ANDERSON KILL, L.L.P.
ATTORNEYS AND COUNSELORS AT LAW

ACC Baltimore

Fleming Prime Steakhouse
December 6, 2018
12:00 pm – 1:30pm

INSURANCE FOR DATA BREACHES: The Nitty-Gritty of Getting Claims Paid

Disclaimer

The views expressed by the participants in this program are not those of the participants' employers, their clients, or any other organization. The opinions expressed do not constitute legal advice, or risk management advice. The views discussed are for educational purposes only, and provided only for use during this session.

SPEAKER:

Rhonda D. Orin, Esq.
Partner
Anderson Kill
Washington, DC
(202) 416-6549
rorin@andersonkill.com

Rhonda D. Orin is the managing partner of the firm's Washington, D.C. office.

Rhonda represents policyholders in coverage cases nationwide, including cyber liability, third-party tort and environmental liability claims, first-party property damage and business interruption claims, directors & officers liability, errors & omissions liability, fidelity bonds and alternative risk transfer arrangements, including for employee benefit plans. She has served as lead counsel in multiple jury and bench trials, argued before the highest courts of several states, and appeared in two cases before U.S. Supreme Court. Over her career, Rhonda has recovered more than a billion dollars for policyholders, including nine-figure recoveries. She has been honored repeatedly for her expertise and results, including recognition by Best Lawyers, The Legal 500, Business Insurance, the Women's Bar Association of DC and many other organizations.

SPEAKER:

Daniel J. Healy, Esq.
Partner
Anderson Kill
Washington, DC
(202) 416-6547
dhealy@andersonkill.com

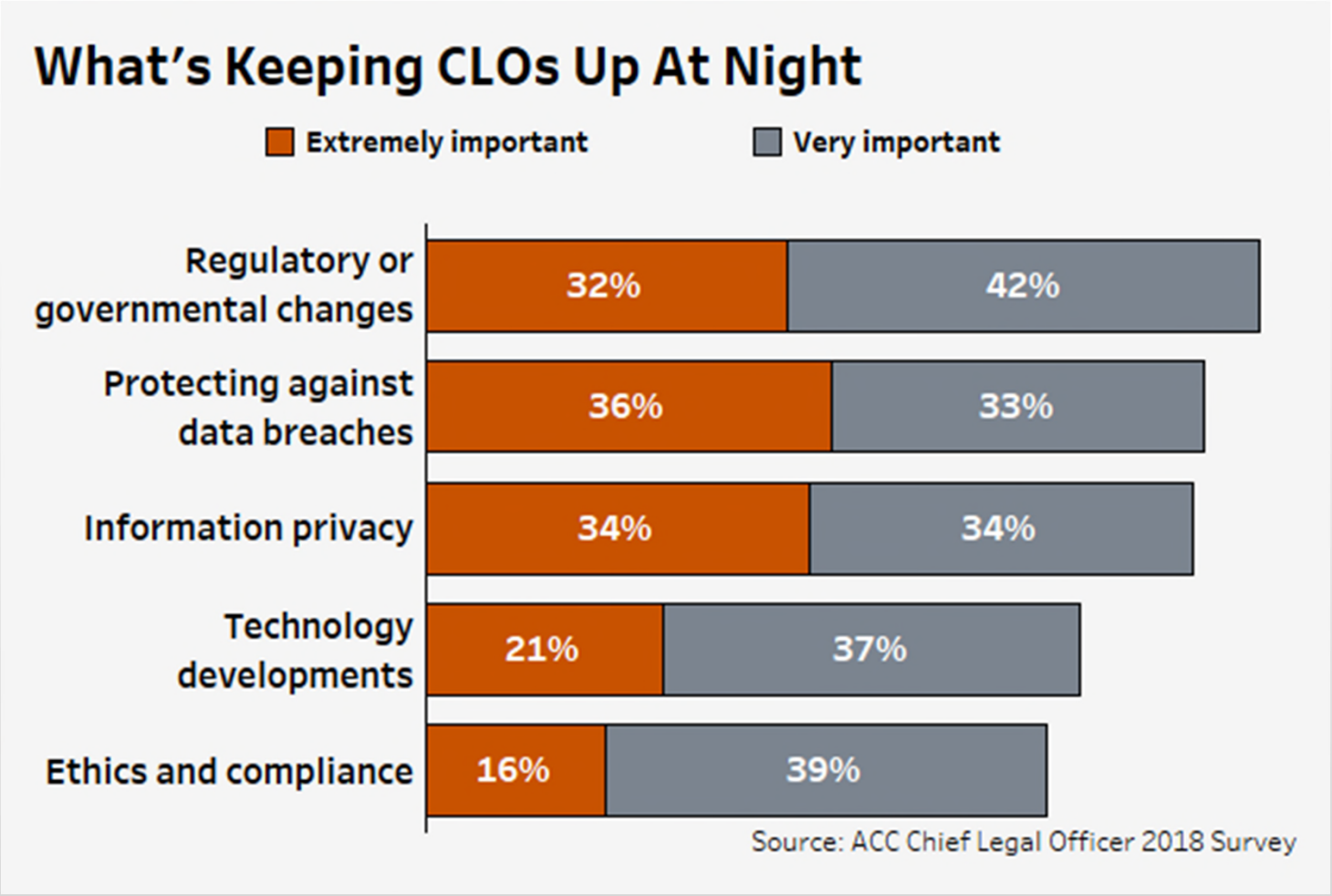
Daniel J. Healy is a partner in Anderson Kill's Washington, D.C. office. He started his career with Anderson Kill and then served over five years as a Trial Attorney with the U.S. Department of Justice, Tax Division. He appeared as lead trial counsel in federal and state courts across the country, received numerous Outstanding Attorney awards and served as the E-Discovery Coordinator for the Tax Division.

