Insurance Coverage for Cyber Risks

September 29,2021

John F. Banghart
Senior Director for Cybersecurity Services | 202.344.4803 | JFBanghart@Venable.com

Ken D. Kronstadt
Counsel | 310.229.0438 | KDKronstadt@Venable.com

John B. Mavretich
Associate | 202.344.4119 | JBMavretich@Venable.com

VENABLE LLP

What Is the Risk?

◆ WSJ NEWS EXCLUSIVE | BUSINESS

Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom

Joseph Blount says he needs to quickly restore service after cyberattack threatened East Coast supply

T-Mobile Says Hack Exposed Personal Data of 40 Million People

The company said that stolen files included the personal information of 7.8 million current customers and 40 million people who had applied for credit.

Cybersecurity

CNA Financial Paid $40 Million in Ransom After March Cyberattack

By Kartikay Mehrotra and William Turton
May 20, 2021, 3:57 PM EDT

VENABLE LLP

What Are the Most Common Types of Malicious Attacks?

- **Malware/ cyberextortion / ransomware**

- **Advanced persistent threats**: network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time.

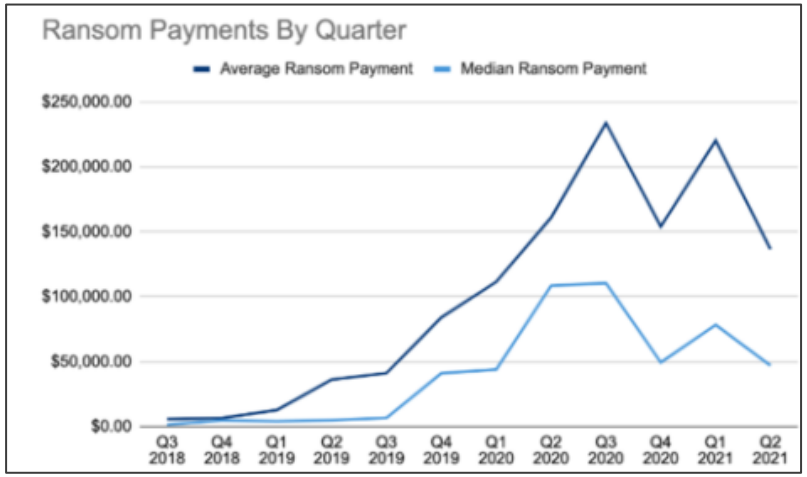
- **Social engineering**: utilizing human behavior to breach security without the participant/victim realizing they have been manipulated (e.g., posing as company executive and tricking an employee into sending confidential information).
  - **Phishing**: attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in electronic communication.
  - **Spear phishing**: personalized email to a select email (e.g., a fake but recognizable email address is created to impersonate a colleague or boss).

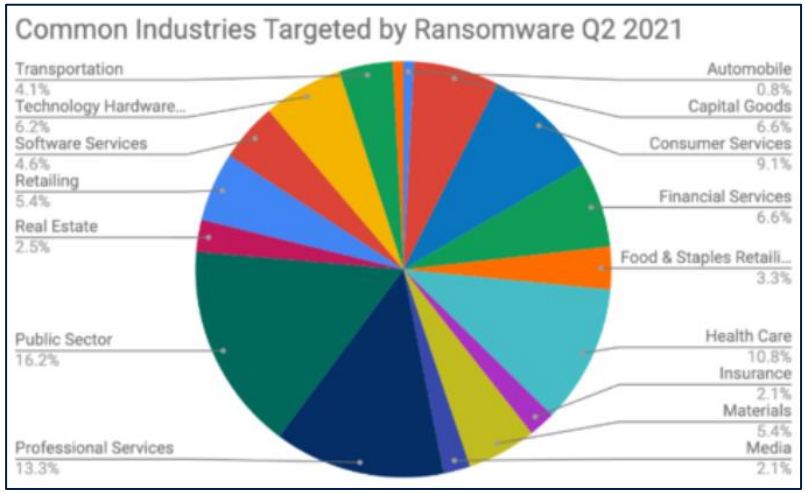
- **Viruses, distributed denial-of-service (DDoS) attacks**: (e.g., making a machine or network unavailable to intended users.)

