The Life Cycle of a Cyber Liability Claim & the Role of Insurance

Southeast Chapter - Tampa, FL
March 10, 2016
Laura Zaroski, Esq.
VP of Professional, Management & Cyber Liability
Socius Insurance Services

What do Cyber Policies Cover?
Cyber Insurance: Why are companies Buying Now?

“Cyber liabilities are the slip-and-fall exposures of the next millennium”  - Adam Fleischer, Esq., Bates & Carey
Common Misperceptions About Cyber Marketplace:

• Coverage isn’t available
  – Cyber/Network Security/Privacy policies are now offered by most carriers
• Apps are too complicated  (short forms available)
• Coverage is too expensive
  – Minimum premiums can be as low as $750
• Coverage is too limited
  – Each product is different. Comprehensive coverage or limited coverage options can be purchased. Policyholders may often select from a menu of coverages being offered.
• Lack of exposure – “I don’t need it”
  – I have coverage for it under another policy, right?
  – I am not at risk, am I?
Underwriting Considerations

- Revenues
- Type of Business
- Number/Types of data handled?
  - (How much data is at risk? Sensitivity of that data? Is it stored/transmitted?)
- Credit/debit card processing (volume?)
- Security measures/procedures (passwords? Anti-virus? patches?)
- Encryption
- Contractual Relationships
  - (security of vendors?) (Legal review of contracts?)
Cyber Policies: Available Coverages

- Pre-Breach Risk Management Services
- Breach Coach Services
- Network Security & Privacy Liability (first party and third party claims)
- Forensic expenses
- Breach Notification costs
- Hacker Damage
- Regulatory Investigations, Fines & Penalties
- PCI Fines, Penalties & Assessments
- Cyber Extortion
- Cyber Business Interruption
- Media Liability
- Reputational Harm
Cyber Policies: PRE-Breach Risk Management Services

- Training /Education (webinars)
- Security checklists
- Incident roadmap
- Best practices (passwords, system segmentation, two factor authentication)
- Pen-testing / Vulnerability scan
- Newsletters
- White Papers /Information on emerging issues
- Legal updates
Breach Coach Services

• Coverage triggers at time of suspected breach

• **Breach coach is usually an attorney** (privilege)

• **Initiate forensic investigation** (determine cause, length of time, data infiltrated, remove virus, identify document damage)

• **Data Restoration (hacker damage)** — (restore or recreate corrupted or destroyed data)
Cyber Policies: Coverage

• Breach Notification costs:
  • Legally sufficient letters to affected parties (*Coverage can be within limits, outside limits, dollar amount or per individual) (Required and Voluntary)
  • Call center (handle angry customers, clients, employees)
  • Credit monitoring / Identity theft monitoring (1 year or more)
Third Party Claims: Network Security & Privacy Coverage

- Failure to protect employee/customer/client info (individual or corporate)
- Failure to secure network
- Failure to mitigate unauthorized access
- Failure to disclose breach (in violation of statute)
- Spreading of malicious code
- Failure/inability to fulfill internet/tech or other miscellaneous professional services to others (web hosting, e-commerce)
- Often class actions lawsuits
Cyber Policies: Coverage

- Regulatory Investigations, Civil Proceedings, Fines & Penalties
  - Request for info from government agencies
  - Healthcare: HIPPA Violations (HHS –OCR)
  - Financial Services: SEC
  - All industries: Attorney General / FTC (unfair business practices, failure to protect consumer info)

- Payment Card Industry - Data Security Standards (PCI-DSS)
  - PCI Fines, penalties & assessments
  - Redress funds, payment card reissuance fees, fraudulent charges
Cyber Policies: Cyber Extortion

- **Cyber Extortion**
  - Pay forensic investigation and expenses pursuant to threat
  - Pay ransom funds – (Cryptolocker -lock you out of your databases/systems)
  - Threats to release info stolen (Ashley Madison) or steal info
  - Threat of a DDOS attack / threats to do harm (introduce malicious code)
• **Cyber Business Interruption**
  - Down time while system is interrupted or being rebuilt
  - Pays lost income / Extra Expense – during period of restoration
  - Waiting period (hours, not retention applies)

• **Reputational Harm / Crisis Management Expenses**
  - Expenses to defend brand – mitigate loss of confidence / damage to reputation (think Target)
  - Crisis Communications - deal with media, news outlets, press releases
  - Public Relations firm (think Olivia Pope)
• Media Liability
  • Related to advertising and publishing on Website/blogs/Linkedin/Facebook
  • Potential claims for:
    – Libel/Slander / Invasion of Privacy
    – Infringement of Copyright /Plagiarism/Trademark /Trade dress
    – False Advertising
    – Misappropriation of ideas/content
    – Infringement of domain name
    – Misdirection by Insured’s site (meta tags)
Cyber Policies: Challenges

