CYBER INCIDENTS

What Happens in the Real World?
Our Experts

Jennifer Lee
Associate
Seal Beach, CA

Amy Yung
Claims Counsel
San Francisco, CA

Nyreese Arzu
Vice President
San Francisco, CA

Brian Alva
Vice President
Cyber Underwriting
Los Angeles, CA
Agenda

• Introduction to the Coverage
• Claims Scenarios
• Third Party Insuring Agreements
• Emerging Coverages
• The Future of Cyber
• Question & Answer
CYBER INCIDENTS

What Happens in the Real World?
## Cyber Insurance Market Conditions – Q2 2019

### Capacity
Market capacity is at an all-time high with over 400 markets actively writing cyber insurance globally. Capacity is now over $750M in limits. Recently there have been an increase in insure-techs.

### Coverage
Coverage continues to evolve and remains highly specialized. Overall, coverage terms and conditions are broadening to the benefit of policyholders and may now include extensions for Crime and Property/GL.

### Losses
After an exponential hike in breaches between 2013-15, loss activity has stabilized and the market has softened for most industries. While frequency of breaches has increased, severity has been reduced as hackers and other malicious actors target smaller organizations. Ransomware continues to be an ongoing issue. Financial demands have escalated from more targeted attacks.

### Retentions
Retentions have remained stable for loss free insureds can be reduced slightly through effective negotiation and marketing. Average retentions in the middle market space are between $5K and $200K with larger organizations seeing retentions of up to $5M+.

### Pricing
Market capacity and competition have led to a very favorable rate environment for policyholders in most industries. There are exceptions, particularly in the higher regulated industries (i.e.- Public Entities, Legal, Title Agents). Rate decreases are often accompanied by new coverage enhancements and present an opportune time for new buyers particularly in the SME sector.

*Provided by PLUS University*
INTRODUCTION TO THE COVERAGE
# The Three Pillars of Cyber Insurance

## Incident Response Coverage
- Forensics
- Legal
- Notification
- Public Relations
- Crisis Management

## First Party Coverage
- Cyber Extortion
- Business Interruption
- Dependent Business Interruption
- System Failure
- Data Restoration

## Third Party Coverage
- Privacy Liability
- Network Security
- Regulatory
- PCI - DSS
- Media

*Provided by PLUS University*
Introduction to the Coverage – Cyber Insuring Agreements (First Party)

• **Triggering Event** – Data Breach, Security Failure, Extortion Threat/Ransomware, System Failure

• **Covered Costs:**
  – **Breach Costs** – legal fees, computer forensics, notifications, call center, identity protection/credit monitoring, crisis management and PR
  – **Data Recovery Costs** – regain access, replace, restore, repair
  – **Business Interruption and Extra Expense** – income loss, extra costs to minimize interruption
  – **Cyber Extortion Costs** – ransom payment, vendor assistance
  – **Reputational Harm** – income loss due to publication of covered event

• **Dependent Business (vs. Insured)**
Introduction to the Coverage – Cyber Insuring Agreements (Third Party)

- **Media Liability** – Insured’s advertising of its services; dissemination of media content
- **Regulatory Investigation** – claim expenses (defense), fines and penalties
- **Payment Card Industry Data Security Standards (PCI DSS)** – contractual fines or penalties for non-compliance; fees
- **Privacy/Security Liability** - assertion of liability, demand against insured
Evolution of Cyber

– Cyber started to emerge in the late ‘90s, mainly as part of other policies focusing on 3rd party exposures
– The regulatory environment pushed privacy coverage forward
  • HIPAA, in the mid-90’s to early 2000’s,
  • California Security Breach and Information Act in 2003
– Mid to late 2000’s stand-alone policies addressing 1st and 3rd party coverages started to become more mainstream, but coverage was still limited
– Our economy has become more connected and exposed and coverage has continued to expand and evolve (Breach outside the limit, Reputation Harm, Business Interruption, Social Engineering)
CLAIMS SCENARIOS
Claims Trends

Percentage of Claims by Sector: 2013–2017
(N=1,201)

*NetDiligence 2018 Cyber Claims Study
Claims Trends

Percentage of Claims by Cause of Loss: 2013–2017
(N=1,201)

- Hacker: 21%
- Ransomware: 15%
- Malware/Virus: 11%
- Lost/stolen laptop/device: 9%
- Phishing: 7%
- Legal Action: 7%
- Staff mistake: 6%
- Rogue employee: 5%
- Business Email Compromise: 5%
- Third Party: 4%
- Paper records: 4%
- Programming Error: 3%
- All Other: 2%

*NetDiligence 2018 Cyber Claims Study
CLAIM SCENARIO I
Cyber Crime: Invoice Manipulation (Reverse Social Engineering)

• “Reverse Social Engineering” Defined – Intentional use of insured’s computer system to mislead or deceive client/vendor; results in client/vendor transferring money intended for insured.

