Gallagher
Insurance | Risk Management | Consulting

We've had a Cyber Incident! Now What?

ARTHUR J GALLAGHER & CO. | 2018

Identify the Exposure

- External Threats
  - Hackers
  - Viruses
  - Social Media
  - Third Party Vendors (VERY COMMON)
    - According to many state laws the liability for the exposure of protected data resulting from the breach of a 3rd party, such as cloud or payroll providers, still falls to the organization that gave the information to the vendor.
  - A Changing Regulatory Environment
    - States are constantly amending laws
    - Federal agencies are bringing action against affected organizations
    - International laws are being implemented causing additional regulatory exposure
- Internal Threats
  - Rogue Employees
  - Human Error
  - Mobile Devices

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

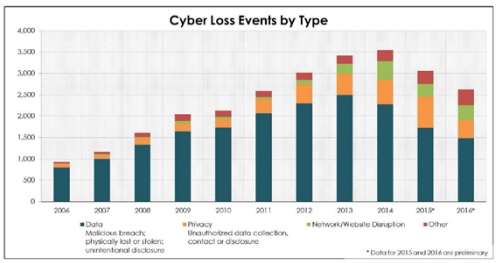
Data Breach Victim's Residency Governs

Regulatory Testing Grounds
- California, Illinois, Massachusetts, New York

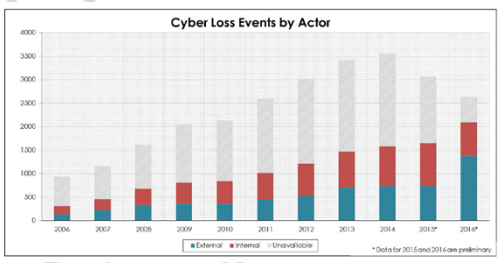
Gallagher
Insurance | Risk Management | Consulting

Claim Trends

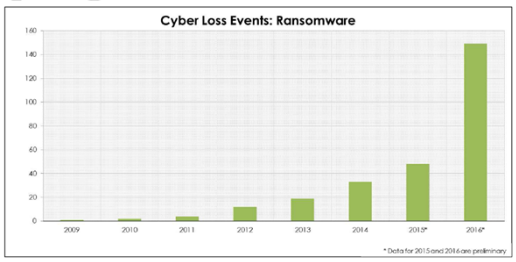
Cyber Threat Trends



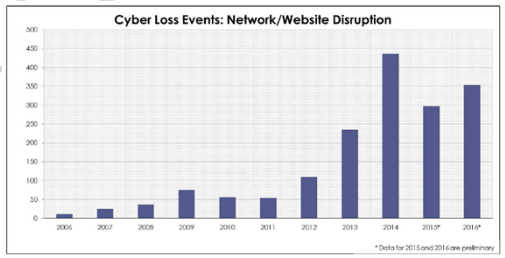
Cyber Threat Trends



Cyber Threat Trends



Cyber Threat Trends



Cyber Threat Trends

Consistent Increase in Cyber Claim Frequency

- SMEs
- All Industries
- Not just data breaches

Internal & External Threats

- 50% incidents involve internal actors
- Third Party Vendors

Ransomware

- 400% increase
- Industry agnostic
- Hollywood Presbyterian

Operational Risks

- Reliance on digital tools
- DDoS / IoT

Breach Examples: Schools

- **Dover School District (December 2015) – Human Error**
- Janitor accidentally threw away envelopes containing personal information of a number of volunteers. The lack of proper disposal lead to the need to notify the potentially affected individuals
- **Lake Norman High School (October 2015) – Hacker**
- Students were able to manipulate a script that the school runs to get access to the system administrators password. 7 students used the password to access sensitive files on the school's system.
- **Bonita Unified School District (July 2015) – Hacker**
- An unidentified individual accessed student records. In addition to changing some student's grades it is believed they also downloaded sensitive information about students saved in the system including social security numbers, medical information and e-mail addresses with passwords.
- **Escondido Union School District (February 2015) – Portable Device**
- A district owned tablet and external hard drive containing protected information on students and teachers was stolen out of a teacher's back pack**.**

Gallagher
Insurance | Risk Management | Consulting

Cyber Risk Management

Cyber Risk Management

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
- Security Controls Due Diligence

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.

3rd Party Liability Coverages

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

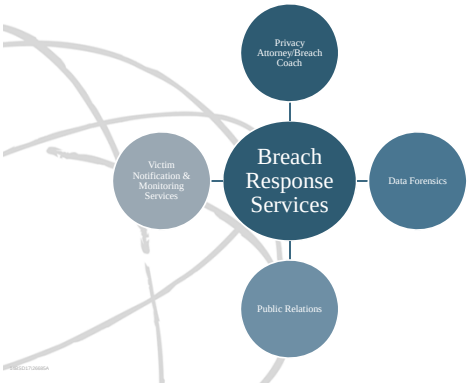
Privacy Liability
- Unauthorized Access or Use
- Failure to protect sensitive information

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

Breach Response Services



First Party Coverage

- Cyber Extortion
- Digital Asset Restoration
- Business Interruption & Extra Expense
- Cyber Crime
- Breach Response Services

Breach Response Process

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.

