

Developments in Cyber Insurance

Colin M. Proksel & Danielle D. Janitch
December 12, 2023



602-640-9000 • omlaw.com
2929 N Central Ave, Suite 2000 • Phoenix, AZ 85012

Presentation Overview

- Basics
- General Coverages – Five
- Coverage Extensions
- Costs Covered
- Possible Exclusions
- Requirements
- Notification/Reporting
- Updates

Cyber Insurance: Basics

- Varying names – Cyber liability insurance, cybersecurity insurance, etc.
- Main purpose – Cyber insurance coverage generally protects against financial (and reputational) losses resulting from events that affect an organization's IT infrastructure, such as data breaches.
- Key caveat – Ordinary business liability policies and traditional insurance products generally do not cover what cyber insurance covers.

Cyber Insurance: Basics (continued)

- There is no clear standard for what a cyber insurance policy must and must not include (yet).
- Each insurance company has its own policy standards, exceptions, and costs, etc.
- Be sure to carefully review policy terms.

Cyber Insurance: Five General Coverages

- Privacy Liability Coverage – goes to private personal information
- Network Security – goes to network security failures, such as data breaches, email-compromise events, extortion, malware, ransomware, etc.
- Network Business Interruption – goes to operational risk, including system failures, such as human error or a failed software patch, and security failures, like a third-party hack

Cyber Insurance: Five General Coverages (continued)

- Errors and Omissions Coverage – goes to errors in the performance of or failure to perform one's services
- Media Liability Coverage – goes to intellectual property infringement, other than patent infringement, resulting from the advertising of one's services

Cyber Insurance: Coverage Extensions

- Extensions or additional coverage varying by insurer
- Examples:
 - ACH Fraud under “social engineering” extension
 - “Invoice Manipulation”
 - “Criminal Reward Costs”

Cyber Insurance: Costs Covered

- First-party costs (faced by organization buying the insurance):
 - Investigations
 - Recovery/repairing of damaged/compromised data or systems
 - Lost income
 - Business interruption
 - Notification costs
 - Extortion
 - Crisis management
 - Credit monitoring
 - Identity restoration
 - Betterment/Improvements

Cyber Insurance: Costs Covered (continued)

- Third-party costs (faced by other organizations or individuals):
 - Litigation expenses/damages
 - Regulatory expenses/fines
 - Crisis management

Cyber Insurance: Possible Exclusions

- Prior breaches
- Pre-existing Vulnerabilities
- Poor security
- Human error
- Insider attacks
- Improvements/Betterment

Cyber Insurance: Key Basic Requirements

- First step is to audit infrastructure, systems, policies:
 - the who,
 - what,
 - where,
 - when,
 - why, and
 - how re risks.
- Second step is to double check the first step

Cyber Insurance: Key Basic Requirements (continued)

- Implementing EDR across endpoints
 - Endpoint – Any virtual environments, devices, and servers connected to a network
 - EDR – Endpoint detection and response software; like anti-virus
- Using multi-factor authentication
- Establishing a backup plan
- Setting up identity

Cyber Insurance: Notification/Reporting

- As of Sept. 2023, new SEC regulations require registered public companies to report material cybersecurity incidents within four business days of determining the incident to be material
 - Discovery?
 - Materiality?
- Historical/traditional standard - “as soon as practicable”

Biometric Information Privacy Act Coverage

- *Citizens Ins. Co. of Am. v. Wynndalco Enterprises, LLC*, 70 F. 4th 987 (7th Cir. 2023)
- Insurer must defend insured in two putative class actions alleging violations of Illinois' Biometric Information Privacy Act
- Business liability insurance policy at issue

Negligence Claims in Employer Data Breach Cases

- *Ramirez v. Paradies Shops, LLC*, 69 F. 4th 1213 (11th Cir. 2023)
- Reversed dismissal of negligence claims in a data breach case
- Explained there may be a duty to protect employees' PII when it is foreseeable, given the size and sophistication of a company and how it could be the target of a cyberattack
- Effectively reduces burden on plaintiffs to provide specific facts about foreseeability in the pleading stage in federal court

