

CRA Charles River
Associates

 Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

VedderPrice

beazley beautifully
designed
insurance

Cybersecurity & Risk Strategies

ARTHUR J GALLAGHER & CO. | BEAZLEY | CHARLES RIVER ASSOCIATES | VEDDER PRICE

Agenda

- Compliance Environment
- IT Security Best Practices and Insurance Impact
- Cyber Threat Trends
- Evolution of Cyber Insurance
- Cyber Risk Management

CRA Charles River
Associates

VedderPrice



Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

beazley beautifully
designed
insurance

Compliance Environment

State Regulatory Environment

48 out of 50 States

- A vast majority of US states have consumer protection statutes that address the safeguarding on consumer data

Personally Identifiable Information (PII)

- Protected / “Sensitive” information is defined differently in each state but there are common characteristics.

Data Owner vs. Data Aggregator

- Transfer of data to a third party does not constitute a shift in responsibility

Data Breach Victim’s State Residency Governs

Regulatory Testing Grounds

- California, Illinois, Massachusetts, New York

Federal, Foreign & Industry Regulatory Environment

Foreign Regulations

- GDPR becomes effective May 2018
- Chinese Cybersecurity Law

FTC

- Bureau of Consumer Protection
- Division of Privacy & Identity Protection
- Federal Trade Commission Act (15 U.S.C. 41, et seq.) – “unfair or deceptive acts or practices”

Payment Card Industry (PCI)

- PCI-DSS
- Merchant Service Agreement

Contractual Obligations

- NDA / Confidentiality
- Insurance Requirements

CRA Charles River
Associates

 Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

VedderPrice

beazley beautifully
designed
insurance

IT Security Best Practices and Insurance Impact

Best Practices

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

CRA Charles River
Associates



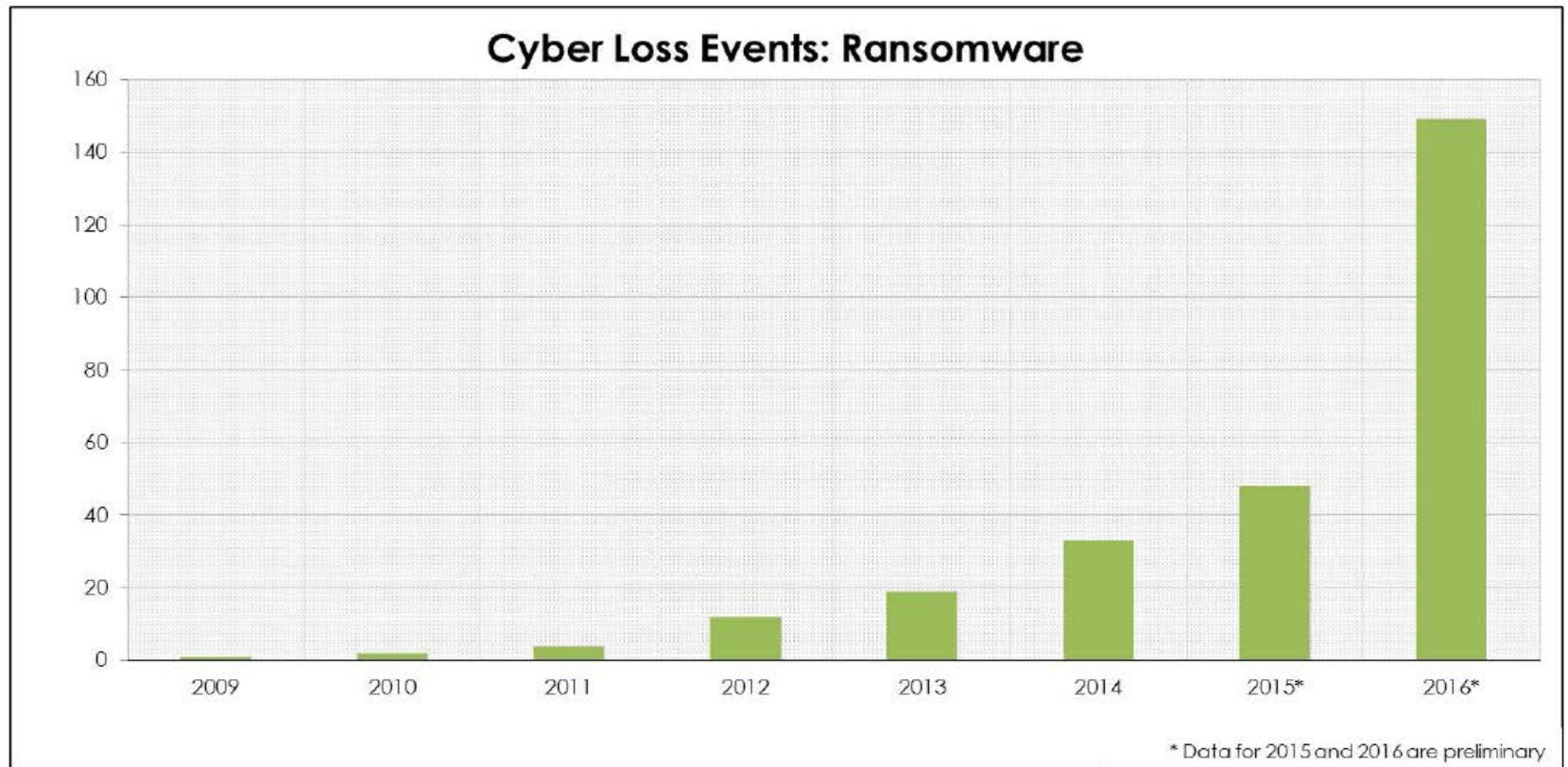
Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

