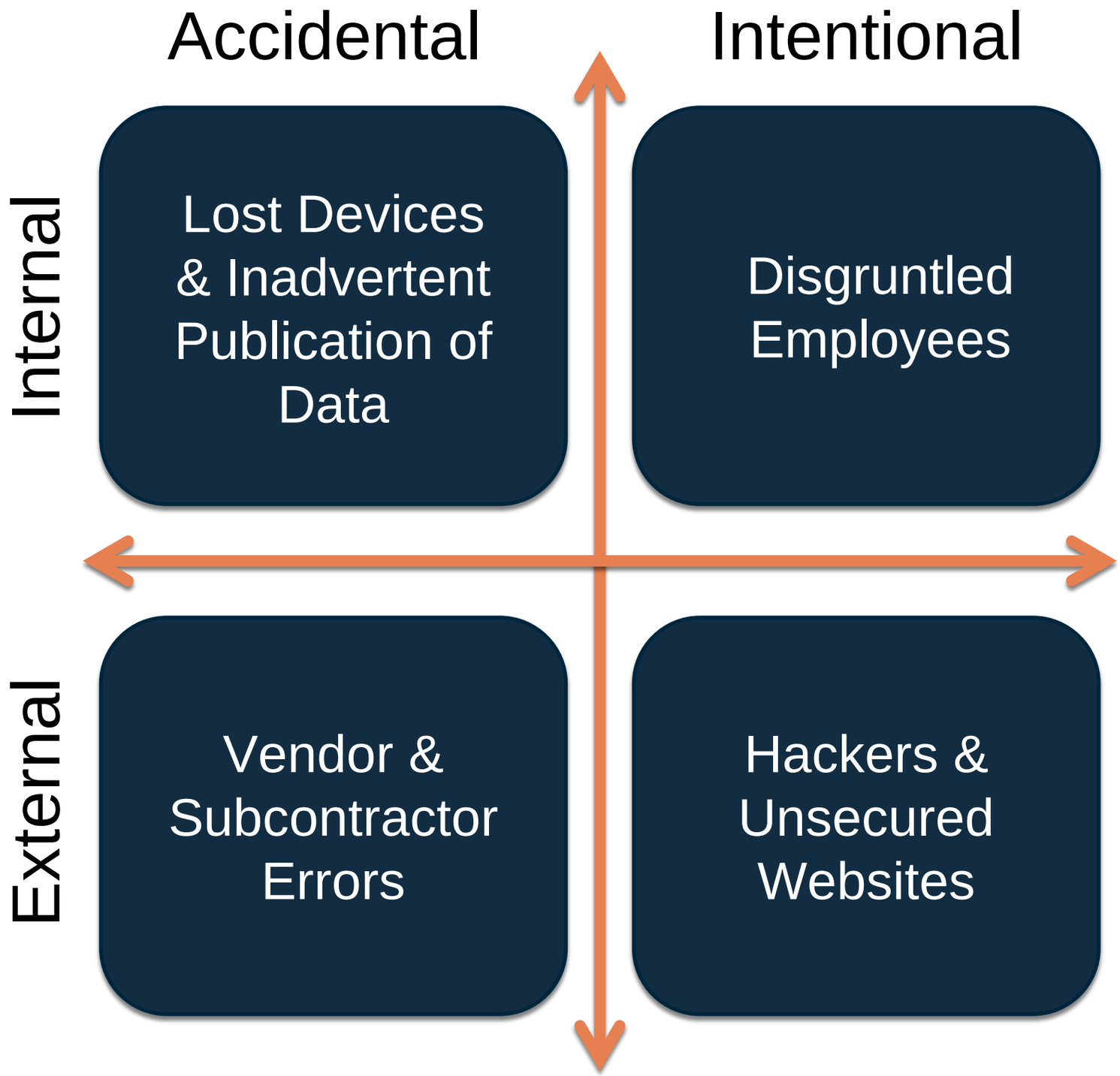
Gallagher

Insurance | Risk Management | Consulting

Claim and Loss Trends

Claim and Loss Trends

Organizations face a number of internal and external threats



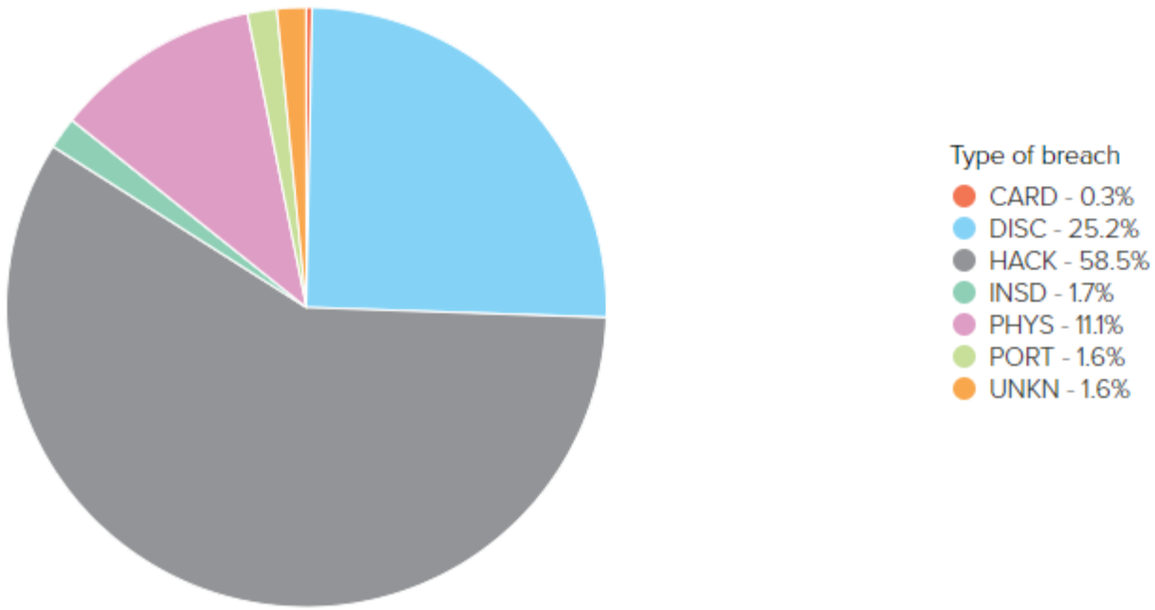
Gallagher

Insurance | Risk Management | Consulting

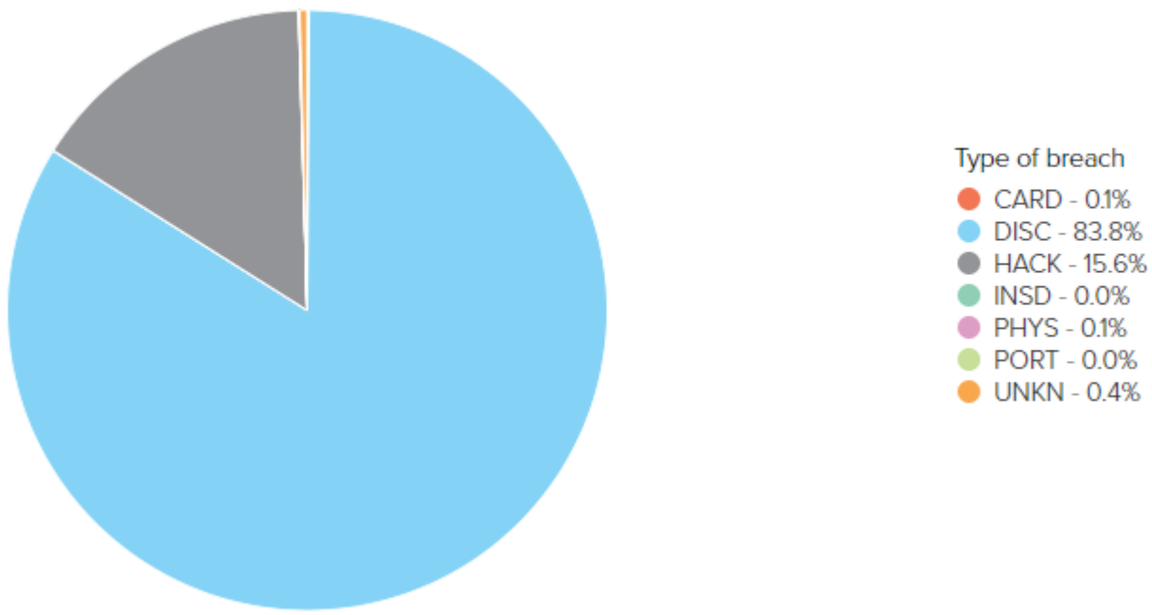
Claim and Loss Trends