Foreign Hackers and War

- *Merck & Co., Inc. v. Ace Am. Ins. Co.*, 475 N.J. Super. 420, 293 A.3d 535 (App. Div.), *leave to appeal granted*, 254 N.J. 506, 298 A.3d 353 (2023), *and leave to appeal granted*, 254 N.J. 522, 298 A.3d 364 (2023)
- Insured pharmaceutical company brought action against insurers, alleging it was entitled to coverage under “all risks” property policies after cyberattack allegedly orchestrated by actors working for or on behalf of Russian government infected and damaged thousands of insured's computers in its global network
- Exclusion for “loss or damage caused by hostile or warlike action” by “any government or sovereign power” did not bar coverage
- Insurers will likely revise language in policies to include non-traditional forms of warfare

Policy Rescission Based on Application

- *Travelers Property Casualty Company of America v. International Control Services, Inc.*, 2:22-cv-02145-CSB-EIL (C.D. Ill. Aug. 30, 2022)
- Ransomware attack
- Insurer denied coverage and sought a declaration that the cyber policy was null and void based on allegedly false information the insured provided in its policy application
- After complaint filed, insured agreed to rescission
- But note at least one EU (Germany) decision to contrary

Pixel-Tracking Privacy Claims

- Cookies v. Tracking Pixels
 - Cookies – User experience and marketing purposes (activity and behavior); Generally cannot follow users across devices; Information is placed on users' browser; Can be blocked or cleared by users from the browser settings
 - Tracking Pixels – Marketing purposes (tracking user activity and behavior); Can follow users across devices; Information is sent directly to web servers by pixels; Not easily disabled by end-user
- May implicate cyber insurance
- Still early – No major state supreme court or federal court of appeals decisions

California Consumer Privacy Act

- *Durgan v. U-Haul Int'l Inc.*, CV-22-01565-PHX-MTL, 2023 WL 7114622 (D. Ariz. Oct. 27, 2023)
- Connection between company's purported failure to implement reasonable security procedures and unknown hackers' ability to exfiltrate PPI via phishing
- "[I]f Defendant had utilized adequate filtering software, the phishing emails would never have reached the employees' inboxes."
- "If Defendant's employees had been adequately trained, the phishing emails, even if they reached the employees' inboxes, would not have been successful."
- "If Defendant had implemented multi-factor authentication, the hackers would not have been able to access Defendant's systems even if the phishing emails had been successful."
- If Defendant had not stored the PII in an unencrypted form in an internet-accessible system, the hackers would not have been able to access or read it even if they had gained access to Defendant's systems."
- "Finally, if Defendant had destroyed the PII when it was no longer in use, much of the PII would not have been stolen regardless of how successful the hackers' scheme was."

“Deep Fakes”

- Use of deep fake technology techniques to attempt to clone and/or spoof voice, image and fingerprint authentications or the like
- May implicate cyber insurance
- Still early – No major state supreme court or federal court of appeals decisions

Artificial Intelligence

- Will likely implicate cyber insurance
- Full of “unknown unknowns”

2024 Market for Cyber Coverage

- Possible price stability
- Likely increase in terms, conditions, and exclusions limiting coverage
- Watch for issues concerning:
 - Cloud outages,
 - Software vulnerabilities, and
 - Nation-state-based bad actors and cyber events – China, Russia, etc.

Cyber Coverage Events

- If you think you have experienced a cyber security event, you may need to contact counsel first...
 - What do you do next internally?
 - What are your coverages?
 - You may have more than cyber.
 - What does your coverage(s) require?
 - To whom do you report? Insurer only? Authorities? Regulators?
 - How do you report?
 - What do you report?

Colin M. Proksel

**[https://www.omlaw.com/
cproksel/](https://www.omlaw.com/cproksel/)**

602-640-9393

cproksel@omlaw.com

Danielle D. Janitch

**[https://www.omlaw.com/
djanitch/](https://www.omlaw.com/djanitch/)**

602-640-9381

djanitch@omlaw.com



Thank you!

Developments in Cyber Insurance
Colin M. Proksel & Danielle D. Janitch
December 12, 2023



602-640-9000 • omlaw.com
2929 N Central Ave, Suite 2000 • Phoenix, AZ 85012