Cyber and Privacy Liability

Presented by:
George Erickson, JD, CPCU, LLM
Siver Insurance Consultants

Caveat

Siver Insurance Consultants is not in the practice of law, and the observations made during this presentation are offered solely as laypersons in our capacity as insurance consultants.

General Treatment/Overview

What we will be covering

- Recent Losses
- Types of Cyber Losses
- Who needs Cyber Liability
- Cost/Consequences of Breaches
- Coverage in Other Policies
- Coverage in Cyber/Privacy Policies

Recent Losses in the News

Yahoo

- Breach in 2013
- Made public in August 2016
- 1 billion users affected
- October 2017, revised to 3 billion
  - Additional users affected discovered during due diligence performed for Yahoo's sale to Verizon Communications
  - Severity of hacks brought the sale price down $350 million

Recent Losses in the News

Yahoo Breach

- 3 billion users - every Yahoo account that existed at time of breach
  - Names, email addresses, phone numbers, encrypted and unencrypted security questions and answers, dates of birth and hashed passwords
- In addition - 2014 Yahoo breach
  - Disclosed in September 2016
  - Affected 500 million accounts

Recent Losses in the News

Equifax (September 2017)

- 145.5 million consumers
  - Names, social security number, birth dates, addresses, driver's license numbers, credit card numbers, dispute documents
- Equifax discovered breach on July 29th
  - Over 40 days to make incident public
  - Lawmakers questioned why so long to report breach

Recent School System Losses

- 2016 Hack of Four Florida School Systems
  - Moroccan hackers
  - Shut down access logging
  - Had access for three months
  - No personal info compromised
  - Were looking for access to other governmental systems including voting systems

Recent School System Losses

- 2015 New Jersey School System
  - NJ School District held by ransomware
  - Demanded 500 bitcoin (~$128k)
- 2015 Florida
  - Hackers successfully shut down standardized testing system vendor's system

Recent School System Losses

- Student Hackers
  - Recent incidents in NY and FL
  - Student hackers accessed school network
  - Attempted to change grades

Recent School System Losses

- School Systems are a potential gold mine for hackers
  - Personal info maintained for:
    - Current students
    - Former students
    - Faculty/employees
    - Parents
- School networks are often set up to emphasize ease of connectivity – not security (this is changing)

What is the Outcome?

- Reactionary, Not Proactive
  - In wake of Equifax, lawmakers introduced flurry of proposed legislation
    - Free credit freeze
    - Free credit monitoring
    - Legislation to expand consumers' rights in disputes with credit reporting companies

Types of Losses

First Party	Third Party
Losses that your organization might incur in the event of a cyber event	Claims made by third parties against your organization arising out of cyber event

Florida Law Considerations

- Florida Statute 501.171
  - Security of Confidential Personal Information
  - Applies to almost all Florida entities that use, store, maintain or acquire personal information.
  - Includes Florida Governments

Florida Law Considerations

- Florida Statute 501.171
  - Requires notice to Florida Dept. of Legal Affairs within 30 days of discovering a breach affecting 500 or more.
  - Requires notice to affected (or potentially affected) individuals with 30 days of discovery
    - Notice can be by US Mail or E-Mail
    - Some exemptions and extensions are available

Florida Law Considerations

- Florida Statute 501.171
  - Personal Information Includes:
    - SS#
    - D/L#
    - Account#
    - Medical Info
    - Health Insurance Policy#
    - Login/Password/Security Question Answers

Florida Law Considerations

- Florida Statute 501.171
  - Requires notice to credit bureaus but does not requiring credit monitoring services to be offered
  - Does not create a separate private cause of action under statute
  - Creates exemption to Public Records Act for much of info gathered

Florida Law Considerations

- Florida Statute 768.28
  - In many cases, the protections of Florida sovereign immunity will not be applicable to losses and costs incurred in relation to a cyber breach.

First Party Losses

- Malware Attack on Systems
- Loss of Data
- Fraud
- Business Income/Extra Expense
- Public Relations/Goodwill

First Party Losses

What is Malware?