VedderPrice

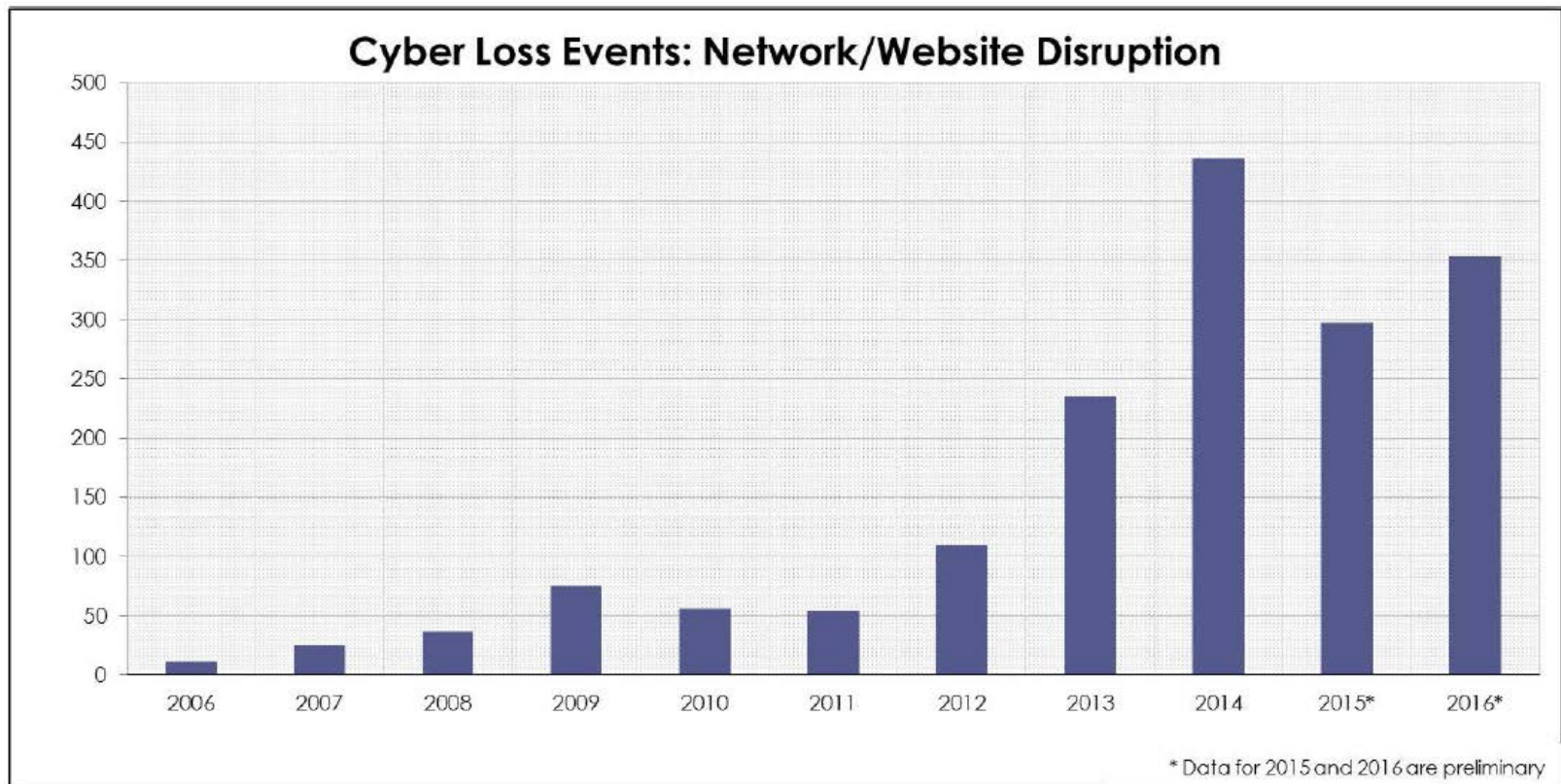
beazley beautifully
designed
insurance

Cyber Threat Trends

Claims and Threat Trends



Claims and Threat Trends



CRA Charles River
Associates

VedderPrice



Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

beazley beautifully
designed
insurance

Evolution of Cyber Insurance

Other Policies

NON-CYBER POLICIES ARE ADDING DATA BREACH EXCLUSIONS

COMMERCIAL GENERAL LIABILITY
FORMS FILING GL-2013-ODBFR

Access Or Disclosure Of Confidential Or Personal Information Exclusions Introduced

About This Filing

This filing introduces mandatory and optional exclusionary endorsements, for use with General Liability Coverage Part, addressing the access to or disclosure of confidential or personal information.

GENERAL LIABILITY
CG 21 06 05 14

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

**EXCLUSION – ACCESS OR DISCLOSURE OF
CONFIDENTIAL OR PERSONAL INFORMATION AND
DATA-RELATED LIABILITY – WITH
LIMITED BODILY INJURY EXCEPTION**

COMMERCIAL GENERAL LIABILITY
CG 21 07 05 14

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

**EXCLUSION – ACCESS OR DISCLOSURE OF
CONFIDENTIAL OR PERSONAL INFORMATION AND
DATA-RELATED LIABILITY – LIMITED BODILY INJURY
EXCEPTION NOT INCLUDED**