• What Happened:
  – Hacker gained access to insured title services company’s computer system and email
  – Clients: prospective homebuyers
  – Auto-forwarding rules on email accounts
  – Changed wire instructions
  – Resulted in third party claim
Cyber Crime: Invoice Manipulation (Reverse Social Engineering)

• **Breach Costs Coverage Triggered** – legal fees and computer forensics

• **Other Potential Coverages:**
  – Breach Costs
    • Notifications
    • Call Center
    • Credit Monitoring
  – Reputational Harm
“Social Engineering” Defined – Intentional misleading or deception of an insured employee by someone pretending to be the insured’s client, vendor, or employee, which results in the insured transferring money.

What Happened:
- Insured manages school retirement plan
- School teacher discovered that $80,000 was distributed from her account without consent
- Bad actor pretended to be school teacher who has retirement plan managed by insured
- Bad actor submitted withdrawal request containing:
  - Name
  - Date of Birth
  - Address
  - Signature
- No SSN, phone, email, or account number
Cyber Crime: Social Engineering

• **Cyber Crime Coverage Triggered** – Covered amount withdrawn from account and interest the teacher would have earned had the money not been withdrawn

• **Other Potential Coverages:**
  – Breach Costs
  – Reputational Harm
CLAIM SCENARIO II
Capital One Breach

• **What Happened:**
  - March 22, 2019 - breach of personally identifiable information of 100 million individuals in the U. S. and 6 million in Canada

• Information included names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income and:
  - 140,000 Social Security numbers of credit card customers
  - 80,000 linked bank account numbers of secured credit card customers
Capital One Breach
How the Breach Occurred

• Exploitation of a Known Vulnerability

• Misconfigured Open Source Web Application Firewall that Capital One was using as part of its operations hosted in the Amazon Web Services Cloud

• Service Side Request Forgery (SSRF) is one of the most serious vulnerability facing organizations that use public clouds

*Capital One built their own web applications on top of Amazon’s cloud data so they can use the information in ways specific to their needs*
Civil War

Who's Liable?

- Capital One expects to incur between $100 million and $500 million in costs related to the hack, including:
  - Customer notifications
  - Credit monitoring
  - Tech costs
  - Legal support
  - Nines
- Customers are responsible for their security in the cloud
- Often times vendors contractually limit their liability
Capital One Breach
Capital One Breach Insurance Coverage Parts Triggered

- **Network Security Liability** – covers the unauthorized disclosure of personally identifiable information
- **Privacy Liability** – failure to comply with their own privacy policy and resulting lawsuits
- **Regulatory Liability** – fines and penalties assessed by regulators
- **Breach Event Expenses** – customer notifications, credit monitoring, forensic investigation expenses
- **Reputational Harm** – any reduction in profit as a direct result of damage to their reputation
CLAIM SCENARIO III
Managed IT Service Providers

- Vendors handle software updates, network security/firewalls, and backups for their clients
- Hackers exploit vulnerabilities in remote log-in software
- Once the third-party gets access into the vendor’s systems and remote log-in credentials, it pushes out ransomware to clients
- Attractive target due to economies of scale
Managed IT Service Providers
Insurance Coverage Parts Triggered

• **First Party:**
  – Incident response and notice
  – Remediation efforts
  – Business interruption

• **Third-Party:**
  – Breach of Contract
  – Negligence
  – Indemnification to Third Parties
10 MINUTE BREAK
THIRD PARTY CYBER
Privacy and Cyber Security Liability

• **Privacy Liability Coverage Defined:** The purpose of privacy liability coverage is to pay for claim expenses and damages/settlements when a third party makes a claim against the insured that results from a covered data breach, security failure, or extortion threat.

• **Covered costs:**
  – Fees, costs, and expenses incurred by attorneys, forensics, or other experts
    – To investigate, defend, appeal
  – Monetary judgment
  – Monetary award
  – Monetary settlement
Privacy and Cyber Security Liability
Claim Example

• **Reverse Social Engineering Example:**
  • Hacker gained access to insured title services company’s computer system and email
  • As a result, prospective homebuyers lost funds
  • Homebuyers filed lawsuit against insured for negligent network security
  • Covered costs:
    – $100,000 in legal fees
    – $300,000 in forensic/expert costs
    – Settlement amount
Media Liability

- **Media Liability Coverage Defined:** The purpose of media liability coverage is to pay for claim expenses and damages/settlements when the insured’s media activities or advertising of its services results in a third party claim.

