

Cyber Coverage: Ten Things I Wish I Knew (But Was Afraid to Ask)

Presented by

Andrew Reidy, Partner, Nossaman

Joseph Saka, Partner, Nossaman

Amy Waller Apostol, Assistant General Counsel, Leidos



Agenda

1. Decoding Your Cyber Insurance Application: Pitfalls and Best Practices
2. Essential Coverage Elements: What Your Policy Should Include
3. The Fine Print: Understanding Exclusions and Hidden Limitations
4. Retroactive Coverage: Protecting Against Unknown Past Incidents
5. Social Engineering and Funds Transfer Fraud: Are You Really Covered?
6. Ransomware Attacks: Policy Considerations and Response Strategies
7. Regulatory Compliance (GDPR and Beyond)
8. SEC Claims, Securities Claims, and D&O Liability
9. Integrating Insurance into Your Incident Response Plan
10. When Claims Get Denied: Strategies for Securing Coverage

1. Decoding Your Cyber Insurance Application: Pitfalls and Best Practices



*"You're asking for pretty detailed information.
Have your hackers gotten more demanding?"*

1. Decoding Your Cyber Insurance Application: Pitfalls and Best Practices

■ Underwriting Process

- Detailed cyber application
- Most recent financials
- Vendor contracts
- Most recent third-party security audit
- PCI Reports and Certifications – including level
- Record count
- Claims/Breach Response Costs



- Representations you make during the underwriting process can lead to coverage disputes

See, e.g., Columbia Cas. Co. v. Cottage Health System, No. 2:15-cv-03432 (C.D. Cal.); Columbia Casualty Co. v. Cottage Health System, No. 16-02310 (Cal. Super. Ct.)

2. Essential Coverage Elements: What Your Policy Should Include

What are your exposures?

- Technology Infrastructure/Equipment
- Business interruption
- Extortion/theft
- Payment card information
- Reputation
- Data manipulation or loss
- Investigation and regulatory costs
- Network security liability
- Media Liability
- Privacy liability

2. Essential Coverage Elements: What Your Policy Should Include

▪ Third Party Liability

- Lawsuits and Written Demands
 - Tip: Should apply regardless whether customer data was actually stolen
 - Tip: Consider whether policy is duty to defend v. duty to reimburse defense costs
- Regulatory Investigations and Action
 - Tip: Ideally, this should cover both costs in defending against regulatory proceedings and the cost of any fines or penalties
- Online media liability – provides defense and indemnity coverage for defamation and infringement claims for material published on company's website

2. Essential Coverage Elements: What Your Policy Should Include

▪ First Party Losses

- Breach Response Expenses
- Data Loss and Restoration Expenses
- Payment Card Industry (PCI) Fines, Assessments & Fraud Recoveries
- Lost profits, normal operating expenses/payroll costs incurred over specified period of time
- Ransomware / cyber-extortion
 - Tip: Consider exposure beyond just ransom payment
- Reputational Harm

2. Essential Coverage Elements: What Your Policy Should Include

▪ “Breach Response” Costs

- Loss containment coverage (forensic investigation and computer security expert expenses; legal services / breach coach expenses; public relations / crisis management costs)
- Notification to Customers and Call Center Costs
 - Tip: Seek highest number for any limit placed on number of persons/entity notified
- Credit / Identity Theft Monitoring
 - Tip: Insurance should provide credit monitoring from as many credit monitoring services as required by law

2. Essential Coverage Elements: What Your Policy Should Include

▪ Data Loss and Restoration Expenses

- Coverage for the cost of restoring and retrieving data that may have been lost or destroyed in a cyber attack
- Tips:
 - Avoid any limitation on type of data (e.g., electronic)
 - Avoid any limitation based on where and when data exists
 - Avoid any limitation due to the fact information is stored by third-parties, such as cloud service providers
 - If possible, obtain coverage for instances where data was inadvertently lost or destroyed

3. The Fine Print: Understanding Exclusions and Hidden Limitations

- **Tip:** Make sure you consider exclusion and definitions



3. The Fine Print: Understanding Exclusions and Hidden Limitations

- **Intentional, dishonest, or fraudulent acts exclusions** – excludes losses caused by fraudulent or illegal conduct
 - **Tip:** for the most favorable language, this should only apply after a “final, non-appealable adjudication in the underlying proceeding”
- **Other Insurance exclusions** – bars coverage if the loss is covered by another policy
 - **Tip:** try to negotiate these exclusions so they are as narrow as possible; focus on eliminating key phrases like “arising out of”
- **Civil fines and penalties**
 - **Tip:** try to limit any such limitation to “criminal” fines and penalties and confirm defense coverage for regulatory claims
- **Acts of war or terrorism exclusion**
 - **Tip:** Given nature of many attacks, insureds should seek deletion of any exclusion for terrorism or state-actors

3. The Fine Print: Understanding Exclusions and Hidden Limitations

- Tricks with Sub-limits - Although sub-limits can sometimes extend coverage that otherwise would not exist under the policy, cyber-insurers commonly use sub-limits to narrow liability for common losses
- Sub-limits may have significant impact on coverage not only under primary insurance policies, but also under excess insurance policies
- Tip: Beware of sub-limits in cyber insurance policies that look like coverage enhancements but are not

4. Retroactive Coverage: Protecting Against Unknown Past Incidents

- Some policies are limited to loss and events taking place after the inception of the policy
- Often, the nature or extent of a breach may not be understood until years later, leaving a significant uninsured loss
- Tips:
 - Where possible, pursue retroactive coverage and seek earliest retroactive date possible
 - Yahoo! Is cautionary tale. Failure to disclose seemingly minor blips can turn to disaster if there is a long delay between breach and claim