- The biggest challenge: Every form is very different.
- Each carrier calls their form and coverage parts by different names.
- Many carriers sub-limit major coverage parts.
- Wordings vary dramatically. Tricky and hidden exclusions can negate coverage!
- Markets/Coverage/Pricing: Constantly Evolving
Proactive Breach Management

PLUS Southeast Chapter Meeting

Matt Cullina, CEO, IDT911

IDT911
Protecting Identities. Enhancing Reputations.
Security vs. Privacy

**Security**
- Confidentiality
- Integrity
- Availability

**Privacy**
- Notice
- Consent
- Use
- Disclosure
- Protected Info
SMBs will have different needs than enterprises, but SMBs may have just as much risk.

**SMB**
- May have less data, or less complex data (but not always!)
- Can likely satisfy needs with simple security plans
- Likely won’t have data security designated staff
- Should consider outsourcing breach mitigation & remediation
- May vet third party vendors for IT and data consulting

**Enterprise**
- May have more data, or more complex data
- If multi-national, will need to abide by different sets of regulations and laws for management and remediation
- May have In-house chief privacy officer, infosec officer, and/or IT directors to oversee data security
Proactive Breach Management

Where Do We Stand Today

Pinpoint Weakest Links

Plan For The Worst
Proactive Breach Management

Where Do We Stand Today

Security Assessment

Pinpoint Weakest Links

Employee Privacy Training

Vendor Due Diligence

Plan For The Worst

Incident Response Plan
• What type of data does my business own and manage?
• Who owns the data and where is it stored or transmitted?
• Do we need this data – now, ever?
• How do we securely dispose of this data?
• Do we have a plan to analyze data, at least, on an annual basis?
Assess Data Risks

Perform a data risk assessment to identify information assets as well as the risks to those assets.

- What information is (or should be) protected?
- What constitutes an “event” or “incident”?
- The signs of events likely to occur
- The impact and probability of an incident type
- What constitutes a “breach”?
Assess and Address Security

- Network Security
  - Firewalls
  - Antivirus Software
  - Encryption
- Data Minimization (information retention/disposition)
- Employee Training
Anticipate An Incident

- Incident Response Plan (IRP)
- InfoSec Policy/Written Information Security Program (WISP)
- Cyber War Gaming/Tabletop Exercises
Breach Response Areas of Focus

- Breach Counseling
- Crisis Management
- Remediation Planning
- Notification Assistance
- Evidentiary Support
Recommendations

- Use technology to identify and protect sensitive data
- Prepare and test an incident response plan
- Deploy encryption and strong authentication solutions
- Educate and train employees on how to manage confidential information
Professional Liability Underwriting Society
- Underwriting Considerations

Glen P. Manjos
AVP Underwriting
Professional & Network Security/Privacy Liability
Cyber is...
• Network Security & Privacy
• D&O, E&O, GL...
• Don’t look for coverage, get the right coverage.

Advisory/Sale side ramped up quickly
• Underwriting and Advisory know what to look for.

The Great Wake-up Call
• Year of the Breach? What year isn't?
How do you get the right quote? The right coverage?

• As recently as 2 Years ago...
  – An agent could get a retail store a quote without submitting POS Detail
  – Healthcare, sure no problem they’re HIPAA compliant, right?
  – Document Management? Min Premium, right?

• Ripple Effect?
  – Other impacted Companies/Industries?
  – Price
  – Contractual Requirements
Prepare to receive a quote by identifying the links in the chain:

– Know what you have and what you don’t have
– Know your downstream and upstream exposure
– It’s not just PRIVACY
– Communicate what you have done
  • Have the proper person answer the questions
– Communicate what you will be doing
  • What are compensating controls?
– Need high limits?
  • Build a proper primary, not the cheapest
    – Look out for the pitfalls
We want to Quote & Bind business, we really do...

- As Easy as the five “Ws”
  - Who, What, When, Where and Why..

And of course

- HOW do you ensure the integrity of the data and the network/systems

An underwriter/Carrier’s responsibility to the Insured?
Claims Trends and Valuation

Richard Mather, Esq.
AVP, North American Claims Group
Allied World Insurance Co.