- **Categories of Covered Claims:**
  - Intellectual property infringement; unfair practices
  - Privacy claims (i.e., invasion of privacy, publication of private facts, misappropriation)
  - Defamation
  - Unintentional infliction of emotional distress
  - Negligence
Media Liability Claim Example

- **Intellectual Property Infringement**
- Insured is an online marketplace that allows artists to upload images that customers can have printed onto apparel and other items
- Claimant is a video game brand
- Lawsuit for trademark infringement, copyright infringement, and counterfeiting
- Covered costs:
  - Legal fees
  - Settlement amount
Recent Regulatory and Civil Activity

**Regulatory**
- GDPR: British Airways (7/2019): $230 million
- GDPR: Marriott (7/2019): $124 million
- OCR: Medical Informatics Engineering (5/2019): $100K
- OCR: Touchstone Medical Imaging (5/2019): $3 million

**Civil**
- Premera Blue Cross: $10M to states + proposed $74M settlement
- Vineyard Vines: lawsuit, redacted credit card #’s on receipts

*Provided by PLUS University*
Expanding Regulation of Privacy

• New York Cybersecurity Regulation for Financial Institutions
  – requires administrative safeguards such as assessments, policies, training, vendor management, access control, application security, testing and auditing, data retention and destruction, and incident response plans
  – requires technical safeguards including encryption and multi-factor authentication
  – requires 72-hour breach notification and annual compliance certification

• California Consumer Privacy Act of 2018
  – takes effect January 2020 and applies to certain entities that collect personal information about California consumers
  – lets California consumers know what personal information about them is collected and the categories of information shared with third parties
  – limits the sale of personal information
  – creates a right to be forgotten by requiring deletion of personal information
  – afford a private right of action in some circumstances and statutory damages

• Other states have new or recent law affecting privacy and/or cybersecurity requirements (e.g., South Carolina, Colorado and Vermont)

*Provided by PLUS University
Expanding Regulation of Privacy

• Other Countries:
  – Australia – Notifiable Data Breach scheme (eff. 2/22/18)
  – Canada – Data breach notification (eff. 11/1/18)
  – EU-GDPR (eff. 5/25/18). Key GDPR provisions:
    • Higher sanctions
    • Expansions in definitions of what is “personal”
    • Individual right to seek compensation
    • Data breach notification (within 72 hours)
    • Greater data subject rights including greater right to access, rectify or erase data.
    • Fines are escalating in amount and public profile (Google, Marriott, British Airways, LaLiga)

*Provided by PLUS University
California Consumer Privacy Act (CCPA)

• What information is covered?
  – Consumers’ Personal Information
    • Consumer: a natural person who is a California Resident
    • Personal Information (PI): Information that identifies or can identify a person or household
      – Biometric information
      – IP address, internet activity, pixels, beacon, device IDs
      – Purchasing history
      – Inferences drawn from PI to create customer preference profile
California Consumer Privacy Act (CCPA)

- What information is **not** covered?
  - Publicly Available Information
  - PI subject to other regulatory schemes:
    - Confidentiality of Medical Information Act
    - Health insurance Portability and Availability Act of 1996
    - Fair Credit Reporting Act
    - Gramm-Leach-Bliley Act (if in conflict)
    - Driver’s Privacy Protection Act of 1994
California Consumer Privacy Act (CCPA)

• Obligations for Businesses
  – Notice requirement prior to collection
    • Categories of data collected
    • Purpose of collection
    • Sale of Personal Information (PI)
  – Respond to consumer requests for:
    – Consequence
      • Disclosure of Personal Information (PI) collected, sources, purpose and shared
      • Deletion of Personal Information (PI)
      • Opt-Out of sale of Personal Information (PI)
California Consumer Privacy Act (CCPA)

- Consequences of Non-Compliance
  - Enforcement actions by the California Attorney General
    - **Fines**: $2,500 or $7,500, if intentional
    - CA AG will begin enforcement actions **six months after issuing implementing regulations** or **July 1, 2020**, whichever comes first.
  - Private Right of Action
    - In the event of a data security incident
    - If the incident resulted from the failure to implement adequate security measures
    - 30-day notice requirement
    - **Statutory Damages**: $100 to $750 per consumer, per incident
    - **SB 561**: Expands private right of action to allow individuals to bring a civil suit for any violations
California Consumer Privacy Act (CCPA)

• Who is Covered?
  – A **for-profit** business that:
    • **Collects** or **controls** the processing of consumers’ PI;
    • Does **business in California**; and
    • Meets one of the following:
      – $25M in **annual revenue**
      – **PI from 50,000+** consumers, households, or devices per year
      – 50% **annual revenue** from selling PI
  
  – A business that:
    • **Controls** or **is controlled by** a covered business; and
    • Shares **common branding** with the covered business
PCI Fines & Penalties

- PCI Security Standards Counsel was founded by large credit card companies to standardize and promote data security standards. Enforcement is carried out by individual brands (i.e. American Express)
  - In the event of a breach credit card brands can investigate and levy fines
  - Typical coverage includes defense and assessment expenses (forensic investigation, card replacement, fraud recoveries, fines & penalties)
Technology Products & Services

- Third Party E&O coverage for companies who perform technology services for a fee
- It can be written in conjunction with Cyber because there is a cross over in exposure
EMERGING COVERAGES
Hardware Replacement Costs

- Loss of use of a hardware due to an unauthorized reprogramming of software.
- Picks up costs to rebuild, replace or repair hardware.
- Commonly referred to as “Bricking”
Social Engineering

• Cyber Crime vs Crime – Where should it go?