- Viruses
- Adware
- Spyware
- Worms
- Trojans
- Ransomware

First Party Losses

Malware Attack on Systems

- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Ransomware
- Hacktivism
- Infrastructure Attacks

First Party Losses – DoS/DDoS

Denial of Service (DoS)

Making a machine or network resource unavailable to its users by flooding it with traffic/data triggering a crash

Distributed Denial of Service (DDoS)

Same as DoS, but flood it with traffic/data from multiple sources simultaneously

First Party Losses – DoS/DDoS

Domain Name System (Dyn) DDoS (October 2016)

- Dyn controls much of the Internet's domain name system (DNS) infrastructure
- Brought down Dyn's servers
- Resulted in crash of numerous websites including Twitter, Netflix, Amazon, CNN, BBC, PayPal, and Visa

First Party Losses – DoS/DDoS

Domain Name System (Dyn) DDoS (October 2016)

- Different than most other DDoS attacks because used the “internet of things” (IoT) devices to coordinate the attack
- IoT is the network of internet-connected devices
  - Smart homes, smart cars, healthcare (heart monitoring implants), wearables (Apple Watch, Fitbit), smart cities (smart energy management systems, transportation and surveillance), drones

First Party Losses – Ransomware

Ransomware

- Malware preventing or limiting users from accessing their system until a ransom is paid
- First known attack in 1989
- Continually evolving and affecting more people and organizations

First Party Losses – Ransomware

WannaCry (May 2017)

- Worldwide ransomware attack targeting Microsoft Windows
- More than 300,000 computers in 150 countries
- Patches were previously released, but not all users installed

First Party Losses – Ransomware

WannaCry (May 2017)

- Effect?
  - Hackers demanded bitcoin to release encrypted data
    - Overall, fairly unsuccessful in terms of ransom actually paid
    - Highlights the importance of software and system patches
  - Organizations implement backup systems

First Party Losses – Ransomware

Variant of Petya Ransomware (June 2017)

- Started in Ukraine, spread throughout the world
- Who was affected?
  - Ukraine – major disruptions in its power grid, banks, government offices, TV channels and airports
  - Also affected many companies in Russia, France, UK, Germany and Norway including manufacturing, shipping and construction companies
  - Chernobly radiation-monitoring system computer shut down, had to monitor manually
  - Merck & Co. pharmaceutical company
  - Cadbury chocolate company

First Party Losses – Hacktivism

Hacktivism

- Hacking into a computer system for a politically or socially motivated purpose
- Includes:
  - Hacking government websites
  - Publicly disseminating private email or confidential records
  - "Doxing" – compiling personal information about targets, such as police officers or officials, and posting it online
  - DoS attacks

First Party Losses – Hacktivism

Examples of Hacktivism:

- WikiLeaks
- January 2016 – State of Michigan website hacked to draw attention to Flint water crisis
- May 2016 – North Carolina website hacked to protest law about transgender people having to use bathrooms that match sex on birth certificate

First Party Losses – Hacktivism

Examples of Hacktivism:

- August 2014 – after shooting of Michael Brown in Ferguson, Missouri
  - Hacker groups used DoS attacks and doxing of state, local and law enforcement officials
  - State website had brief outages in August 2014 and three months later after grand jury decision to not indict
  - Although the State of Missouri was successful in counter-acting the attacks, it spent $150,000

First Party Losses – Hacktivism

Effects:

- Public unable to access government websites
- Governments have to pay for additional staff time and technology to combat (with costs ultimately passed on to taxpayers)
- “Doxing” targets potentially at risk

First Party Losses – Infrastructure Attacks

Dallas Emergency Sirens hacked (April 2017)

- All 156 emergency sirens sounded for 90 minutes in the middle of night panicking residents
- Resulted in double amount of calls to 911
- Hackers used radio signals, not computers
- While no data breach, leads to other concerns such as infrastructure and 911 emergency service vulnerabilities

First Party Losses

Loss of Data

- Malicious destruction of data
  - Outside – hackers, malware, etc.
  - Internal – rogue employees
- Accidental damage to data
- Failures in IT system
- Electrical power surges
- Natural disasters

First Party Losses

Fraud

- Outside fraud
  - Social Engineering – when a criminal tricks employee into transferring funds or revealing confidential information usually by impersonating a vendor, client or supervisor in an email, phone, in person or through text
- Internal fraud
  - Employee theft
  - Employee destruction of intangible assets