Hillard M. Sterling, Esq.
Managing Partner of Chicago Office
Winget, Spadafora & Schwartzberg, LLP
Claims Trends: Summary

- Intensified Regulatory Activity
  - OCR
  - FTC
- Intensified Ransomware
- Intensified Insider Threats
- Relaxed Standing
  - Potential Harm Sufficient
  - Statutory Standing Beyond Article III
- War Stories
Intensified Regulatory Activity

• Office of Civil Rights (OCR):
  – Applicable Rules
    • HIPAA and Privacy and Security Rules protect PHI.
    • Breach Notification Rule requires report to OCR.
  – 9/15: DHS Inspector General critiques OCR.
    • “Should strengthen its follow-up of breaches.”
    • “Should strengthen its oversight of compliance.”
  – Likely Results:
    • More complaints against covered entities.
    • More ammunition for plaintiffs.
    • More claims for alleged PHI breaches or incidents.
    • Disconnect between actual harm and settlements – See e.g., Lahey Hospital ($850,000 settlement for 599 stolen records).
• Federal Trade Commission (FTC):
  – Applicable Rules
    • Section 5 of the FTC Act (“unfair” or “deceptive” practices)
    • Multiple policy pronouncements
    • “Lessons learned” from prior enforcement actions
    • Multiple others: 33 different rules, laws, and guides.
  – Wyndham Caved and Settled.
    • Must establish and implement comprehensive InfoSec program for 20 years.
    • Must be “reasonably designed” to protect Cardholder Data.
    • Must have administrative, technical, and physical safeguards “appropriate to” Wyndham’s “size and complexity,” its “activities,” and data “sensitivity.”
    • Must undertake risk assessment, implement reasonable safeguards, retain capable service providers, test and monitor, and evaluate and adjust.
    • Must certify annual compliance as assessed by a third-party professional.
    • Must have PCI forensic investigator assess within 180 days of breach.
• Likely Results: Same as OCR: More actions, lawsuits, claims, and expensive settlements disconnected from actual harm.
Intensified Ransomware

- **Coverage:** Extortion and/or Business Interruption
- **Emerging Virulent Variants:**
  - CryptoLocker, TorrentLocker, CryptoFortress
  - Encryption of any file found through wildcard searches
  - Encryption of files in network shares
  - Volume shadow copies deleted to prevent restoration
  - “Freemium” offer to convince victims that they can recover files
- **Damages and Harm Expanded Exponentially**
  - More data at risk
  - Ransom paid in bitcoins
  - Amounts increasing – hundreds to thousands
  - Repeated ransom demands – “Thanks, but we want more.”
Intensified Insider Threats

• Coverage: Cyber, theft, business interruption

• Emerging Threats:
  – Privileged Users
  – Weaker Controls
  – Risky Access: Databases and File Services
  – Difficult to Detect

• Potential Ways to Reduce Claims or Exposure:
  – Digital Vaults for Sensitive Data
  – Real-Time Monitoring and Detection
  – Strong Password, Access, and Use Processes and Controls
  – Expeditious Disabling of Credentials and Access
  – Solid policies and training
Relaxed Standing

- Many Prior Decisions Dismissed on Standing Grounds
  - No tangible harm
  - Damages were not “certainly impending” under *Clapper*.
- Clear Trend to Deny Motions to Dismiss
  - Target – Unlawful Charges, Inability To Pay Other Bills, Fees
  - Increased Risk of Harm Sufficient
    - Sony and Adobe (California District Courts)
    - Neiman Marcus -- Seventh Circuit Court of Appeals
  - Reimbursement doesn’t defeat actual harm
- The New Frontier – Statutory Penalties Sufficient
  - Actual harm unnecessary
  - Currently Before U.S. Supreme Court -- *Spokeo, Inc. v. Robins*
• Media Wrongful Act: Defamation
  – Vendor sued for alleged defamation on website
  – Media Wrongful Acts

• Hospital System: Stolen Desktop Computer
  – Stolen computer with PHI
  – First-Party Coverages, then Liability Coverage

• HIPAA Allegations
  – Medical entity sued for unlicensed use of software
  – Coverage – Reading of medical information unauthorized

• Subscriber Information
  – Publisher sued for sharing with third parties without permission.
  – Coverage – Breach, despite absence of any theft or harm.
Valuation

• Costs, Expenses, Fees
  – Most Payouts are First Party Coverage
  – No claim against insured
  – Items
    • Attorneys’ fees
    • Forensics experts and expenses
    • Notification costs
    • Credit monitoring and repair
    • PR experts
• Claims Valuation
  – Facts and law
  – Predictions, estimates for resolution
    • MTD?
    • Summary judgment?
  – Attorneys’ Fees – Defense and plaintiffs’ attorneys if class action, statutory
  – Other costs, expenses, and fees – See above
Alex Ricardo
The Data Breach Response Methodology

Phase 1
Discovery & Assessment
- Incident Discovery
- Trigger Incident Response Plan