Most common causes of a breach and records affected in 2017

ANNUAL PERCENT AND NUMBER OF TOTAL BREACHES BY TYPE



ANNUAL PERCENT AND NUMBER OF RECORDS BREACHED BY TYPE



Summary	
Year	2017
Breaches Made Public	638
Total Affected Records:	1,926,360,102

Source: www.privacyrights.org

Gallagher

Insurance | Risk Management | Consulting

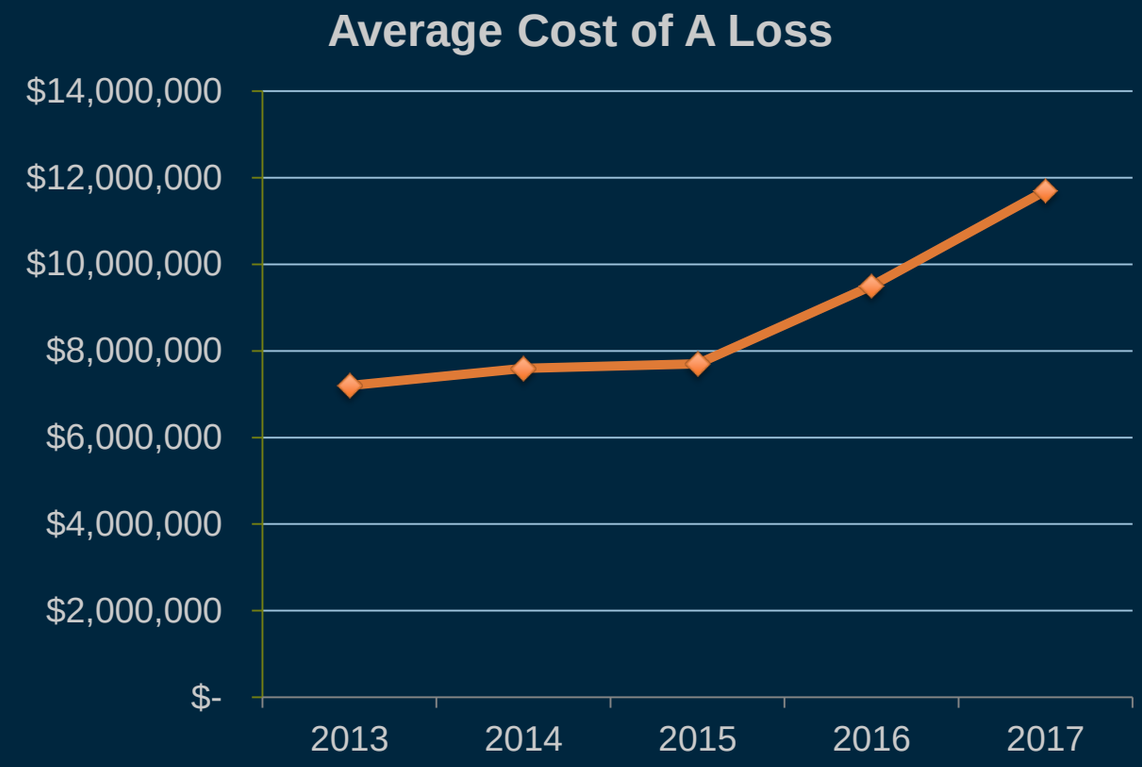
Claim and Loss Trends

A year-over-year comparison

Cyber Claims Frequency

- The frequency of cyber attacks has increased after a few years of relative stability
- The shifting mix of claims has many carriers concerned about future claim costs trending upward
- Chart only reflects reported incidents; high probability that more actually occurred
- **Source:** Advisen (As of Oct. 2017)

