Cybersecurity: Emerging Threats & Legal Landscape

Alyssa Watzman
Lewis Brisbois Bisgaard & Smith LLP
August 21, 2019

Contact: Alyssa.Watzman@lewisbrisbois.com
(O) 720-292-2052; (C) 240-398-8255
Agenda

1. Trends in Data Security
2. Legal Landscape
3. Financial Implications
4. Questions
1. Trends in Data Security
Social Engineering Attacks

- Email Account Compromises
  - Credential Harvesting
  - Spear Phishing

- Attack Monetization
  - Sensitive Data Sales
  - Wire Transfer Redirects
  - Direct Deposit Redirects
  - W2 Image Exploits

- Prevention
  - Two-factor authentication
  - Employee Training / Testing
  - Spam Filtering
Extortion Attacks

- Increasing Ransom Demands
  - Attacker Reconnaissance
  - Back-Up Data Encryption
- Accompanying Attacks
  - Banking Trojans
  - Distributed Denial of Service
- Ransomware Ruse
- Prevention
  - RDP Ports
  - End-Point Monitoring
  - Employee Training / Testing
  - Patch Management (Kaseya)
System Intrusion Attacks

- Payment Card Data
  - E-Commerce site hacks
  - POS systems

- Malicious Network Use
  - BotNet Launching Sites
  - Stolen Records Storage
  - Crypto-Mining

- Intellectual Property Theft
A sophisticated cyber underground exists through which malicious actors, acting either alone or in groups, sell a variety of services.

- **Criminal Online Forums**: Criminals operate through a variety of online forums to buy / sell products and services.
- **Bullet Proof Hosting**: Criminals operate dedicated servers / domains to provide a vital infrastructure for hosting infected web sites, malware, botnet command and control stations, VPNs and proxies
- **Data Monetization**: Sensitive data sales
- **Coding Services**: Criminals customize malware, tailoring it to specific targets and improving its ability to bypass anti-fraud mechanisms
- **Anti-Virus Services**: Criminals run malware through numerous anti-virus products to maximize infection rates.
- **Exploit Kits**: Criminals utilize a variety of tools to identify and exploit vulnerabilities on victim systems
- **Anonymization**: Criminals employ means to communicate securely and to receive untraceable payments (i.e. virtual currencies)
Lessons Learned

• **Targets:** Businesses in all locations, in all industries, and of all sizes
  – Especially accounts receivable / invoicing or HR

• **Sophistication:** Attacks are increasingly sophisticated
  – Attacker due diligence / “Spear phishing”

• **Frequency:** Businesses are targeted daily by email / brute force attacks

• **Success:** Increasingly successful encryption attacks
  – Enterprise ransomware
  – Negotiation of ransom unsuccessful
  – Bitpaymer, Ryuk, Trickbot (propagate within and beyond email)
  – Increasing ransom demands
2. Legal Landscape
Regulatory Environment (1/2)

- Regulators have operations budgets funded by assessments
- State Regulations
  - 50 State Statutes (plus D.C., Guam, Puerto Rico, Virgin Islands).
  - Require Consumer Notification: Statutes require notification for breaches of unencrypted personal information (“PI”).
  - Notification Obligation Identification: Notification obligations are determined by the location of the consumer, not the business.
  - PI Definition: PI is generally defined as first name or initial and last name, combined with one or more of the following data sets:
    - All states include SSN, DL or State ID Card Number, or financial account information with means to access the account.
    - Some states add medical information, health insurance information, biometric information, online credentials, etc.
State Regulations (Cont.)

- **Notification Timing**: Statutes generally require notification in the “most expedient time possible”. **In WA, the time limit is 45 days.**
- **Regulatory Notification**: 25+ states require notification of state regulatory officials where notification is provided to state residents.
- **Information Security Standards**: Required security programs.

Federal Regulations

- HIPAA – Privacy Rule, Security Rule, Breach Notification Rule
- Securities Exchange Act
- FERPA

PCI DSS Regulations
Regulatory Trends

• **Definition of PII expansion**
  - **GDPR**: Regulates information about any person who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, an online identifier, or to factors specific to one’s physical, physiological, genetic, mental, economic, cultural, or social identity.
  - **CCPA**: Regulates information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

• **Shortening of notification timeframes**
  - **GDPR**: Data controllers must report a breach to relevant data protection authorities within 72 hours (where “feasible”) of discovery of the breach.
  - **US**: Approximately 15 states require notification within a specified timeframe.