Dan currently is the Co-Chair of Anderson Kill's Cyber Insurance Recovery Practice Group, and a member of the firm's Blockchain & Virtual Currency and Regulated Products Groups. He was selected by his peers for inclusion in The Best Lawyers in America for Insurance Litigation and was recognized by Super Lawyers as a Super Lawyer for Insurance Coverage.

He represents policyholders seeking insurance coverage. He has experience obtaining coverage under a variety of insurance policies for corporate policyholders. He has successfully represented railroads, banks, financial service providers, manufacturers, retailers, technology companies and food and beverage providers, including through jury trial.

Dan also litigates all areas of intellectual property. He regularly writes and speaks about insurance recovery and IP issues and was a co-editor of a book entitled *ADR and the Law* published jointly with the American Arbitration Association.

SO WHAT'S THE PROBLEM?



WHO ARE THE THREATS?

MORE THAN HOODED SILHOUETTES

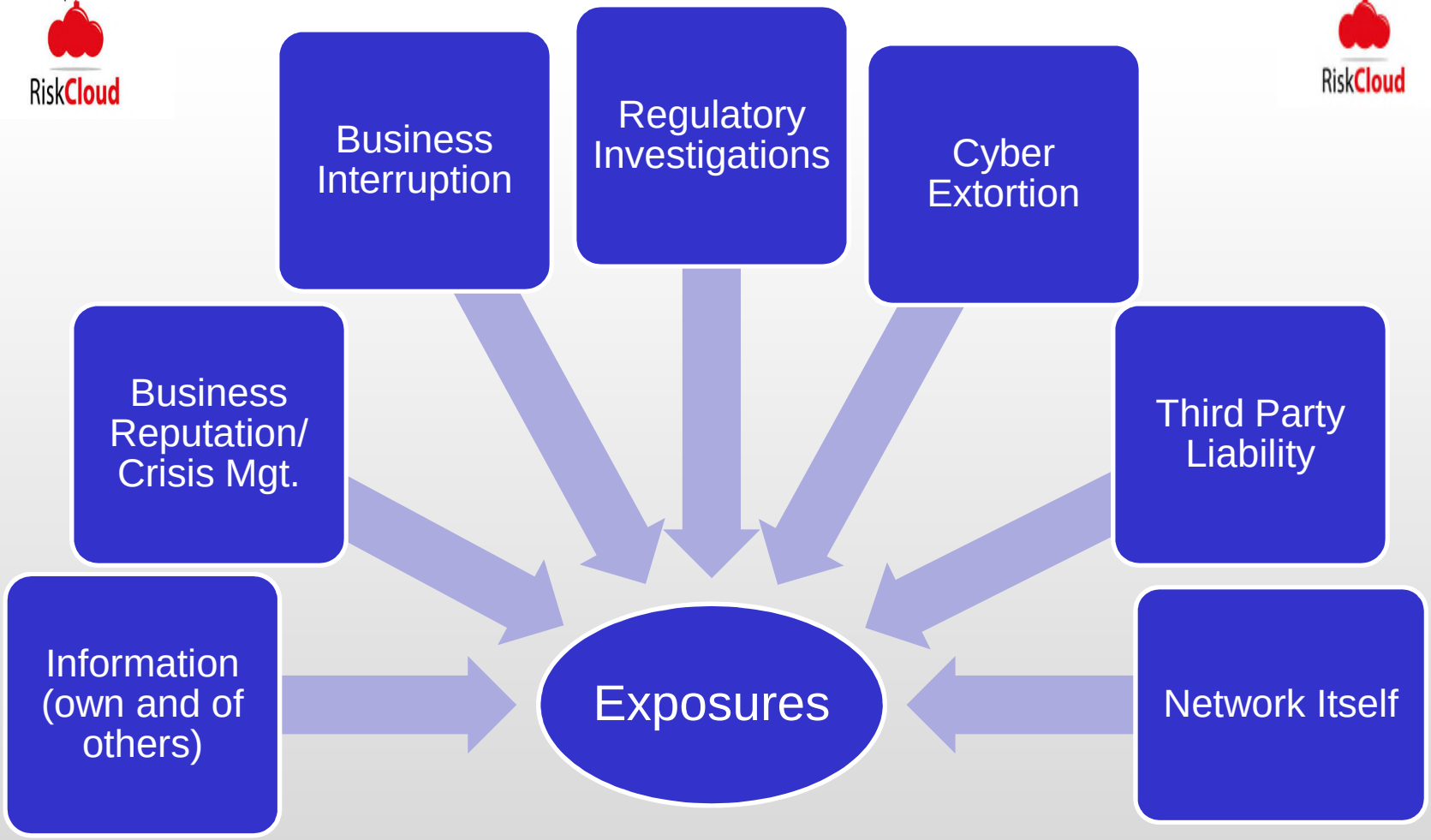
- The modern cyber risk landscape is populated by threat actors with myriad motivations.
- Some attack targets, but many are opportunists who attack vulnerabilities wherever found.
- Attack methods can very from highly-targeted and deliberate attacks that develop over months, to mass-scale, self-spreading malware.