Cost of a Claim Year over Year



- Please note that the Ponemon Institute includes a variety of costs in their calculations. In general, Advisen defines the costs associated with a Cyber Incident more broadly than others – including the insurers.
- The cost of a breach depends heavily on the type of information affected; information subject to a higher degree of care/stricter regulations cost more than less regulated data
- **Source:** Advisen (As of Oct. 2017)

Examples of Education Data Breaches

- **South Washington County School District – Unintentional Disclosure**
  - Personal information on approximately 9,600 students and families were sent out mistakenly by an employee as part of a back-to-school e-mail
- **Langston Hughes Young Explorers Academy – Physical Disclosure**
  - Papers containing private medical information and social security numbers of students were left fully exposed in the street
- **Nazareth Area School District – Hack**
  - Private data was compromised after a student hacked into the school's system and download sensitive information on to a USB thumb drive
- **Park Hill School District – Malicious Insider**
  - The District informed current and former employees that a former employee downloaded employment files on to an external hard drive without authorization. The information included social security numbers.

Why should we be concerned?

Gallagher
Insurance | Risk Management | Consulting

Tangible Costs

Investigation Expenses (ex. legal counsel, forensics, notification, and public relations)

Defense expenses and Legal Damages

Business Interruption and Extra Expenses

Ransom Payments

Damage to Data/Recovery Expenses

Regulatory Fines, Penalties and Assessments

Gallagher

Insurance | Risk Management | Consulting

Information Security Recommended Best Practices

Build a Culture of Awareness

It takes a village…

Gallagher

Insurance | Risk Management | Consulting

Management Team

- Understand the organization's goals and operations
- Establish enterprise-wide policies and procedures
- Set an example for employees to follow (encourage skepticism)

Legal/Risk Management

- Works with Management to evaluate and adhere to compliance requirements
- Review contractual liability and indemnification exposures
- Work with IT when reviewing formal engagements with 3rd party providers

Human Resources

- Review controls for managing employee data
- Implement privacy policies in employee handbook
- Work with IT and Legal to establish protocols for terminating network access for former employees

I.T./Technology Team

- Responsible for implementing network safeguards
- Team with Legal to vet controls of 3rd party providers collecting, storing, or accessing data on behalf of the organization
- Work with Legal and Human Resources to limit employee access privilege/terminate privilege of former employees

Employees

- First line of defense
- Participate in employee training to become aware of company best practices

Understand your compliance requirements

Gallagher

PCI-DSS / Regulatory Compliance

- Payment Card Industry Data Security Standards
- Federal Regulations
- State Laws

Cyber Security Readiness

- Network Assessments
- Remediation of Vulnerabilities

Treatment of Private / Confidential Information

- Policies, Access Controls, Security Measures
- Quantification of Record Count / Transactions
- Encryption – At Rest, In Transit, On Portable Media Devices

Breach Preparation

- Incident Response Plan
- Business Continuity Plan / Back-up Procedures

Vendor Management

- Contract Review
- Professional E&O / Cyber Insurance and Indemnification Agreement

Gallagher

Insurance | Risk Management | Consulting

Available Coverages

Types of Coverage

A Cyber Policy is designed to protect the organization in a variety of situations