Phase 2
Investigation
- Privacy Counsel
- Forensics
- Conclusion & Results

Phase 3
Response
- Crisis Management
- Communications & Services

Phase 4
Claims Defense
- Class-Action Lawsuits
- Regulatory Investigations, Fines, Penalties
- Reputational Damage
- Business Income Loss

Risk Can Still Be Managed

“Cannot Un-Ring the Bell”
Emerging Trends

PLUS Southeast Chapter Meeting

Matt Cullina, CEO, IDT911

IDT911
Protecting Identities. Enhancing Reputations.
Exploits/Attacks Using Social Engineering

• The ‘Ish-es’:
  – Phishing
  – Spear-phishing
  – Vishing
  – SMiShing

....and Whaling.

Trending...W2 Request Email Fraud
• Fraudulent EFT transactions: a thief will move money from a victim’s account (business or personal bank account) to their own by engaging with someone at the business, client or financial institution.

• Coverage gaps for policyholders regarding Electronic Funds Transfer (EFT) fraud related to social engineering, email hacking, phishing, etc. and the misdirection of wire transfer funds to fraudster.

  – Other coverages, such as crime coverages, may cover losses.
Exploits/Attacks

- Ransomware
- DDoS/DoS Attacks
- Zero Day Vulnerability
- Malware/Malicious Code
  - Virus
  - Trojan Horse
  - Worm
- Spyware
  - Key Logger
• Franchisee/Franchisor data breach confusion
  – Finger pointing – payments and data storage of PII may be at the store-level, so security measures can vary among different stores
  – If one store is lax, it can hurt the entire brand; similarly if the franchisor experiences a breach, it affects the franchisee
  – Exposure can be through POS systems, malicious insider, 3rd party vendor
  – Information security has been a touchy subject, as franchisees may clash with the franchisor over the cost of new security measures
Common Breach Scenarios
Situation: Policyholder reports a missing computer device storing Personally Identifiable Information (PII), such as a laptop, USB flash drive or portable hard drive

Possible Scenarios

• Laptop stolen from a parked vehicle at the mall
• Luggage containing a laptop or portable storage device fails to arrive at destination
• Laptop or portable storage device stolen from a place of business or a home office
Mis-mailing

**Situation:** Policyholder reports that documents with one person’s PII were mistakenly sent to someone else

**Possible Scenarios**

- Documents faxed to the wrong number
- Bill, statement of benefits, or other documents sent to wrong person or address
- Attachments containing PII emailed to incorrect recipient
Erroneous Data Posting

**Situation:** Policyholder posts or prints PII in a public venue

**Possible Scenarios**
- Erroneous web site posting
- Failure to redact PII that may become public record prior to submission to a government entity

---

*DataBreaches.net*
December 28, 2015
191 million voters’ personal info exposed by misconfigured database

*Medical records of 2k patents left unprotected on contractor’s server*
Compromised System or Network (Hacking)

**Situation:** Policyholder reports that a computer or network housing PII has been compromised

**Possible Scenarios**
- Computer system has a virus, spyware, “bot” or Trojan horse
- Company Wi-Fi (wireless) network improperly secured or left open
- System has been hacked or accessed
**Situation**: Policyholder reports that paper documents containing PII were lost, stolen or exposed

**Possible Scenarios**

- Shipped documents fail to arrive at destination
- Documents improperly exposed due to flood, hurricane, tornado or other disaster
- Documents stolen or missing from premises following a break-in
Situation: Policyholder loses back-up data containing PII

Possible Scenarios

- Remote online storage service used by Policyholder suffers data security breach
- Back-up data tape being shipped to co-location facility is lost or missing
- Custody chain and access of back-up data tape is uncertain due to temporary loss and subsequent recovery of tape
Situation: Policyholder utilizes an outside vendor for services that involve PII or PHI of the Policyholder’s customers, clients, or employees and the vendor had a breach.

Possible Scenarios:
- Payroll processor or benefits provider suffers a breach that exposes employee PII.
- Business process vendors lose data while handling PII for Policyholders.
Situation: Policyholder improperly disposes of documents or equipment that contain PII or PHI of the Policyholder’s customers, clients or employees

Possible Scenarios

• Backup data tape submitted for destruction is unaccounted for
• Documents and/or document destruction storage areas are left unsecured
• Documents/equipment containing PII are improperly disposed of or are recycled or left exposed
**Situation:** Policyholder reports that an employee or contractor accessed files containing PII for reasons unrelated to their job function

**Possible Scenarios**

- A disgruntled employee announced his resignation and then was caught copying files from his computer to a flash drive
- A curious employee accessed his co-workers HR files
Why Can’t companies stop the breaches?