Cyber and Other Policies

Coverage & Gaps

	Property	General Liability	Crime / Bond	K&R	E&O	Cyber
1st Party Privacy / Network Risks						
Physical damage to Data only	Yellow	Red	Yellow	Red	Red	Green
Virus / Hacker damage to Data only	Yellow	Red	Yellow	Red	Red	Green
Denial of service attack	Yellow	Red	Red	Red	Red	Green
B.I. Loss from security event	Yellow	Red	Red	Red	Red	Green
Extortion or threat	Red	Red	Red	Yellow	Red	Green
Employee sabotage of Data only	Yellow	Red	Yellow	Red	Red	Green
3rd Party Privacy / Network Risks						
Theft / Disclosure of private info.	Red	Yellow	Yellow	Red	Yellow	Green
Confidential corporate info. breach	Red	Yellow	Yellow	Red	Yellow	Green
Technology E&O	Red	Yellow	Red	Red	Green	Yellow
Media Liability (electronic content)	Red	Yellow	Red	Red	Green	Green
Privacy breach expense / notification	Red	Red	Red	Red	Yellow	Green
Damage to 3rd party's Data only	Red	Yellow	Red	Red	Green	Green
Regulatory privacy defense / fines	Red	Red	Red	Red	Yellow	Green
Virus / Malicious code transmission	Red	Yellow	Red	Red	Yellow	Green
Coverage Provided?	Green	* For reference and discussion only; policy language and facts of claim will require further analysis				
Coverage Possible?	Yellow					
No Coverage?	Red					