REGULATORY ENVIRONMENT

- NIST, FTC, HHS, FDA & SEC/FINRA
  - Top down governance issues
  - Industry standards and norms for evaluating reasonableness
  - Handbooks, guidance and other literature
  - Section 5 of Federal Trade Commission Act ("FTC Act")

- FEDERAL REGULATORY ENFORCEMENT
  - FTC v. Wyndham Worldwide
  - FTC v. Uber
  - SEC v. Craig
  - SEC v. McKeown and Ryan
  - OCR – Presence Health
  - OCR – Children's Medical Center of Dallas

ALIGNING POTENTIAL RISKS WITH COVERAGE



EVALUATING COVERAGE

- First-party losses
- Liability (third-party) claims
- Gaps, overlapping policies and definitions
- Exclusions

FIRST STEPS

- Identify all potentially applicable policies.
  - Your own, and those of others (vendors, banks)
- Provide timely notice - Even if you're told there's no coverage!
- Assemble the Team.
- Determine immediate proof of loss/documentation requirements.

FIRST-PARTY COVERAGE ISSUES

- Crime Policy
- 11 coverage parts
  - Employee theft
  - Premises Coverage
  - In Transit
  - Forgery
  - Computer Fraud
  - Funds Transfer Fraud
  - Money Orders and Counterfeit Currency Fraud
  - Credit Card Coverage
  - Employee Theft/Forgery
  - Expense Coverage
  - Social Engineering Fraud Coverage “Endorsement”

FIRST-PARTY COVERAGE (CONT'D)

- Identify and target the best/most likely provisions of the applicable policies.
  - Avoid needless fights.