• Loss of funds or property due to a cyber event (usually a compromised email account)
  – Funds Transfer Fraud/Cyber Deception
  – Invoice Manipulation
  – Phishing Attack
Utility Fraud

• Coverage typically includes:
  – Cryptojacking – unauthorized use of computer system to mine cryptocurrency
  – Telecommunications Fraud – unauthorized use of phone system

• Covers an increase in expenses related bloated utility costs (gas, electricity, mobile data, etc.)
THE FUTURE OF CYBER
Silent Cyber

• What is it?
  – Non-affirmative cyber exposure.

• Why now?
  – Increasing concern over cyber aggregation
  – NotPetya and WannaCry ransomware viruses affected large, global businesses
  – Costly, public coverage disputes (Mondelez, Merck)

• What’s next? The market is begging to address the “silent” aspect.
  – Lloyds ”silent cyber mandate”
  – AIG announced that as of January 2020 commercial property and casualty policies will begin affirmatively covering or excluding cyber exposures

• Opportunity – Standalone cyber policies to address new gaps in coverage.
Analytics & Vulnerability Scans

• Digital tools to analyze digital risk
• Software that examines independent data sets and scans IT Security assets of an organization.
• A non-invasive process that does not require applicant permission
• Machine learning can be used to continually analyze data sets to improve precision and analytics
Anatomy of Vulnerability Scan

Score

81
out of 100

Recommendations

LOW IMPACT  Email Security : Email Authentication

DESCRIPTION
Email authentication (SPF or DKIM) is not implemented for 1 domains. Email authentication schemes of SPF and DKIM help prevent email spoofing, a scheme commonly used in phishing attacks. Malicious actors frequently use email to target people with fraudulent messages and also to deliver malicious links and attachments. Email authentication prevents malicious actors from using your domain name to impersonate a member of your organization. Using a domain name trusted by the message recipient increases the likelihood of recipient becoming a victim of the scheme.

RECOMMENDATION
Implement email authentication on all owned domains.

LOW IMPACT  DNS Security : DNS Hijacking (Protection)

DESCRIPTION
We observed that 1 domain is missing domain-hijacking protection settings. Domains are administered by domain registrars. As a third-party to the domain owner, domains are susceptible to hijacking by convincing the domain registrar to grant administrative control to an unauthorized party or to make unauthorized changes to the record.

RECOMMENDATION
Reduce the likelihood of domains being hijacked by requiring strong access control for any domain administration. Implement domain hijacking protection codes and also select reputable domain registrars that provide additional administrative controls. Each domain should have the client/TransferProhibited domain status flag implemented. The client/TransferProhibited flag directs the domain registrar to perform strong authentication of any agent attempting to modify the domain.
Q & A
Ever wonder what happens when a Cyber Incident is reported? Our panel of experts will provide real world examples of how policies have responded to incidents. This insight will help provide a broader understanding of the expansive world of Cyber coverage. The seminar will dive into different insuring agreements and decipher what they mean and how they are applied. A light continental breakfast will be served. CE/CLE: CA (pending)

**Speakers:**

**Moderator:** Nyreese Arzu, Vice President, Lockton Insurance Brokers  
Brian Alva, Vice President, Cyber Underwriting, Corvus Insurance  
Jennifer Lee, Associate, Freeman Mathis & Gary, LLP  
Amy Yung, Claims Counsel, Hiscox

**Your Investment:** Member $35 | Non-member $60

**REGISTER ONLINE!**

Thank You 2019 Annual Sponsors

**PLATINUM**

- Berkley Crime
- Gallagher
- Lewis Brisbois
- WSHB
- KBR

**GOLD**

- Allianz Global Corporate & Specialty  
  Allied World Insurance Company  
  Beazley  
  Fisher & Phillips LLP  
  Hiscox USA  
  Markel

- Philadelphia Insurance Companies  
  RT Specialty, LLC  
  Socius Insurance Services, Inc.  
  Thompson Coe & O’Meara, LLP  
  Travelers  
  Worldwide Facilities, LLC

**SILVER**

- AP Specialty  
  Collins Collins Muir + Stewart, LLP  
  CRC

- Gordon Rees Scully Mansukhani, LLP  
  Ironshore Insurance Services  
  Pleiss Sitar McGrath Hunter & Hallack