3rd Party Liability Coverages

Network Security

- Failures in computer security
- Transmission of malicious software / viruses
- DDoS Attacks

Privacy Liability

- Unauthorized Access or Use
- Failure to protect sensitive information

Media Liability

- Online Content / Multimedia
- Libel / Slander / Defamation
- Copyright infringement

Regulatory Defense, Fines & Penalties

- Regulatory Proceedings & Investigations
- Fines and Penalties where insurable by law

PCI Defense, Fines & Penalties

- Defense Costs
- Fraud Assessments

First Party Coverage

Cyber Extortion

Digital Asset Restoration

Business Interruption & Extra Expense

Cyber Crime

Breach Response Services

CRA Charles River
Associates

 Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

VedderPrice

beazley beautifully
designed
insurance

Cyber Risk Management: Incident Response Planning & Vendor Management

Cyber Incident Response Preparation

Incident Response Plan & Provider Identification

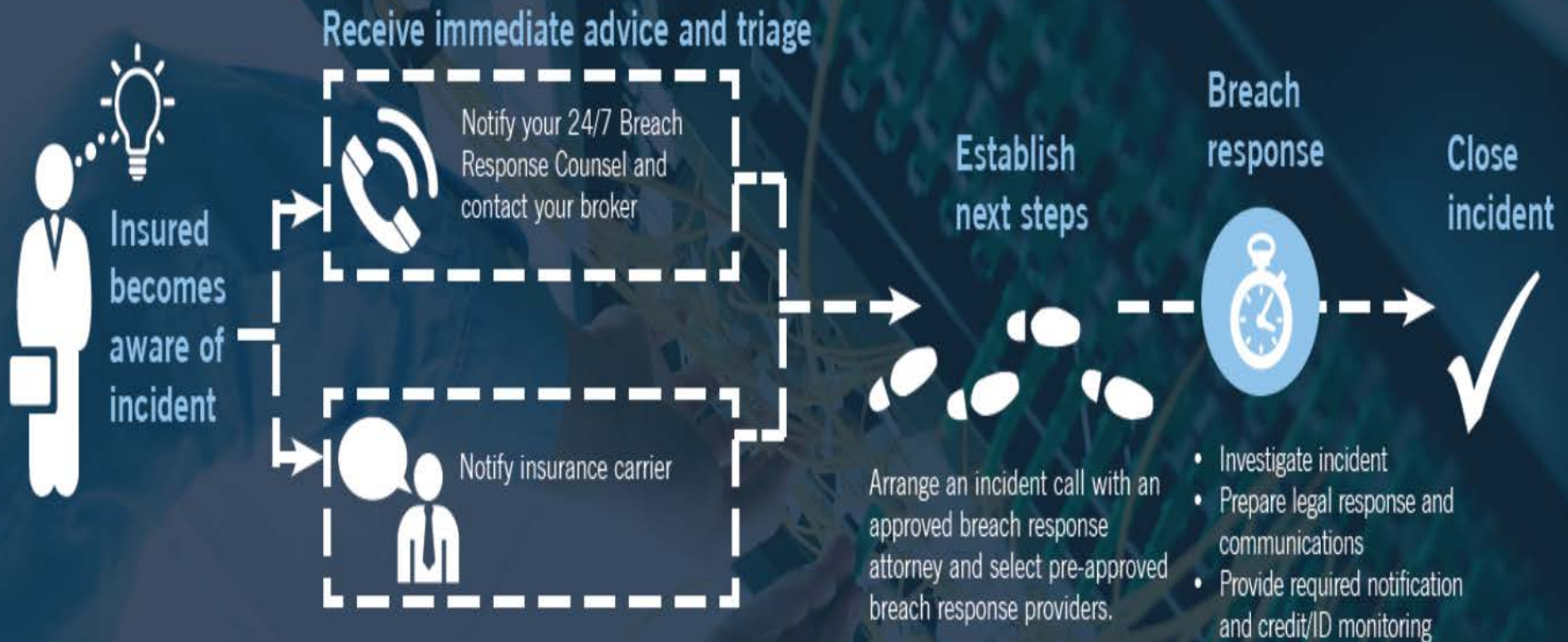
- ✓ Successful creation and implementation of an Incident Response Plan (IRP) is an extremely important step in cyber risk management
- ✓ An Incident Response Plan is essential for guiding you through a breach at the time of a crisis event
 - Complete an IRP that includes a your chosen providers
 - Complete a Table Top Workshop to test your IRP
 - Pre-negotiate service agreements with breach response providers
 - Seek insurance carrier approval for chosen providers