Gallagher
Insurance | Risk Management | Consulting

Data Breach Example

Incident Discovered

- Accounting discovered alterations to payroll file on Friday, 6/26
- Concerns about possible hacker making changes and re-routing funds
- Steps taken to stop transfers and resend correct payroll file
- Two communications sent to School employees same day
- Contact made with Insurance Broker team
  - Cyber Team
  - Crime Team
- Due to the potential loss of funds, claims also reported to the Crime insurance carrier
- Incident noticed to Cyber Insurance Carrier by e-mail on 6/26 and conference call placed to Insurance Carrier Breach Response team for guidance that afternoon:
  - Key members of IT staff out of town - conference call scheduled Monday morning, 6/29, to coordinate incident response efforts
  - Insurance Carrier recommended privacy attorney and computer forensic firm

 20

Response Begins

- Conference call held 6/29 with School, Cyber Insurance Carrier, Privacy Attorney, Computer Forensic Firm and AJG to determine next steps
- Provider service contracts sent – Cyber Insurance Carrier negotiated rates used
- Local media made of aware of incident 6/29 – Privacy Attorney advised on how to respond
- Communications to affected employees continued by e-mail on a weekly basis - Privacy Attorney advised of appropriate messaging
- Computer Forensic Firm began investigation week of 6/29 after on-site visit
- Crime Insurance Carrier acknowledged receipt of crime loss report

 21

Response Continues

- Fraudulently altered payroll file resulted in the following:
  - Total Amount Diverted: $243,496.46 (148 transactions out of 391 potential transactions)
  - Total Amount Recovered: $126,053
  - Total Crime amount recovered: $117,443
- Computer Forensics results not immediately conclusive – several weeks to finalize
- Board meeting on 7/13 required an incident update mid-investigation – talking points / guidance provided by Privacy Attorney
- Privacy Attorney advised on steps to formally notify all affected individuals

 22

Data Breach Mitigation

Steps taken from July – Present:

- Final letter to Affected Employees – 9/4
- Mail Distribution
- Offer credit monitoring and other services
- Call Center coordinated including FAQ's prepared by Privacy Attorney
- Daily Call Center reports
- Call Escalation & Log (11 out of 4400 letters)

 23

Insurance Coverage

Insurance Carrier insured the following expenses:

- Notification expenses
- Credit monitoring and other services
- Call center services
- Computer Forensic investigation expenses – after retention / deductible
- Privacy attorney fees – after retention / deductible

 24

BBR Services Team

Critical Assistance Provided:

- Screened employee notices; Board update; response to media and concerned employees; and School's response to past and current employees' notification
- Coordinated computer forensic investigation
- Established attorney-client privilege applicable to all breach response providers
- Responded to inquiries and data requests from local and federal law enforcement
- Determined extent of legal notification required; drafted letter for mailing; established Q & As for call center; and established an escalation plan (included monitoring)

Key Take-Aways - Privacy Response

- Dual-edged sword of communication:
  - Due to delay and payroll issues, School took on enormous burden of notifying employees over the weekend
  - Caution - Early communication risks breach of client-attorney privilege and possible incorrect info, unnecessary scrutiny / publicity
- Fine-tune and test incident response plan
  - Phone Tree - Be prepared, able to reach IT/Network staff, Legal, Senior Leadership and other key personnel - know who to call first, second, third…..
  - Prepare a formal incident response plan and review it regularly
- Computer forensic investigation can be slow / frustrating – trust privacy counsel advice
- Notifying Insurance Carrier / breach response experts immediately and allowing them to spring into action would have avoided the burden placed on various administrative staff
- Minimize PII exposure by purging information for past employees - bank account and driver's license at a minimum – Store the least amount of information for the least amount of time required.

Key Take-Aways – Computer Forensics

Recommended Best Practices:

- Separate login accounts for ERP and network access
- Two factor authentication
- Increase depth, breadth, and backups of audit logs
- Preserve image of infected devices
- Enforce password best practices: complexity, minimum length, shorter expiration
- Provide Information Security Awareness training
- Conduct regular security scans and risk assessments
- Implement malware solution, retain malware logs
- Restrict remote access to sensitive data via allowed IP addresses
- Implement single purpose computers

Most Important Forensic Information Provided to School:

- Log-in credentials of School PeopleSoft application administrator had been compromised
- Unclear how the log-in credentials were obtained, but the PeopleSoft application administrator's computer did have malware present on it
- Log-in was used to modify certain School employees' direct deposit account and routing numbers
- The unauthorized party was only in the PeopleSoft application for a limited period of time
- There was no forensic evidence of any personal information being exported

Gallagher
Insurance | Risk Management | Consulting

Thank You

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