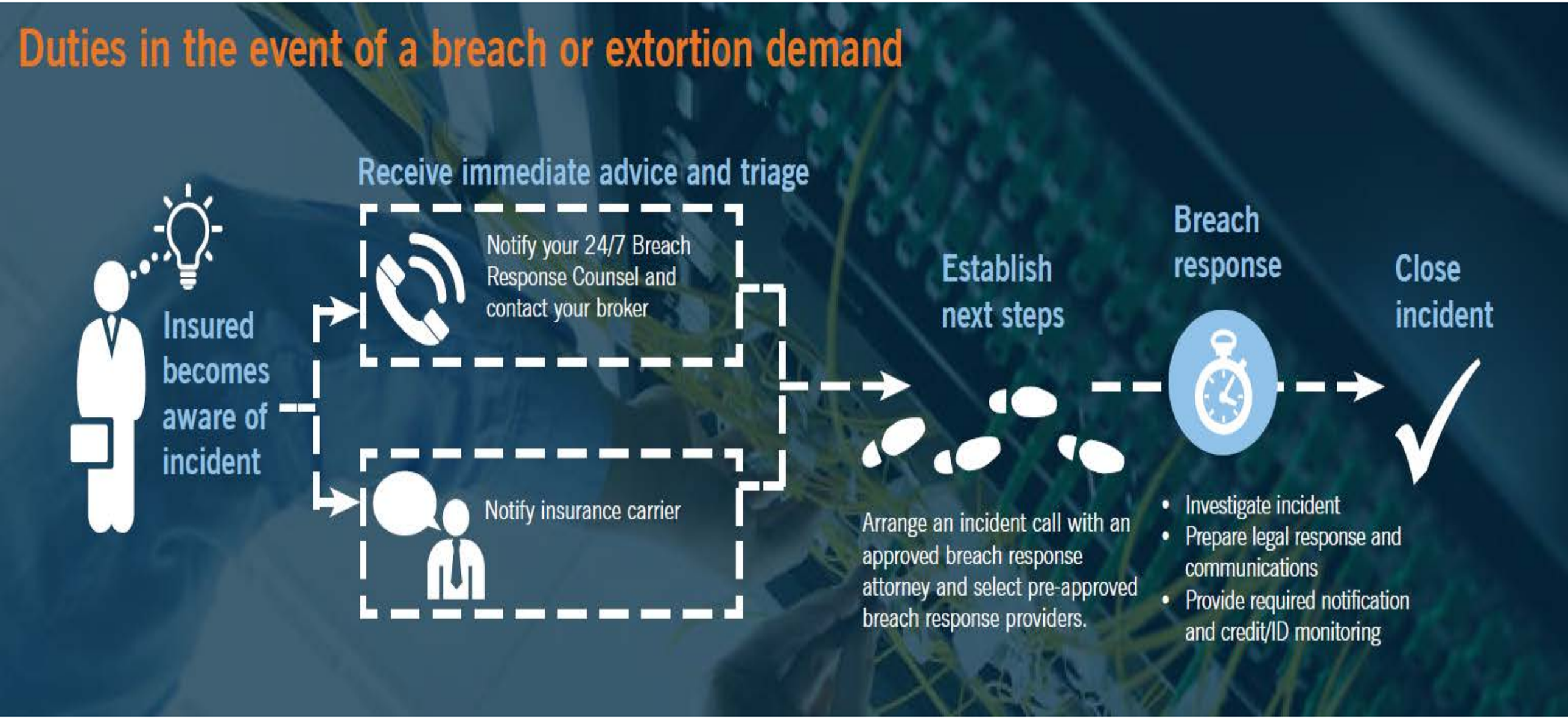
- **3 Types of Insuring Agreements:**
  - **3rd Party Liability Coverages** – provides coverage for claims brought by an independent third party (defense expenses and damages)
  - **Event Management/Incident Response** – provides coverage for the expenses incurred to investigate an incident and comply with privacy notification requirements
  - **1st Party Loss Coverages** – indemnifies the insured for expenses incurred in responding to an incident
- **Coverage is "Claims Made"**
  - Policies will only apply to incidents occurring during the policy term