Business Continuity Plan/Back-up Procedures

- ✓ Preparation is essential to minimize disruption of networks and continue operations without unnecessary delay.
- ✓ A thought out response may protect your organization's image, brand, and reputation
 - Create and rehearse your business continuity

Cyber Incident Response

LIFE CYCLE OF A CYBER INCIDENT



Vendor Management

UNDERSTANDING YOUR VENDOR RELATIONSHIPS

Contract Review & Professional E&O / Cyber Insurance Requirements

- ✓ Proper indemnification from your vendors will help to mitigate your vicarious liability should your chosen partner make an error that is out of your control
- ✓ Vendor Acceptance Process is vital
 - ❑ Develop Errors & Omissions, Cyber, and Crime Insurance Contract Language designed to be made part of your existing insurance contract requirements
 - ❑ Develop reasonable requirements that are relevant to the current cyber risk environment
 - ❑ Prepare a vendor evaluation worksheet!!!

Vendor Management

SAMPLE CONTRACT WORDING – CYBER, E&O AND CRIME

Vendor) shall obtain at its own expense and evidence via Certificate(s) of Insurance the following insurance requirements before commencement of any awarded work and throughout the duration of the Agreement:

A) Errors and Omissions (E&O), Technology E&O / Technology Products E&O: minimum of \$5 million limit and in the annual aggregate, inclusive of defense costs

B) Network Security / Privacy Liability; including

- (1) computer or network systems attacks
- (2) denial or loss of service
- (3) introduction, implantation, or spread of malicious software code
- (4) unauthorized Access and Use of computer systems
- (5) privacy liability
- (6) breach response coverage

- Liability coverages should have a minimum of \$5 million limit and in the annual aggregate
- Breach response sublimits of at least 50% of the liability limit

C) Crime Insurance: Vendor, at its sole cost and expense, shall obtain and maintain in full force and effect, Third Party Crime/Employee Dishonesty Insurance in an amount not less than \$1,000,000. The insurance shall name _____ as a loss payee.

If policy or policies are written on a claims-made basis, coverage must be in place for a period of at least 12 months after the completion or termination of the Agreement. "INSURED" and subsidiaries must be named as an additional insured under E&O, Technology E&O / Technology Products E&O and Network Security / Privacy Liability coverage sections. Further, an appropriate endorsement deleting the Insured vs. Insured exclusion must be evidenced, so as not to impede a claim by "INSURED" and subsidiaries for a wrongful act of (Vendor). All insurance carrier(s) must carry an A.M. Best rating of at least A-, Class VIII.

CRA Charles River
Associates



Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

VedderPrice

beazley beautifully
designed
insurance

Thank You

Jeremy Gillespie
VP, Cyber Liability Practice
Arthur J. Gallagher & Co.
312-803-7394
Jeremy_Gillespie@ajg.com

Myles Miller
Underwriter
Beazley Group
312-476-6268
Myles.Miller@Beazley.com

Cuyler Robinson
VP, Forensic Services
Charles River Associates
312-619-3394
Crobinson@crai.com

Bruce Radke
Shareholder
Vedder Price
312-609-7689
Bradke@vedderprice.com