- Most likely coverages in this case.
  - Computer Fraud
  - Forgery
  - Funds Transfer
  - Social Engineering

COMPUTER FRAUD INSURING CLAUSE

- "The Company shall pay the Organization for direct loss of Money ... sustained by an Organization resulting from Computer Fraud committed by a Third Party."

- "Computer Fraud [is] the unlawful taking or the fraudulently induced transfer of Money ... resulting from a Computer Violation."

COMPUTER FRAUD INSURING CLAUSE (CONT'D)

- "Computer Violation" → "the fraudulent (a) entry of Data into or deletion of Data from a Computer System; (b) change to Data elements of program logic of a Computer System, which is kept in machine readable format or (c) introduction of instructions, programmatic or otherwise, which propagate themselves through a Computer System," directed against an Organization.

- "Data" → "a representation of information, knowledge, facts, concepts or instructions which are processed and stored in a Computer System."

BUT – "SOCIAL ENGINEERING" ENDORSEMENT

- Coverage "for loss resulting from an Organization having transferred, paid or delivered any Money or Securities as the direct results of Social Engineering Fraud committed by a person purporting to be a Vendor, Client or an Employee who was authorized by the Organization to instruct other Employees to transfer Money or Securities."

- "Social Engineering Fraud means the intentional misleading of an Employee, through misrepresentation of a material fact which is relied upon by an Employee, believing it to be genuine."

- **Excludes** coverage for "loss or damage due to ... Forgery, Computer Fraud, Funds Transfer Fraud[.]"

KEY CRIME CASES

- *Medidata Sols., Inc. v. Federal Ins. Co.*, 268 F.Supp. 3d 471 (S.D.N.Y. 2017), *aff'd*, 729 Fed. Appx. 117 (2d Cir. July 6, 2018).
- *American Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co.,* 16-12108, 2017 US Dist. LEXIS 120473, *rev'd*, 895 F.3d 455 (6th Cir. 2018).
- *Principle Sols. Grp. v. Ironshore Indem.,* Inc., No. 1:15-CV-4130-RWS, 2016 U.S. Dist. LEXIS 194245 (N.D. Ga. Mar. 22, 2016).
- *Pestmaster Servs. v. Travelers Cas. & Sur. Co. of Am.*, 2014 U.S. Dist. LEXIS 108416 (C.D. Cal July 17, 2014).
- *Apache Corp. v. Great Am. Ins. Co.*, 662 Fed. Appx. 252 (5th Cir. 2016).

THIRD-PARTY COVERAGE ISSUES

- Not Crime policies; Cyber and E&O
- For claims against the insured
    - Usually fraud or similar misuse of compromised data
- Scope of Coverage
- Key Exclusions
  - Contractual Liability

CYBER COVERAGE

Over 12 Coverage Parts:

- Network Security & Privacy Liability Coverage
- Media Liability Coverage
- Professional Services Liability
- Technology Services Liability
- Incident Response (Breach Consult./Data Forensics/Breach Resp./Public Rel.)
- PCI Expenses Coverage
- Network Extortion
- Cyber Crime Coverage
- Data Restoration Coverage
- Business Interrupt. & Extra Exp.
- Supplemental Expenses Coverage
- Disciplinary Proceedings

P.F. Chang's China Bistro v. Fed. Ins. Co.

- *2016 U.S. Dist. LEXIS 70749, 2016 WL 3055111 (D. Ariz. 2016)*
  - $50,000.00 — Case Management Fee
  - $163,122.72 — ADC Operational Reimbursement
  - $1,716,798.85 — ADC Fraud Recovery

- Privacy Injury – BAMS not injured
- Notification Costs – whose costs?

P.F. Chang's (cont.)

- **Exclusion**
  - With respect to all Insuring Clauses, [Federal] shall not be liable for any Loss on account of any Claim, or for any Expense . . . based upon, arising from or in consequence of any . . . liability assumed by any Insured under any contract or agreement

- **Definition**: PCI Expenses means expenses assessed against an Insured pursuant to a Payment Card Industry Data Security Standards (PCI DSS) Merchant Services Agreement, …

INDEMNIFICATION

Contractual Liability, is it covered or excluded?