VENABLE LLP

Ransomware by the Numbers

- **Targets:** All Industry Sectors Globally
- **Average Ransom Payment Q2 2021:** $136,576
  - Payouts in the millions happen frequently.
- **Median Ransom Payment Q2 2021:** $47,008
- **Average Downtime in Days:** 23
- **Average Ransomware Remediation Cost within the United States**: $2.09M
- **Percentage of Organizations Hit by Ransomware in the Past 12 Months by Sector:** Distribution and Transport (25%), Energy (36%), Manufacturing & Production (36%)





VENABLE LLP

Sources: Sophos *The State of Ransomware 2021*, Coveware *Ransomware Marketplace Report Q2 2021*

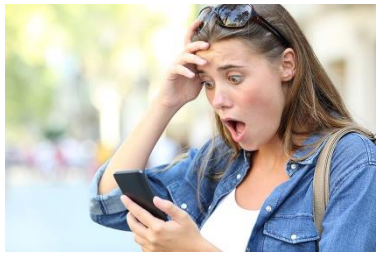
Cyber Threats Represent Huge Potential Liability for Companies

- Payment of ransom to hackers
- Government fines
- Class action lawsuits
- Government investigations

VENABLE LLP

Is This Covered by Traditional Insurance Policies?

- **Commercial General Liability Insurance**
  - Typically covers three things:
    - (1) bodily injury
    - (2) (third-party) property damage
    - (3) personal and advertising injury



  - Cyber risks generally do not fall within any of these three categories

  - Recent exception (data breach as "publication"): *Landry's, Inc. v. Ins. Co. of the State of Pa.*, No. 19-20430, 2021 WL 3075937 (5th Cir. July 21, 2021)

VENABLE LLP

Is This Covered by Traditional Insurance Policies? (cont'd.)

- **First-Party Property Insurance**
  - Generally covers "direct physical loss of or damage to" covered property
  - …but what is "covered property?"

  - ***Nat'l. Ink & Stitch, LLC v. State Auto Prop. & Cas. Ins. Co.*, 435 F. Supp. 3d 679 (D. Md. 2020)**
    - Ransomware attack resulted in loss of data and less efficient software operation
    - "Covered Property" defined to include data on various storage media
    - Court found attack caused "direct physical loss of or damage to Covered Property," regardless of whether storage media also incurred damage

  - ***State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More*, 147 F. Supp. 2d 1113 (W.D. Ok. 2001)**
    - Policy covered physical injury or loss of use of "tangible property"
    - "…computer data cannot be touched, held, or sensed by the human mind; it has no physical substance. It is not tangible property."

VENABLE LLP

Is This Covered by Traditional Insurance Policies? (cont'd.)

Directors & Officers Liability Policy

- Generally covers liability to directors & officers (and, depending on the policy, the company) for claims based on mismanagement, breach of duty, etc.

- Examples of potentially covered cyber claims:
  - Shareholder derivative suit against managers related to cyber breach
  - Government investigation related to failure to secure data

- **BEWARE** explicit cyber exclusions and/or hidden cyber exclusions (such as exclusions related to invasion of privacy, contract, IP).

VENABLE LLP

Is This Covered by Traditional Insurance Policies? (cont'd.)

- **Crime Insurance**
  - Generally covers first-party losses due to theft or other dishonesty
  - Various coverage grants, such as:
    - Employee dishonesty
    - Forgery or alteration coverage
    - Computer fraud coverage
    - Funds transfer fraud coverage
    - Kidnap, ransom, or extortion coverage
    - Money and securities coverage
  - Slight variance in policy language can drastically affect coverage…

VENABLE LLP

Crime Policies: Pay Close Attention to the Words

***Apache Corp. v. Great Am. Ins. Co.*, 662 F. App'x 252, (5th Cir. 2016) (applying Tex. law)**

Coverage grant: We will pay for loss of, and loss from damage to, money, securities, and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises:

a. to a person (other than a messenger) outside those premises; or

b. to a place outside those premises.

- Scheme started with a phone call from purported vendor. Impostor then created a fake email address and sent a follow up email (with attachment on fake letterhead) requesting payments be made to new account.
- Court: "The email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money. To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would…convert the computer-fraud provision to one for general fraud."
- Court determined **no coverage** because loss did not "result directly from the use of any computer."

VENABLE LLP

Crime Policies: Pay Close Attention to the Words

***Medidata Solutions, Inc. v. Fed. Ins. Co.*, 729 Fed. App'x 117 (2d Cir. 2018)**

Computer Fraud Coverage protected against "direct loss of Money, Securities or Property sustained by an Organization resulting from Computer Fraud committed by a Third Party."

Funds Transfer Fraud protected against "direct loss of Money or Securities sustained by an Organization resulting from Funds Transfer Fraud committed by a Third Party.

