Privacy & Security Forum
Fall Academy

The Transformation of Cyber Insurance and Reinsurance Law

Bridget Quinn Choi, Booz Allen Hamilton
Michael Phillips, Resilience Cyber Insurance Solutions
Edward Brown, Wiley Rein LLP

Agenda

Ransomware and Cyber Threats Driving Change
- Ransomware is a National Security Threat
- The Continued Challenge of Attribution
- Spectrum of State Responsibility

The "Silent Cyber" Issue
- Affirmative Cyber Cover
- Silent Cyber as Reaction to Ransomware
- A New Arena for Litigation?

How Cyber Reinsurance Contracts May Shift
- Shifts in Terms, Shifts in Law?

Discussion

Privacy+ Security Forum

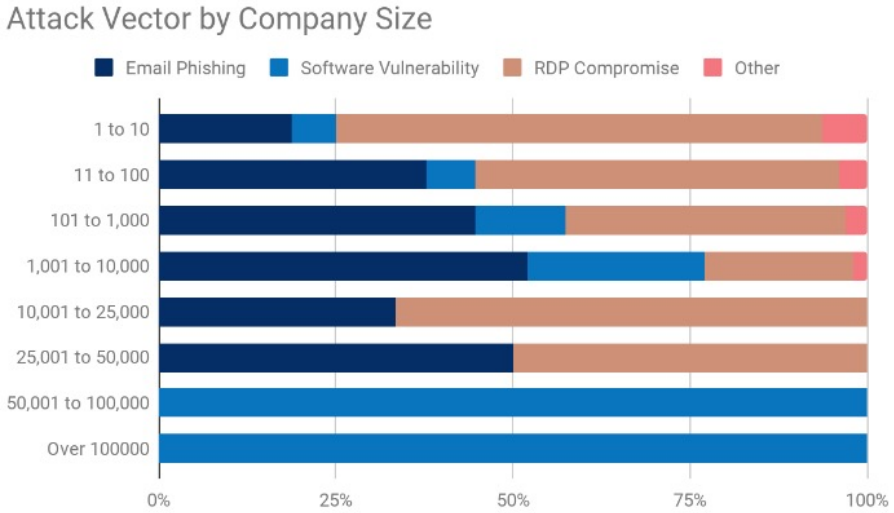
Ransomware Becomes a National Security Threat

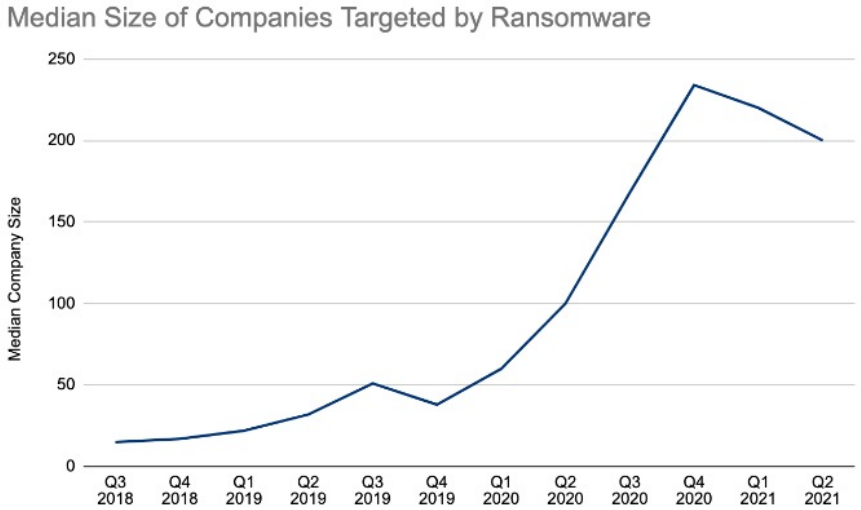
- **Ransomware** attacks are on the rise, with malicious actors becoming bolder and increasingly targeting larger organizations with **higher ransom demands**.
- The issue has become **a national security and public health and safety threat**, affecting a broad array of public and private systems, ranging from companies to schools, hospitals, police stations, city government, military facilities and critical infrastructure.
- **Foreign nation-state adversaries** either directly support and cultivate ransomware actors **or** permit ransomware activities to operate from within their borders with impunity.