• **Rights of data subjects**
  - Right to Information: Data subjects have the right to know what information is collected
  - Right to be Forgotten: Data subjects may ask a data controller to erase their personal data

• **Increasing penalties**
  - **GDPR**: 20 million Euros or up to 4% of annual revenue
  - **CCPA**: $2,500 per violation or $7,500 per intentional violation (no cap)
3. Financial Implications
Financial Implications

- **First-party costs:**
  - Data loss; software loss; hardware loss;
  - Income loss; business interruption costs; restoration costs;
  - Cyber extortion; other crime loss.

- **Third-party costs:**
  - Media liability (copyright and trademark infringement); privacy liability for breach of privacy; bodily injury;
  - Litigation: class actions; derivative actions; regulatory actions.

- **Remediation costs:**
  - Legal services; forensics services; crisis management services; costs associated with notification and monitoring services.

- **Fines and penalties:**
  - Expenses of regulatory investigations; civil judgments; fines and penalties levied by regulatory authorities; and fines and penalties for payment card industry compliance violations.
Anatomy of a Data Breach

Alyssa Watzman – Lewis Brisbois Bisgaard & Smith LLP
Greg Pendleton – Gordon Tilden Thomas & Cordell LLP

August 21, 2019
Security Incident Lifecycle

1. Preparation
2. Detection & Analysis
3. Containment, Eradication & Recovery
4. Post-Incident Activity
Preparation

- **Insurance**: Discuss cyber coverage.
- **Stakeholders**: Identify those responsible for data management (i.e. IT, HR) and those who are first responders (i.e. Legal, CEO).
- **Data Review**: Identify the types of data you collect / process (i.e. PII / PHI / PCI), where that data is stored, and how it is protected.
- **Compliance**: Identify applicable laws and the requirements thereof for compliance.
- **Incident Response Plan (“IRP”)**: Develop a risk assessment and mitigation plan.
- **Policies + Procedures**: Develop policies and procedures for compliance.
- **Table-Tops**: Exercises to test the IRP.
Detection & Analysis

• **Preliminary Assessment**: Conduct an assessment with IT personnel.
  – Review evidence of unauthorized access
  – Review evidence of potentially impacted data sets
  – Determine if there is an ongoing threat and, if so, implement the IRP.

• **Internal Notification**: Notify those in your organization who need to know.
  – Not every incident triggers external notification
  – Choose your words carefully as emails can be discoverable
  – Note the date and time of incident discovery (notification timelines)
  – Privilege considerations

• **External Notification**: Assemble a response team including key partners.
  – Broker / Insurer (Coverage)
  – External breach counsel (Privilege / Coordination)
  – Forensic investigation firm (Containment / Remediation)

• **Data / Document Preservation**
Containment & Recovery

- **Preliminary Containment**: Work with IT personnel to contain the incident.
  - Disable accounts and change passwords
  - Block malicious IP addresses / URLs
  - Isolate impacted systems
  - Preserve digital evidence, including critical logging data

- **Investigate**: Determine whether sensitive data has been impacted.
  - Privilege considerations
  - Involve a forensic firm to analyze unauthorized access or acquisition
  - Involve law enforcement as appropriate

- **Legal Analysis**: Determine whether the incident is reportable
  - State data breach notification statutes
  - Federal laws (i.e. HIPAA)
  - Crisis communications
Post-Incident Activity

• **Notification**: Notify consumers and regulators as necessary.
  – Consumers: Call center, Credit monitoring / Identity Protection
  – Regulatory Agencies: State Attorneys General, HHS/OCR
  – Third Parties: Contractual Obligations
  – Media: If required by law.
  – Law Enforcement

• **Follow-Up Inquiries**: Response to requests for additional information.
  – Regulators: Indiana AG, HHS/OCR
  – Media

• **Final Report**: Consider how to prevent similar occurrences in the future.
Mistakes to Avoid (Pre-Claim)

• Not selecting appropriate coverage limits – be aware of sub-limits!
• Ignoring conditions precedent to coverage
  – Review coverage with your broker or coverage counsel
  – Underwriting negotiations: are your security protocols and procedures commercially reasonable?
  – Adopt and implement conditions precedent
  – Train and educate employees
• Not taking advantage of pre-claim consultation services.
Mistakes to Avoid (All Claims)