- Fraudsters sent email (posing as company president) to Medidata employees requesting payment to contractual counterparty. Fraudsters also called employee impersonating counterparty. Employee made two wires to fraudsters as a result.
- Insurer argued that there was no "direct loss" as a result of the spoofing attack.
- Court found direct loss = proximate cause and that the spoofed emails were the proximate cause of loss: "While it is true that the Medidata employees themselves had to take action to effectuate the transfer, we do not see their actions as sufficient to sever the causal relationship between the spoofing attack and the losses incurred."
- Summary judgment AFFIRMED in favor of policyholder.

VENABLE LLP

What Does a Cyber Policy Cover?

- Cyber coverage is relatively new and there are **no form policies**
- Typically **named-peril** policies
- Typically **claims-made** policies
- Covers both first- and third-party liability
- Carriers often provide multiple coverages that may be purchased buffet style

VENABLE LLP

What Does a Cyber Policy Cover? (cont'd.)

Common first-party coverage:

- **Network/business interruption**
- **Data/digital asset loss and restoration**
- **Cyberextortion/Ransomware**
- **Reputational Damage**
- **Civil fines/penalties**
- **Losses due to theft of trade secrets, intellectual property, or funds**
- **Event breach costs [*Hybrid first- & third-party coverage*]:** Costs incurred by an organization arising out of:
  - Forensic investigation of breach
  - Public relations/crisis management firms and associated costs
  - Notification costs
  - Call centers, consumer notification, credit/identity monitoring, etc.

VENABLE LLP

What Does a Cyber Policy Cover? (cont'd.)

Common third-party coverage:

- **Security and privacy breaches**
- **Internet Media Liability**
- **Liability associated with defamation, copyright infringement, product disparagement or reputational damage**
- **Vendor loss of third-party data or information**

VENABLE LLP

Cyber Policies: Exclusions

Common exclusions:

- **Representations and warranties about data security**
- **Failure to follow stated security practices**
- Exposures insured elsewhere: no coverage for loss insured in whole or in part by another valid policy
- Bodily injury and property damage: no coverage for loss arising out of, or attributable to bodily injury or property damage/damage to infrastructure
- Lost business or profits stemming from harm to reputation

Less common:

- Acts of war/terrorism
- Copyright, trademark, and patent infringement
- Breach of contract or warranty

VENABLE LLP

Ransomware Coverage on the Chopping Block?

FINANCIAL

Cyber insurance market encounters 'crisis moment' as ransomware costs pile up

Written by Tim Starks

AUG 23, 2021 | CYBERSCOOP

Ransomware now accounts for 75% of all cyber insurance claims, up from 55% in 2016, according to the credit ratings agency AM Best. The percentage increase in claims is outpacing that of premiums, said a June report which concluded that "the prospects for the cyber insurance market are grim." Fitch Ratings in April found that the ratio of losses to premiums earned was at 73% last year, jeopardizing the profitability of the industry.

"What is more common than very public exits, are strategy changes that might signal an exit," said Phillips. That could mean covering fewer and fewer aspects of ransomware costs, he said. AXA, for instance, has said it will stop paying ransom demands for future policyholders, partly in response to French government pressure to halt the practice.

"They're going to say, 'You want to buy it from us, fine, but you're only going to get a tenth of what you got last year,'" Phillips said.

Others might limit coverage in other ways. "As companies are deemed risky then maybe there's a higher deductible, or the insurance company might say, 'I'm not going to write a $5 million limit on your cyber, I'm just going to limit my exposure to you to $500,000,'" said Sridhar Manyem, director of industry research at AM Best.

VENABLE LLP

Cyber Policies: Pitfalls and Practical Tips

Before obtaining/renewing a policy,

- **Ensure your company has cybersecurity policies and practices in place.** With relatively unstable underwriting data and constantly changing security threats, one of the only things insurers can do to control risk is to make sure the prospective policyholder has robust security measures in place.
  - Policies often have a "failure to maintain" exclusion which may apply if the policyholder does not keep these cybersecurity protections in place and in proper working order

Insurers Push For Security Standards Amid Cybercrime Crush

By **Ben Kochman**

Law360 (September 2, 2021, 4:08 PM EDT) -- As Congress continues to drag its feet on enacting federal cybersecurity rules, the insurance industry has stepped in to fill the void behind the scenes, pushing policyholders to adopt strict security practices as a condition of receiving coverage for cyberattacks.