First Party Losses

Business Income/Extra Expense

Public Relations/Goodwill

Third Party Losses

- Disclosure of Private Information/Breach of Privacy
- Defamation or Slander
- Transmission of Malicious Content
- Cyber Extortion
- Virus Promulgation
- Errors and Omission

Third Party Losses – Disclosure of Private Information

Personal Information

- Gmail Phishing Attack (May 2017)
  - Infected emails made to look like they were from a trusted contact asking the user to open a Google Doc
  - Affected 1 million users
  - Google quickly quashed attack
  - Effects:
    - Compromised email accounts sent phishing email to infected users' contacts – spread quickly
    - Criminals can use information from user's email account to potentially access user's other accounts such as emails, retail, etc.

Third Party Losses – Disclosure of Private Information

Personal Information

- IRS Data Breach (April 2017)
  - IRS tool Free Application for Federal Student Aid (FAFSA) hacked
  - 100,000 taxpayers had personal information stolen
  - Estimated that 8,000 fraudulent returns filed, processed and refunds issued
  - Fraudulent refunds totaled $30 million

Third Party Losses – Disclosure of Private Information

Personal Information

- Anthem Blue Cross Blue Shield (2017)
  - Settlement of consolidated litigation over 2015 hacking
  - 78.8 million people affected
    - Names, birthdays, social security numbers, addresses, emails, employment and income information
    - Credit card and medical information not compromised
  - Settled for $115 million
    - Used to pay for 2 additional years of credit monitoring for class members

Third Party Losses – Disclosure of Private Information

Medical Information – HIPAA

- U.S. Dept. of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces HIPAA Rules
  - Civil fines and criminal penalties
- 2016 – record year for HIPAA enforcement fines
  - Over $23 million
  - Included largest settlement to date (Advocate Health Care - $5.5 million fine)

Third Party Losses – Disclosure of Private Information

Medical Information – HIPAA

- Common Causes of Fines
  - Stolen protected health information (PHI)
    - e.g., laptops, flash drives, compromised networks
  - Untimely breach reporting
  - Failure to conduct risk analysis, implement risk management plans
  - Failure to monitor/audit

Third Party Losses – Disclosure of Private Information

Medical Information – HIPAA

- Other Causes of Breaches
  - Failure to encrypt electronic devices
  - Business Associate/Vendor agreements not HIPAA compliant
  - Cloud storage – data hosting agreements
  - Document sharing applications
  - Employees' actions
    - e.g., inadvertently downloading malware in email attachments, former employees improperly accessing databases when access not immediately terminated

Third Party Losses – Disclosure of Private Information – HIPAA

Photocopier Breach Case (2013)

- Affinity Health Plan failed to erase the data from the copiers' hard drives when it returned machines to leasing agents
- Copiers contained electronic protected health information (ePHI) on internal hard drives
- Over 344,000 individuals affected
- $1.2 million payment to OCR by Affinity

Third Party Losses

- Defamation or Slander
- Transmission of Malicious Content
- Cyber Extortion
- Virus Promulgation
- Errors & Omissions

Who Should Have Cyber/Privacy Liability Coverage?

Historically, most people did not think needed cyber/privacy liability exposure if organization was not doing business on the Internet or collecting sensitive data

Who Should Have Cyber/Privacy Liability Coverage?

But the Nature of Losses Have Changed:

- Originally – to protect data privacy and data breaches
- Now – range of exposures goes beyond privacy and data breaches

Who Should Have Cyber/Privacy Liability Coverage?

Internet-of-Things (IoT) is changing the landscape of cyber and privacy exposures

Any organization can be impacted!

Who Should Have Cyber/Privacy Liability Coverage?

Contractual Requirement

Some organizations may be required to purchase cyber/privacy liability due to contractual requirements.

Who Should Have Cyber/Privacy Liability Coverage?

2016 RIMS Cyber Survey

25% of respondents purchased cyber/privacy liability coverage due to contractual requirements.