Colonial Pipeline

Ransomware Becomes a National Security Threat

- **Ransomware Impacts Companies of All Sizes.**
  - SME focus, though companies of all sizes are targeted.
  - Average Downtime -- 23 days, highlighting operational interruptions





COVEWARE

Ransomware Becomes a National Security Threat

The September 21, 2021 Updated OFAC Advisory on Potential Sanctions Risks for Facilitating Ransomware Payment

- Discourages paying of ransoms.
- Lays out expanded “significant mitigating factors” in the face of potential sanctions risks, including:
  - Demonstrating proactive cyber resilience (offline backups, incident response planning, employee training, endpoint protection)
  - “full and ongoing” cooperation with law enforcement
- For victims and IR firms, outstanding questions about attribution, due diligence obligations, and definition of “facilitation”
- For insurers, new complexity

The Continued Challenge of Attribution

- **Victim organizations struggle with attribution during their incident response.**
- **Ransomware syndicates operating in adversarial safe havens.**
- **Major cybersecurity events may have a foreign intelligence angle.**
  - SolarWinds Supply Chain Attack
  - The Microsoft Exchange “HAFNIUM” Attack
- **How do policyholders and insurers respond?**

JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), AND THE NATIONAL SECURITY AGENCY (NSA)

Original release date: January 05, 2021

The Spectrum of State Responsibility

Passive	Ignoring or Abetting		Ordering or Conducting	
State-prohibited: The national government will help stop the third-party attack.	State-ignored: The national government knows about the third-party attacks but is unwilling to take any official action.	State-shaped: Third parties control and conduct the attack, but the state provides some support.	State-ordered: The national government directs third-party proxies to conduct the attack on its behalf.	State-executed: The national government conducts the attack using cyber forces under their direct control.
State-prohibited-but-inadequate: The national government is cooperative but unable to stop the third-party attack.	State-encouraged: Third parties control and conduct the attack, but the national government encourages them as a matter of policy.	State-coordinated: The national government coordinates third-party attackers such as by "suggesting" operational details.	State-rogue-conducted: Out-of-control elements of the national government's cyber forces conduct the attack.	State-integrated: The government is in control of the targets, timing and tempo of the intrusion.

ATLANTIC COUNCIL

What does cyber traditionally cover?

The Market's Historical Development

- Rapid, competitive product evolution

Typical Coverages of a Cyber Policy

- Suite of coverage grants across crisis, first-party, and third-party
- Incident Response, Extortion, Business Interruption
- Privacy Liability, Regulatory
- Typically triggered by a defined set of cybersecurity or privacy-related events

How is the cyber market evolving?

In response to the rise in destructive cyber attacks:

- Potential barriers to entry and higher UW standards
- Co-insurance, lower limits
- Changes to business interruption and dependent
- Attention to extortion coverage terms and conditions
- Approaches to breachless claims

The Silent Cyber Issue

Silent cyber refers to the absence of explicit inclusion or exclusion of cyber events as a trigger to insurance coverage.

As cyber attacks cause more (and more varied) harms:

- Policyholders seek coverage for cyber losses from non-cyber policies
- Cyber exclusionary language within non-cyber policies are tested
- “Silent cyber” insurance coverage disputes arise.

The Silent Cyber Issue as Ransomware Reaction

As ransomware attacks become increasingly destructive and harm victims without cyber insurance:

- Policyholders will seek coverage for cyber losses from non-cyber policies
- Cyber exclusionary language within non-cyber policies are tested

Coverage Litigation Spotlight

- **Crime Policy -** *G&G Oil Co. of Indiana, Inc. v. Contl. W. Ins. Co.,* 20S-PL-617, 2021 WL 1034982 (Ind. Mar. 18, 2021)
- **Business Owner's Policy -** *National Ink & Stitch, LLC v. State Auto Property and Casualty Insurance Company,* Civil Case No. SAG-18-2138 (District of Maryland)

A New Arena for Litigation?

- How do the newly-drafted insurance policy terms and conditions work?
- How does cyber coverage interact with other first-party and third-party lines of insurance with respect to the damages caused by sophisticated cyber attacks and liabilities flowing from emerging data protection statutes like BIPA, CCPA, and the CPRA?
- Where do losses involving a cybersecurity event but manifesting in physical damage, bodily harm, or other consequential harm sit?
- Do “silent cyber” restrictions encourage more organizations to pursue litigation (say, against their vendors) who may be liable for a ransomware loss?

Cyber Reinsurance Contracts: Shifts in Terms, Shifts in Law?

- **Regulatory and Jurisdictional (The challenges of private sector attribution / spectrum of state responsibility).**

- **Attention to Clash Reinsurance (The age of supply chain attacks, ransomware syndicates, variants, and attack campaigns).**

- **Follow the Fortunes/Settlements and Allocation.**

- **Access to Records/Privilege.**

Discussion & Thanks

Q&A