Available Coverages

Insuring Agreement	Description
3rd Party Liability Coverage	Coverage for defense expenses; settlements & damages; and, where insurable by law, fines & penalties
Network Security Liability	Coverage for defense expenses and damages resulting from allegations by a 3rd party that an Insured's Computer System fails to prevent a Security Breach
Privacy Liability	Coverage for defense expenses and damages resulting from allegations by a 3rd party that an Insured fails to protect electronic or non-electronic information in their care custody and control
Media Liability	Coverage for defense expenses and damages resulting from allegations that an Insured, through the distribution of media content, infringed upon a 3rd party's Intellectual Property rights (*excluding patents)* or caused Personal Injury – coverage available for either content in any format (multimedia) or electronic only.
Regulatory Defense & Penalties *Penalties Included Where Insurable By Law*	Coverage for lawsuits or investigations by Federal, State, or Foreign regulators relating to the violation of applicable Privacy Laws, Regulations, and Statutes
Payment Card Industry Assessments & Penalties	Coverage for assessments, fines and penalties owed under the terms of a Merchant Services Agreement due to non-compliance with the Payment Card Industry Data Security Standard (PCI-DSS) which lead to the compromise of debit & credit card information
Incident Response Coverage	Coverage for Insured's expenses related to investigating and responding to a data compromise
Legal Expenses	Insured's expenses to engage Privacy Counsel to advise and guide organization on complying with applicable Privacy Regulations and Statutes
Notification Expense	Insured's expenses to notify affected individuals as required by applicable Privacy Regulations and Statutes
Credit /ID Monitoring	Insured's expenses to offer Credit or Identity Monitoring Services to affected individuals
Forensic Investigations	Insured's expenses to engage an IT Forensics Firm investigate a system intrusion into an Insured Computer System
Public Relations/Crisis Management	Insured's expenses to hire a Public Relations firm to assist in mitigating damage to the organization's reputation and engage a Call Center to address questions from individuals that have received notification letters
1st Party Loss Coverage	Coverage for Insured's losses resulting from to a network-security event
Cyber Extortion	Incurred expenses related to a threat and ransom demand made by a 3rd party to attack an Insured's Computer System
Digital Asset Restoration	Incurred expenses related to investigating the ability to and, if possible, restore an Insured's electronic data damaged by a Malicious Attack to its pre-loss state (or as close as possible)
Insured's Network Security Failure Income Loss	Profit loss and extra expenses resulting from a **failure of network security (e.g. virus or hacker)** that impairs business-critical Computer System(s) under the **Insured's** direct operation and control

Incident Response Process Overview

Cyber policies can make for a more efficient investigation



Gallagher

Insurance | Risk Management | Consulting

Gallagher

Insurance | Risk Management | Consulting

Avoiding Coverage Conflicts

Avoiding Coverage Conflicts

Duplication of Coverage Issues

Gallagher
Insurance | Risk Management | Consulting

- Multiple policies may respond to a cyber incident
- Cyber policies typically respond first to cover the investigation, but will hand off litigation to another policy
- **Amend the Other Insurance Clause**
  - Identify overlaps and structure the program accordingly

Coverage & Gaps

	Property	General Liability	Crime / Bond	K&R	E&O	Cyber
1st Party Privacy / Network Risks						
Physical damage to Data only						
Virus / Hacker damage to Data only						
Denial of service attack						
B.I. Loss from security event						
Extortion or threat						
Employee sabotage of Data only						
3rd Party Privacy / Network Risks						
Theft / Disclosure of private info.						
Confidential corporate info. breach						
Technology E&O						
Media Liability (electronic content)						
Privacy breach expense / notification						
Damage to 3rd party's Data only						
Regulatory privacy defense / fines						
Virus / Malicious code transmission						

Coverage Provided?	
Coverage Possible?	
No Coverage?	