• Not calling your insurance broker / carrier / lawyer immediately
• Not using appropriately skilled and resourced vendors
• Choosing vendors without pre-approval from carrier
• Not understanding your coverage
  – Cyber policies can contain both first-party and third-party coverage.
  – Insuring agreements can be written on “occurrence” or “claims made” basis
  – For late-noticed claims, must the insurer show prejudice in your jurisdiction?
• Not providing appropriate internal notification
Mistakes to Avoid (Extortion)

• Attacker Communications
  – Failing to utilize an anonymous email domain
  – Disclosing information about the victim’s infrastructure
  – Unresponsive or aggressive communication
• Ransom payments
  – Failing to exhaust other resources for decryption keys
  – Failing to require “proof of life” before payment
  – Failing to ensure that payment comports with OFAC regulations
• Critical Evidence Preservation
  – Wiping devices without obtaining forensic images
  – Failing to preserve all network and firewall logs
• Enabling operations without identifying and securing vulnerabilities
  – Failing to conduct a global password reset / update default passwords
  – Failing to disable unsecured RDP accessibility
• Making unnecessary public statements
Mistakes to Avoid (Data Exfiltration)

- Not calling your insurance broker / carrier immediately.
- Not using appropriately skilled and resourced vendors.
- Critical Evidence Preservation
  - Wiping devices without obtaining forensic images
  - Allowing event and access logs to roll over on relevant evidence
- Allowing continued use of compromised email account
  - Failing to require a global password reset / complex passwords
  - Failing to audit user accounts and disable those not in use
  - Failing to investigate and remove malicious rules
  - Failing to implement dual factor authentication
- Making unnecessary public statements
- Failing to monitor fraudulent activity
  - Wire transfers / Invoices
  - Direct deposit re-directs
  - Spear phishing
Mistakes to Avoid (Wire Transfer Re-Directs)

• Not immediately contacting the FBI
  – File a written IC3 Report
  – Attempt to initiate the “Financial Fraud Kill Chain”

• Allowing continued use of compromised email account
  – Failing to require a global password reset / complex passwords
  – Failing to audit user accounts and disable those not in use
  – Failing to investigate and remove malicious rules
  – Failing to implement dual factor authentication

• Failing to monitor fraudulent activity
Prevention and Response

- **Improve cyber defense**
  - Email and spam filtering
  - Endpoint monitoring

- **Improve human defense**
  - Employees must protect against cyber threats
  - Malicious actors use social engineering to thwart all the technological perimeter defenses
  - Regular training
Presenters

• Alyssa Watzman, Lewis Brisbois Bisgaard & Smith LLP
• Greg Pendleton, Gordon Tilden Thomas & Cordell LLP
• Michael Handler, Cozen O’Connor
• Kip Boyle, CEO of Cyber Risk Opportunities

Moderators

• Peter Marchel, Marchel Risk Consulting LLC
5th ANNUAL CYBER LIABILITY SYMPOSIUM

Cyber Claims Litigation

August 21, 2019
Seattle, Washington

Michael Handler, Cozen O’Connor: mhandler@cozen.com
Greg Pendleton, Gordon Tilden Thomas & Cordell: gpendleton@gordontilden.com
I. Background of Stand-Alone Cyber Coverage
   A. Evolution of cyber crime
   B. Types of coverage

II. Key Coverage Cases
   A. Data Breach Events, Social Engineering, Hacking
   B. Common Coverage Defenses

III. Interplay Between Cyber Coverage and Other Policies
   A. Insurer Coverage Counsel Perspective
   B. Policyholder Coverage Counsel Perspective
A Decade of Growth

- Cyber attacks are the fastest growing crime in the U.S.
- 61% of companies based in the U.K., the U.S., and Europe reported being hit by one or more attacks in 2018, compared with 45% in 2017.
- Companies lost $369,000 on average in 2018 after being attacked, compared with $229,000 in 2017.
- Experts predict cybercrime will cost the world in excess of $6 trillion annually by 2021, up from $3 trillion in 2015.