RIMS Cyber Survey

Respondents who purchased stand-alone cyber insurance:

- 2015 – 51%
- 2016 – 80%
- 2017 – 83%

RIMS Cyber Survey

Respondents who transferred cyber exposures to third parties:

- 2015 – 58%
- 2016 – 68%
- 2017 – 72%

Cost of a Data Breach

Average cost of a data breach is $4 million according to the 2016 Ponemon Cost of a Data Breach Study.

Consequences of Breaches

Expenses to Organization

- Legal fees
- Costs of investigating incident
- Data restoration expenses
- Remediation expenses (costs of responding to a data breach)
- Costs of downtime

Consequences of Breaches

Expenses to Organization

- Compliance violations (e.g., HIPAA enforcement fines)
- Extortion – ransom costs
- Crisis Management expenses
  - Expenses associated with managing the loss event (e.g., PR experts)
- Business Income and Extra Expense

Consequences of Breaches

Third Party Liability

- Breach or loss of data
- Legal judgments/settlements

Consequences of Breaches

Response Costs

- Notification to third parties whose data may be compromised
- Identity recovery (helping those affected recover from the breach)
- Monitoring
- Can be mandatory or voluntary

Coverage in Other Policies

- Shrinking coverage – are your policies silent on the issue?

- Most policies now have specific cyber liability exclusions.
  - No "Loss of Electronic Data" coverage (CGL) resulting from physical injury to tangible property
  - ISO 2014 CGL "Exclusion – Access or Disclosure of Confidential or Personal Information and Data-related Liability with Limited Bodily Injury Exception"

Coverage in Other Policies

Property Insurance – EDP Coverage

- May cover damage and losses of data resulting from various cyber events

Coverage in Other Policies

Directors and Officers Policies

- May cover suits against directors and officers resulting from cyber loss

Coverage in Other Policies

Fidelity/Employee Dishonesty

- Cyber policies usually do not include coverage for certain types of losses for acts committed by employees
- Computer fraud

Coverage in Cyber Liability Policies

Various Names for Cyber Policies:

- Cyber Liability
- Cyber and Privacy Insurance
- Information Security and Privacy Insurance
- Cybersecurity Insurance
- Errors and Omissions policies

Coverage in Cyber Liability Policies

- First Party Coverage
- Third Party Coverage

Coverage in Cyber Liability Policies

Types of First Party Coverage:

- Theft of Property Coverage
- Post-Breach Response Coverage
- Time Element Coverage

First Party Coverage – Theft of Property Coverage

Extortion/Ransom Coverage – Covers ransom threats:

- To commit intentional computer attack
- Damage or shut down insured's computer system
- Disclose confidential information
- Block access to system
- Introduce a virus into computer system

First Party Coverage – Theft of Property Coverage

Extortion/Ransom Coverage

- Insurance may pay:
  - Cost of ransom
  - Costs to prevent further extortion
    - e.g., computer security systems expert
  - Costs for expenses in dealing with extortionist
    - e.g., cost of experts hired to negotiate with extortionist
- Usually does not cover acts committed by employees

First Party Coverage – Theft of Property Coverage

Data Asset Coverage and Restoration

- Coverage for the cost of recovering and restoring lost data when insured's computer system is breached
- No coverage for cost of recreating lost data from scratch, but covers expenses incurred by electronic recovery methods
  - e.g., recovering lost data from a backup

First Party Coverage – Theft of Property Coverage

Data Asset Coverage and Restoration

- No coverage for loss of data caused by intentional employee acts
- No coverage for software upgrades, including cost of upgrading software or other programs during data restoration process

First Party Coverage – Theft of Property Coverage

Computer Fraud

- Coverage for loss from intentional, fraudulent, or unauthorized entry into a computer system resulting in theft of money/data
- Usually does not cover acts committed by employees

First Party Coverage – Theft of Property Coverage

Funds Transfer Fraud

- Coverage for losses when funds are transferred from one financial institution to another
- Usually does not cover acts committed by employees

First Party Coverage – Theft of Property Coverage

Social Engineering

- Coverage for losses resulting from insureds transferring monies or revealing confidential information based on what appears to be legitimate instructions to transfer the money or provide confidential information
  - Phishing, Vishing, etc.