  - **Know your organization's risk profile and take steps to mitigate risks**

VENABLE LLP

Cyber Policies: Pitfalls and Practical Tips

When obtaining/renewing a policy,

- **Holistic approach to insurance**

- **Seller's market**
  - **Premiums rising**
  - **Limits falling**

- **Language matters**

VENABLE LLP

Cyber Policies: Pitfalls and Practical Tips (cont'd.)

SOCIAL ENGINEERING FRAUD INSURING AGREEMENT ENDORSEMENT

2. The following **INSURING AGREEMENT** is added to section ***I. INSURING AGREEMENTS***:

SOCIAL ENGINEERING FRAUD

The Company will pay the **Insured** for the **Insured's** direct loss from the transferring, paying or delivering **Money** or **Securities**, directly caused by **Social Engineering Fraud** committed by a person purporting to be:

a. a **Vendor**; or

b. a **Client**,

provided that, prior to transferring, paying or delivering **Money** or **Securities,** the **Insured** performed a **Callback Verification** with respect to each **Communication**. Such **Callback Verification** must be recorded, logged, or otherwise documented by the **Insured**.

3. The following are added to section ***III. DEFINITIONS***:

Callback Verification means a verbal conversation with a purported **Vendor** or **Client**, using a **Pre-Determined Telephone Number**, to verify the identity of the **Vendor** or **Client** and the authenticity of a **Communication**.

Communication means an electronic, telegraphic, cable, teletype, telephone, or written instruction received by an **Employee** that:

1. directs the **Employee** to transfer, pay, or deliver **Money** or **Securities**;

2. contains a misrepresentation of a material fact; and

3. is relied upon by the **Employee**, believing the material fact to be true.

VENABLE LLP

Cyber Policies: Pitfalls and Practical Tips (cont'd.)

SECURITY AND PRIVACY INSURING AGREEMENT

The **Insurer** shall pay on an **Insured's** behalf all **Loss** in excess of the applicable Retention that such **Insured** is legally obligated to pay resulting from a **Claim** alleging a **Security Failure** or a **Privacy Event.**

(l) **"Privacy Event"** means the following occurring on or after the **Retroactive Date** and prior to the end of the **Policy Period:**

(1) any failure to protect **Confidential Information** (whether by "phishing," other social engineering technique or otherwise) including, without limitation, that which could result in an identity theft or other wrongful emulation of the identity of an individual or corporation;

(p) **"Security Failure"** means the following occurring on or after the **Retroactive Date** and prior to the end of the **Policy Period:**

(1) a failure or violation of the security of a **Computer System** including, without limitation, that which results in or fails to mitigate any unauthorized access, unauthorized use, denial of service attack or receipt or transmission of a malicious code;

VENABLE LLP

Cyber Policies: Pitfalls and Practical Tips (cont'd.)

- **BEWARE**: Cyber criminals have even targeted insurance carriers to gain access to application and underwriting data related to insureds

LAW360 Insurance Authority

PROPERTY --- GENERAL LIABILITY --- SPECIALTY LINES

Analysis

Cyberinsurance Carriers Top Hackers' Hit List

By Daphne Zhang and Ben Kochman · September 7, 2021, 5:19 PM EDT

Cybersecurity

CNA Financial Paid $40 Million in Ransom After March Cyberattack

By Kartikay Mehrotra and William Turton
May 20, 2021, 12:57 PM PDT

VENABLE LLP

Cyber Insurance: Summary

- Cyber risks are a relatively new and developing area of potential liability for companies. The risk, especially for companies that have complex operations or possess large amounts of protected data, can be enormous.

- Cyber insurance is a relatively new form of coverage that is still developing. Unlike traditional forms of insurance (like CGL or Property policies), there is no "standard" cyber form. Thus, it is critical that insureds fully understand what is (and isn't) covered under their cyber policy. An experienced professional can assist insureds with this important task.

- Similarly, case law in relation to insurance coverage for these risks continues to evolve and can result in unexpected results (both positive and negative for policyholders).

- While cyber insurance can provide an important "backstop" if things go wrong, it is not a substitute for diligent cybersecurity efforts. In fact, insurers now require proof that an insured is taking such diligent efforts to protect itself from attack before issuing a cyber policy.

VENABLE LLP

John F. Banghart
Senior Director of Cybersecurity Services
202.344.4803
JFBanghart@Venable.com

Ken D. Kronstadt
Counsel
310.229.0438
KDKronstadt@Venable.com

John B. Mavretich
Associate
202.344.4119
JBMavretich@Venable.com

VENABLE LLP

VENABLE LLP