** For reference and discussion only; policy language and facts of claim will require further analysis*

Avoiding Coverage Conflicts

Misunderstood Exclusions

Gallagher
Insurance | Risk Management | Consulting

- **War and Terrorism**
  - Carriers will not remove the war exclusion
  - Inconsistent Carrier Approach
- **Potential Resolutions**
  - **Approach #1:**
    - War exclusion does not make reference to “Terrorism” and “Acts of Foreign Enemies”
    - Cyberterrorism coverage is granted (definitions of Cyberterrorism are inconsistent)
  - **Approach #2:**
    - War exclusion references “Acts of Foreign Enemies”
    - Cyberterrorism coverage is granted (definitions of Cyberterrorism are inconsistent)
    - An additional carveout is for Cyberterrorism is also granted to add clarity of intent
  - **Approach #3:**
    - War exclusion references “Terrorism” and “Acts of Foreign Enemies”
    - War & Terrorism exclusion adds a carveout for Cyberterrorism to add clarity of intent
    - Cyberterrorism coverage is defined broadly
  - **Approach #4:**
    - War exclusion references “Terrorism” and “Acts of Foreign Enemies”
    - War & Terrorism exclusion adds a carveout for acts perpetrated electronically

Avoiding Coverage Conflicts

Misunderstood Exclusions

Gallagher
Insurance | Risk Management | Consulting

- **Prior Acts (Retro Dates) & Prior Circumstances**
  - Dispute over actions that happened prior to the retroactive date being covered under cyber polices
  - The Prior Circumstance exclusion IS NOT a prior act exclusion
    - However, the exclusion is interpreted by some to test for knowledge of circumstances that can give rise to a claim.
- **Potential Resolutions**
  - Always try to limit knowledge to the highest managerial level position
  - In Cyber, the CIO/CISO will often be considered for knowledge

Avoiding Coverage Conflicts

Misunderstood Exclusions

Gallagher
Insurance | Risk Management | Consulting

- **Bodily Injury & Property Damage Exclusion**
  - Cyber polices often afford coverage to Financial Loss
  - Data Recovery may have a carveback (e.g., Intellectual Property is not Physical Property)
  - What about the Unauthorized access exclusion in the GL policy
  - Internet of Things (IoT) and Artificial Intelligence
- **When it comes to losses involving data, hardware, media, and other property;**
  - Remember your non-cyber policies.
  - Numerous all risk property policies have been found to apply to computer-related loss including viruses.
  - General Liability insurance may also respond to class action litigation alleging violation of rights of privacy or property damage.
    - Portal Health decision by Fourth Circuit underscores this: inadvertent disclosure of sensitive health information resulting in class action suit covered by CGL policy. However, the “unauthorized access” exclusions can preclude coverage for losses occurring after 2015

Avoiding Coverage Conflicts

Misunderstood Conditions and Definitions

Gallagher
Insurance | Risk Management | Consulting

- **Older polices may bury clauses to maintain systems at the same level as underwritten**
  - Failure to maintain an ambiguous “appropriate” level of network security can result in declination of coverage
  - Typically found in endorsements added on to CGL, E&O, and Property Policies
- **Notice provisions require timeliness**
  - Carriers typically have different requirements for different agreements
    - Example: “as soon as practical” for liability claims vs. 10 days for cyber extortion
- **Applications can be made part of the policy**
  - Many questions phrased as “Yes/No” and can be grey
  - Attaching an addendum with clarifying answers can be beneficial as your statements may be used against you to contest coverage
- **Computer System Definition:**
  - Are Cloud Providers and other Independent Contractors covered?
  - Mobile Devices / thumb drives / unconnected PCs

Avoiding Coverage Conflicts

Misunderstood Conditions and Definitions

Gallagher
Insurance | Risk Management | Consulting

- **Pre-Approval of Vendors before engagement of Breach Response Services**
  - All carriers have pre-approved vendor panels in place for use under the policy
  - Some carriers will consider adding additional vendors while others won't
  - Failure to obtain approval before engaging a provider can result in a denial or limitation of coverage
- **Defense Costs – Pre-Approval issues**
  - Similar to breach response, carriers have pre-approved panels in place
  - Not all carriers cover pre-claim defense costs or limit the scope of covered expenses
- **Subsidiary Definition:**
  - Are Partnerships and Joint Ventures covered?
  - Is there a timeframe to report new acquisitions?

Gallagher

Insurance | Risk Management | Consulting

Please Contact Me With Questions

Matt Gullickson
Senior Account Executive
Matt_Gullickson@ajg.com
Phone: 312-416-6821
300 S. Riverside Plaza, Suite 1500
Chicago, IL 60606