First Party Coverage – Theft of Property Coverage

Social Engineering

- On a cyber policy, coverage is often excess of applicable crime insurance
- May have requirements insured must comply with for coverage
  - e.g., no coverage unless insured performed a callback verification with respect to each communication; no coverage unless fraudulent instruction was verified using two-factor authentication process

First Party Coverage – Theft of Property Coverage

Investigative Costs (including forensic)

- Costs to establish whether security breach occurred
- Assess cause and scope of event
- May also assist in improving future risk control

First Party Coverage – Post-Breach Response Coverage

Crisis Management/Public Relations

- Breaches are very costly
- Target Data Breach (2013)
  - 40 million credit and debit cards
  - 70 million customer records
  - Cost Target $252 million
    - Cost after insurance reimbursement – $162 million
    - Cost after tax deductions – net losses of $105 million

First Party Coverage – Post-Breach Response Coverage

Crisis Management/Public Relations

- Coverage pays for direct expense required to respond to breach immediately after it occurs

- What services are often offered under this coverage?
  - Remediation – Forensic Services
    - Secure insured's system after breach
    - Determine cause of breach
    - Advice on preventing future breaches
  - Reputation Management
    - Public Relations and Crisis Management Assistance

First Party Coverage – Post-Breach Response Coverage

Crisis Management/Public Relations

- Services offered:
  - Call Center
  - Notification to Customers/Clients
  - Credit Monitoring
  - Identity Theft Monitoring
  - Notification to Banks and Credit Card Companies (if financial information has been compromised)

First Party Coverage – Time Element Coverage

Business Income/Extra Expense

- Coverage for actual loss of business income or extra expense incurred due to interruption of insured's business resulting from cyber event
- Examples of extra expense:
  - Cost to buy or replace software
  - Cost of alternative network services
  - Employee overtime to respond to the breach

Coverage in Cyber Liability Policies

Types of Third Party Coverage:

- Information Security and Privacy Liability Coverage
- Regulatory Defense and Penalties Coverage
- Website Media Content Liability Coverage
- PCI Fines and Assessments Coverage
- Bodily Injury and Property Damage Liability Coverage

Third Party Coverage

Information Security and Privacy Liability

- Provides coverage for insured's liability for breaches of third party's private information
- Can include data/information of clients, customers, employees, business partners

Third Party Coverage

Information Security and Privacy Liability

- What is covered?
  - Liability from loss, theft, or unauthorized disclosure of personally identifiable information (PII) in insured's care, custody, or control
  - Damage to third party data stored in insured's computer systems
  - Transmission of malicious code or DoS to third party's computer system

Third Party Coverage

Information Security and Privacy Liability

- What is covered?
  - Failure to timely disclose data breach
  - Failure of insured to comply with its privacy policy
  - Failure to administer identity theft program required by governmental regulation
  - Coverage for cost of defending these claims

Third Party Coverage

Regulatory Defense and Penalties

- Provides coverage for:
  - Costs of legal defense required by regulatory actions
  - Payment of fines and penalties regulators levy against insured

Third Party Coverage

Website Media Content Liability

- Provides coverage for insured's liability incurred in conjunction with material published on website
- Does not respond to data breaches or electronic intrusions that do not involve theft of data (e.g., DoS attacks)

Third Party Coverage

Website Media Content Liability

- Covers:
  - Intellectual property violations
  - Personal injury (e.g., defamation, libel, slander, invasion of privacy, etc.)
  - Miscellaneous improper web-based activities (e.g., improper deep linking)
  - Social media liability from activities engaged in on social media sites

Third Party Coverage

PCI Fines and Assessments

- Provides coverage for fines and penalties assessed against insured by credit card companies for claims that allege insured did not comply with PCI data security standards (DSS)
- Provides defense expense coverage

Third Party Coverage

Bodily Injury and Property Damage Liability

- Potential coverage gap – cyber policy may exclude BI and PD and commercial general liability may exclude BI and PD resulting from cyber attack

Third Party Coverage

Bodily Injury and Property Damage Liability

- Examples of BI and PD arising from cyber attack:
  - March 2016 – hackers infiltrated water utility's control system and changed the levels of chemicals treating tap water
    - Also had access to personal and financial records of 2.5 million customers
    - Due to sensitive nature of the breach, the name of the water company and the country it resides in was not released