1) Do you have liability insurance coverage for indemnity obligations?
    - Probably yes.
2) Where is that coverage?
    - (Hint: it starts with C, ends with L and has G in it)
    - The contractual liability exclusion has a carve back, usually for “Insured Contracts”

INDEMNIFICATION

- Carve back:

Assumed Liability of Insured

The **Insured Entity** is insured for liability it assumes in a written contract … under which it assumes the tort liability (liability that would be imposed by law in the absence of any contract or agreement) of another party incurred by such third party as a result of an **Insured's Wrongful Act** … provided:

a. liability to such party … has also been assumed in such contract …; and,

b. such attorney fees and litigation expenses are for defense of that party against a civil or alternative dispute resolution proceeding in which **Damages** to which this insurance applies are alleged….

LOSS CATEGORIES

"Loss does not include:

a. taxes, fines, and penalties, except for those fines and penalties for a Network Security and Privacy Wrongful Act ...;

b. profits, future royalties, costs of licensing, ..., or disgorgement …;

c. the costs to comply with orders ...;

d. remedies due pursuant to a contractual provision, ... except to the extent that an Insured could be held liable in the absence of such contract or agreement;

e. matters that are uninsurable under applicable law; [GDPR?]

f. … upgrade of computers, ...;

g. any cost … to correct ... any Professional Services … except … [to] settle …

h. the return, reinvestment, reimbursement or replacement of funds, ..."

REGULATORY INVESTIGATIONS

- Defense costs, exclusions for salaries and overhead
- Coverage for outside counsel and others
- Coverage for fines and penalties

WHAT CAN TRIGGER COVERAGE?

- "Claim" defined including "civil, arbitration, administrative or regulatory proceeding against any Insured commenced by … the filing of a notice of charge, investigative order or like document." (D&O)

- "Claim" means …
    1. written demand for monetary, … or injunctive relief;
    2. civil proceeding ...;
    3. administrative or regulatory investigation,...;
    4. alternative dispute resolution proceeding; or
    5. written request to toll or waive a statute of limitations

COVERED LOSS

Cyber policy “Loss” may include

- fines and penalties assessed pursuant to any law or regulation in any local, state, federal or foreign jurisdiction for a Network Security and Privacy Wrongful Act;
- any amounts an Insured becomes legally obligated to pay as a result of a Claim;

EXCLUSIONS

- Breach of contract (unless liable in absence of a contract)
- Patent infringement / Misappropriation of Trade Secret
- Return of Fees or Recall Expense
- Direct Bodily Injury or Property Damage (mental anguish/distress from Cyber breach?)
- False/Deceptive Advertising
- Known network security vulnerabilities
- Unsolicited communication
- Unauthorized or wrongful collection of information (coverage varies)
- Breaches or security failures that began prior to retro date
- Intentional acts or fraud by management
- Liquidated damages
- Coupons, discounts, or incentives to Insured's customers
- System upgrades or repairs
- Cyber Terrorism and Cyber War

WATCH OUT!

- Fear of Reporting Claims?
- Timely Notice
- Waiting Periods vs. Dollar-Based Retention
- Proofs of Loss
- Suit Limitation Clauses
- Careful What Gets Disclosed During Discovery:
  - E.g., Sensitive Data, Customer Information, Network Security Blueprints
- Litigation Issues
  - Not Much Precedent
  - What Exists is Not Uniform

10 TIPS FOR NAILING DOWN RESPONSIVE CYBER COVERAGE

1. Applications
2. Retro dates
3. Look for a clear policy structure: Modules and key coverage grants
4. Symmetry with other insurance (*e.g.*, CGL, Crime, D&O, All Risk)
5. Sub-limit concerns, “endorsements” and other carve outs
6. Beware contractual liability exclusions
7. Look to other policies for coverage
8. Beware conditions on "reasonable“ cyber security measures
9. Business Interruption – is it clear, including how measured
10. Give Notice!

QUESTIONS.

THANK YOU.

Rhonda D. Orin, Esq.
Partner
Anderson Kill
Washington, DC
(202) 416-6549
rorin@andersonkill.com

Daniel J. Healy, Esq.
Partner
Anderson Kill
Washington, DC
(202) 416-6547
dhealy@andersonkill.com