5. Social Engineering and Funds Transfer Fraud: Are You Covered?

- Consider whether spoofing/social engineering attacks are covered under any traditional insurance policies.
 - But, to avoid gaps, clients should consider stand-alone coverage for these types of losses
- Social Engineering Fraud Endorsements
 - Tips:
 - Avoid insurance language that requires verification of payee identity by telephone.
 - Beware sublimits that reduce, rather than expand, the amount of available coverage.
 - Many insurers offering \$250,000 sublimit (but may secure higher limit if “good” risk)
- Distinguishing Funds Transfer Fraud from Social Engineering Losses

6. Social Engineering and Funds Transfer Fraud: Are You Covered?

- Medidata Sols., Inc. v. Fed. Ins. Co., No. 15-CV-907 (ALC), 2017 WL 3268529, at *6 (S.D.N.Y. July 21, 2017) (finding coverage for spoofing attack under computer fraud coverage that insured loss “resulting from Computer Fraud committed by a Third Party.”)
- Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., No. 16-12108, 2017 WL 3263356, at *3 (E.D. Mich. Aug. 1, 2017) (no coverage for social engineering claim under fidelity bond covering direct loss caused by “the use of a computer to fraudulently cause a transfer . . . From inside the Premises.”)
- Aqua Star (USA) Corp. v. Travelers Cas. & Sun. Co. of Am., No. 16-35614, 719 Fed. Appx. 701, 702 (9th Cir. 2018) (computer fraud policy’s exclusion for loss resulting from the input of electronic data by a person with authority to enter the computer system barred coverage)

6. Ransomware Attacks: Policy Considerations and Response Strategies

- Current ransomware trends and tactics
- Key coverage considerations
 - Look beyond ransom payment itself - coverage should extend to business interruption; costs to restore data; breach response; bricking coverage (i.e., costs to replace hardware); and reputational harm
 - Secure your preferred vendors - If you have specific vendors or lawyers that you want to use in the event of an attack, make sure they are named at the highest possible rate
 - Consider war exclusions
- Incident response planning for ransomware events

7. Regulatory Risks: GDPR and Beyond

- Overview of global regulatory landscape
- GDPR-specific consideration
 - Confirm coverage for regulatory fines and penalties up to policy limits
 - Assure coverage for breach response costs
- Coverage for fines and penalties
 - Avoid language tying coverage to whether amounts are “insurable”
 - Add provision that coverage will exist so long as amounts are insurable under the laws of any applicable jurisdiction most favorable to the insured
- Emerging regulations – ensure coverage based on new statutes that provide for private right of action

8. SEC Claims, Securities Claims, and D&O Liability

- SEC's cybersecurity disclosure requirements
- Intersection of cyber incidents and securities / D&O claims
 - Stock drop lawsuits
 - Shareholder derivative actions
 - Allegations of misleading statements about cybersecurity
 - D&O liability in the context of cyber events
- Consider coordination between cyber and D&O policies:
 - Interplay between cyber and D&O policies – consider coverage gaps and overlaps
 - Entity coverage for securities claims
 - "Professional Services" exclusions - potential gaps for technology companies or service providers

9. Integrating Insurance into Your Incident Response Plan

- **Notice Requirements**

- Make sure systems in place to track all applicable insurance policies in the event of a claim
- Understand your Cyber policy's notice requirements
 - Some versions of AIG's CyberEdge Policy requires that notice of circumstances "be presented in chronological order"
 - Some policies may require insureds to "waive professional privilege"
 - Consider details required by "notice of circumstances" provisions

9. Integrating Insurance into Your Incident Response Plan

- **Documenting and obtaining coverage for the loss**
 - Keep thorough and detailed records of all loss and expenditures including any loss associated with business interruption
 - Comply with any requirements for tendering a loss (e.g., is sworn statement necessary)
 - Seek to have counsel present at any sworn examination
 - Obtain advanced approval for rates of counsel and consultants
 - Understand whether consent is required before incurring certain costs and, if so, seek approval
 - Cooperate with reasonable insurer requests


9. Integrating Insurance into Your Incident Response Plan

- **Consider All Sources of Coverage**
 - Commercial General Liability
 - Commercial Property Insurance
 - Errors & Omissions and Technology E&O
 - Directors & Officers
 - Crime/Fidelity
 - Kidnap & Ransom
 - Business Contracts – Indemnification and Additional Insured Coverage

10. When Claims Get Denied: Strategies for Securing Coverage

- Fully understand the strengths and weaknesses of your own claim and seek intelligence on insurers' positions in other cases
- Evaluate impact of ADR provisions
- Bring business relationships to the table
- Decide who is best to represent your company in the negotiation
- Consider other terms may help to close the deal? (agreement not to pursue similar claims, renewal, etc.)
- Assess whether initiation of coverage litigation will help resolve the dispute

Cyber Checklist

- Understand specific cyber threats relevant to your organization
 - Look for policies with a broad “computer system” definition – coverage should extend to all technology assets (e.g., hardware, software, cloud services, and mobile devices)
 - Ensure coverage for social engineering attacks and invoice manipulation losses
 - Verify if the policy covers GDPR violations and new state privacy laws
 - Seek retroactive coverage for full prior acts
 - Check availability for full dependent business interruption coverage
 - Evaluate if policy limits are adequate and pay attention to sub-limits
 - Consider any protection under “traditional” insurance policies and business agreements
 - Incident Response Planning – confirm coverage for incident response costs and access to pre-approved cybersecurity experts (and print your policy).
- 

Questions?



Andrew M. Reidy

Nossaman LLP
202-887-1412
areidy@nossaman.com



Joseph M. Saka

Nossaman LLP
202-887-1420
jsaka@nossaman.com



Amy Waller Apostol

Leidos
571-526-6703
amy.apostol@leidos.com