Third Party Coverage

Bodily Injury and Property Damage Liability

- Examples of BI and PD arising from cyber attack:
  - 2014 – German steel mill's network and production system hacked, shutting down parts of the plant and leading to "massive damage" of a blast furnace
    - Hackers used a phishing scheme to get the information to help them hack into the network
- Internet of Things (IoT)

Third Party Coverage

Bodily Injury and Property Damage Liability

- Some insurers now offer coverage for cyber-related BI and PD liability

Limits and Limitations

- Policy forms vary – no standard form
  - Must review insuring agreements to determine when coverage applies
    - some coverages will only apply when legal liability of insured is established
      - e.g., by judgment or settlement in response to lawsuit
    - some coverages will only apply when there is an actual theft of data, not merely an intrusion
      - e.g., DoS attack has no theft of data

Limits and Limitations

- Premiums vary – lack of claim history makes it difficult to price

- Lack of litigation – Most cases dealing with cyber issues are cases of first impression, meaning that the questions or issues have never arisen before in a reported case

Limits and Limitations

- Aggregate limits – most cyber policies are subject to aggregate limit of liability

- Sublimits – most cyber policies have specific limits of liability for each coverage part
  - Important to look closely at the sublimits

Limits and Limitations

- Defense costs – are defense costs in addition to the limit or outside the limit?

- Choice of vendors
  - Some insurers allow you to choose your own vendors
  - If insurer allows, select vendor in advance of breach and work out the contractual terms ahead of time

Exclusions Found in Cyber Policies

- Portable Electronic Device Exclusion – cyber breaches resulting from portable devices

- Intentional Acts Exclusion
  - If employee accidentally caused cyber breach, resulting loss may be covered
  - If a different employee caused exact same cyber breach intentionally, resulting loss may be denied

Exclusions Found in Cyber Policies

- Terrorism/Cyber Terrorism Exclusion
  - Many cyber policies exclude coverage for acts of terrorism, including acts of any foreign enemies or nations
  - Many data security breaches originate abroad, some may be alleged to be directed by a foreign nation or by groups that would be considered foreign enemies

Exclusions Found in Cyber Policies

- Negligent Computer Security Exclusion
  - Insureds must install software updates and patches
  - Insureds must encrypt data or use appropriate security for devices/networks
  - BYOD – Bring Your Own Device
    - May not have coverage for breaches that occur on non-company owned devices, such as if your employees use their personal cell phones to conduct business

Exclusions Found in Cyber Policies

As the policies evolve, insurers may offer coverage for some of these exclusions.

Notice to Insurers of Possible Breach

- Many cyber policies require notice to insurers at an early stage
- Policy may require insurers consent to expenditures incurred early on
  - e.g., retaining breach vendors, notification costs, etc.

Add-on Services Available from Insurers

Most insurers are partnering with outside vendors to offer a broad range of add-on services in the cyber and privacy liability market.

Add-on Services Available from Insurers

- Security risk assessments
- Legal consultation on security protocols
- Incidence response planning
- Threat detection services

Add-on Services Available from Insurers

- Employee education and training
  - e.g., phishing awareness training
- Crisis management and breach response services

Requiring Cyber Liability from Vendors

- Why require it?

- Key elements to look at:
  - Be sure to know what is covered
    - Limited to only breach of personally-identifiable information?
  - Who are the insureds? Additional insured?
  - Limits, deductibles/SIRs, coverage territory, etc.
  - Contractual liability exclusion? Defense coverage?

Requiring Cyber Liability from Vendors

Additionally, consider your vendor contracts.

- Indemnification and hold harmless provisions
- Contractual liability limitations

Final Thoughts

- Even with cyber and privacy liability insurance, vigilance is important
- Need to be aware of ransomware, phishing, spoofing
- Need to train employees and continue to educate them

Insurance Consultants
SIVER

Questions or Comments?

Insurance Consultants
SIVER

Thank you!

George W. Erickson, JD, CPCU, LLM

(727) 577-2780
gerickson@siver.com