Types of Cyber Crime

• Social Engineering – Phishing, Spear Phishing, Whaling
• Hacking and Computer Fraud
• Funds Transfer Fraud and Fraudulently Induced Transfers
• Ransomware and Cyber Extortion
• Confidence Tricks and Advance Fee Scams
Investigation Costs

Legal Liability

Regulatory Liability

Business Interruption

Direct Theft Costs

Customer Relations & Reputation

Costs of Cyber Crime
Types of Cyber Insurance

**Third Party Liability**
- Commercial General Liability
- Professional Liability (D&O and E&O)
- Cyber Liability

**First Party**
- Commercial Crime
- All Risk
- BOP
- FI Bonds
- Stand-Alone Cyber
Types of Cyber Insurance – Stand Alone Cyber

- Incident Response
- Legal and Regulatory
- Crisis Communication
- Privacy Breach Management
- Funds Transfer Fraud
- Fraudulently Induced Transfer
- Theft of Funds Held in Escrow
- Extortion

- Identity Theft
- Telephone Hacking
- Phishing
- System Damage & Rectification
- Business Interruption
- Reputational Harm
- Loss Adjustment Costs
- Liability – network security, privacy, management, regulatory fines
Cyber Coverage in the Courts

- **CGL Coverage**

- **Coverage for PCI Fees**

- **Professional Liability Coverage**
  - Defense cost coverage? *Spec’s Family Partners, Ltd. v. Hanover Insurance Co.*, 739 Fed. App’x. 233 (5th Cir. 2018) (defense cost reimbursements for an underlying lawsuit about the insured’s credit card processor charges.)
Cyber Coverage in the Courts

Ninth Circuit

- Pinnacle Processing (W.D. Wash. 2011)
- Taylor & Liebermann (2017)
- Pestmaster (2016)
- Aqua Star (2018)

Sister Jurisdictions

- Apache Corp. (5th Cir. 2016)
- Medidata (2d. Cir. 2018)
- American Tooling (6th Cir. 2018)
Common Coverage Defenses

• No “Direct” Loss

• Transfer of Funds not “Unauthorized”
  - *Aqua Star* (9th Cir. 2018)

• Voluntary Parting Exclusions
  - *Schweet Linde & Coulson v. Travelers* (W.D. Wash. 2015)

• Claims-Made Defenses

• Voluntary Payment Clauses
Interplay Between Cyber Coverage and Other Policies

- Insurer Coverage Counsel Perspective
- Policyholder Coverage Counsel Perspective
Questions?
Fifth Annual Cyber Liability Symposium
Wednesday, August 21, 2019 | 1:00 - 7:00 p.m.
1:00 PM Registration/Check-in
1:30 PM - 5:00 PM Cyber Seminar
5:00-7:00 PM Happy Hour Networking Reception

Cybersecurity: Emerging Threats & Legal Landscape

- Cybersecurity: Emerging Threats & Legal Landscape
- Anatomy of a Data Breach
- Claims Litigation
- Preparing for the Incident Before it Happens

What are the reasonable management practices insurance professionals should be employing to assist insureds in making a claim? Experts will discuss the latest trends in Cyber Data Security, the most commonly encountered types of incidents and the lessons learned from participating in a team that is poised to assist with 1000+ data security incidents this year, and the related ever-changing legal landscape. Learn how to prepare for a data security incident and as to what happens from the time a claim is discovered to the time that it is contained, and remediated, and what mistakes to avoid during this process. CE/CLE pending in OR, WA.

Speakers:
Kip A. Boyle, CEO, Cyber Risk Opportunities LLC
Michael D. Handler, Member, Cozen O’Connor
Greg D. Pendleton, Partner, Gordon Tilden Thomas & Cordel
Alyssa R. Watzman, Partner, Data Privacy, Lewis Brisbois Bisgaard & Smith LLP
Moderator:
Peter Marchel, Esq., President, Marchel & Associates Risk Consulting

Program
One Union Square Board Room
600 University Street, Seattle, WA 98101

Reception
Hagerty’s Lower Club Room at the Washington Athletic Club
1325 Sixth Ave, Seattle WA 98101-1709

Your Investment: Member $80 | Non-member $80 | Other Fees $80 RIMS Member, $80 CPCU Member

Thank you
2019 PLUS Northwest Annual Sponsors

PLATINUM
Cooper & McCloskey Inc.

GOLD
Cozen O’Connor

SILVER
Gordon Rees Scully Mansukhani, LLP

REGISTER ONLINE!
August 21, 2019
1:00 – 4:30
One Union Square Board Room, Seattle, WA
Fifth Annual Cyber Liability Symposium

1:00 – 1:25 pm Registration

1:25 – 1:30 pm Program Overview
Peter Marchel – Marchel & Associates Risk Consulting

Alyssa Watzman – Lewis Brisbois

a. Trends in Data Security (20 minutes)
   a. Social Engineering Attacks
   b. Extortion Attacks
   c. Hacking / System Intrusions
   d. Monetization
   e. Lessons Learned

b. Legal Landscape (15 minutes)
   a. The Regulatory Environment
   b. Regulatory Trends

   c. Financial Implications (5 minutes)

Synopsis: Our objective is to provide the audience with genuine information regarding types of cyber incidents currently occurring. The speaker will discuss the most commonly encountered types of incidents, lessons learned from participating in a team that is poised to assist with 1000+ data security incidents this year, and the related ever-changing legal landscape.

2:15 – 2:30 Break - 15 Min.
Anatomy of a Data Breach - 60 Min.
Alyssa Watzman – Lewis Brisbois
Greg Pendleton – Gordon Tilden

**Synopsis:** Our objective in this session is to provide the audience with guidance as to how to prepare for a data security incident and as to what happens from the time a claim is discovered to the time that it is contained, and remediated. We will also address mistakes to avoid during this process.

In this 60-minute session, we will discuss preparing and making a claim:

1. Security Incident Lifecycle (10 minutes)
   - Preparation
   - Detection & Analysis
   - Containment & Recovery
   - Post-Incident Activity

2. Mistakes to Avoid (Coverage) (30 minutes)
   - Take advantage of pre-claim consultation services
   - Selecting appropriate coverage limits
     - Be aware of sub-limits
   - Conditions precedent to coverage
     - Reviewing coverage with brokers and coverage counsel
     - Underwriting negotiations – are your security protocols and procedures commercially reasonable?
     - Adopting and implementing required verification procedures
     - Educating employees
   - Incident Response – Coordinating with the insurer
     - Selection of vendors
     - Avoiding unnecessary coverage disputes
     - Internal and External notification
   - Notifying your insurer
     - Cyber policies can contain both third-party and first-party coverage
     - Claims-made versus occurrence coverage
     - For late-noticed claims, must the insurer show prejudice in your jurisdiction?

3. Mistakes to Avoid (Incident Specifics) (10 minutes)
   - Extortion
4. Prevention and Response (10 minutes)

Our objective is to focus heavily on the reasonable management practices insurance professionals should be employing to assist insureds in making a claim.

3:30 – 3:45 Break - 15 minutes

3:45– 4:35 Claim Litigation - 50 minutes

Michael D. Handler, Member, Cozen O’Connor
Greg D. Pendleton, Partner, Gordon Tilden Thomas & Cordell LLP

Background of Stand Alone Cyber Coverage and Evolution to Date (10 Mins)

a. Cyber coverage is subject to as many variations as there are insurers in the market.

b. First party coverages.

c. Third party coverages.

d. Differences from Professional Liability policies; and CGL Policies.

Touchstone Cases on Insurance Coverage for Data Breach Events (15 Mins)


Recent Case Law on The Above (and Developing) Coverage Issues (15 mins)


- **Social Engineering and Other Fraud**


  ii. 2018 opinions in the Ninth Circuit consistent with strictly applying computer-fraud provisions of a crime insurance policy.

- **Common Coverage Defenses to Emerging Insurance Claims**

  - Claims-made defenses and potential gaps to be aware of.
- Voluntary payment clauses and other conditions precedent.

Interplay Between Cyber Coverage and Other Policies (10 mins), Incl. hypothetical questions

- (Handler) Insurers’ Coverage Counsel’s Perspective on Advanced Coverage Issues, Endorsements For Specialized Risks, and responses to case law trends to find no coverage for a incidents under CGL and/or Crime policies.

- (Pendleton) Personal/Policyholders’ Counsel’s Perspective: locating coverage, or at least reimbursement for defense costs under PL policies; and more emerging issues.

(Both) Concerns for PL Insureds: e.g., law firms entrusted with clients’ financial interests.

4:35 – 5:05 Preparing for the Incident before it happens - 30 minutes
Kip Boyle – Author of “Fire Doesn’t Innovate, founder and CEO of Cyber Risk Opportunities.

Synopsis: With limited resources (money, and time), Kip will provide a three phase approach that will help audience members safeguard their own business from cyber attacks.

5:10 – 5:20 Wrap up / Questions

5:20 – 7:00 Happy Hour