GT GreenbergTraurig

What is Cybersecurity Insurance and Why is it Important?

Louisiana Department of Insurance Conference

March 7, 2022

9:00 AM – 9:50 AM CT

Fred E. Karlinsky

Greenberg Traurig, P.A.

LDI CONFERENCE 2022

Fred E. Karlinsky

Shareholder & Global Chair,
Insurance Regulatory &
Transactions Practice

Greenberg Traurig, P.A.

(954) 768-8278

Karlinskyf@GTLaw.com

Biography

Fred E. Karlinsky is the Global Chair of Greenberg Traurig's Insurance Regulatory and Transactions Practice Group. Fred has nearly thirty years of experience representing the interests of insurers, reinsurers and a wide variety of other insurance-related entities on their regulatory, transactional, corporate and governmental affairs matters.

Fred has been recognized for his work in insurance law by *The Best Lawyers* and *Chambers and Partners.* In addition to his role with Greenberg Traurig, Fred has been an Adjunct Professor of Law at Florida State University College of Law since 2008, where he teaches a course on Insurance Law and Risk Management. Fred currently chairs the Florida Supreme Court Judicial Nominating Commission, which he has served on since 2014.

Agenda

- The Threat Environment
- 2021 Cyber Attacks
- The Importance of Cyber Insurance
- Cyber Insurance Basics
- Cyber Insurance Coverages
- Other Cyber Considerations


The Threat Environment

Cyber Risks

- Loss of information
- Cyber-extortion
- Legal liability for security breaches
- Expenses to respond to a cyber attack

Threat Analysis

- Cyber attacks are increasing
- Attacks cost the U.S. economy anywhere from $57 billion to $109 billion annually and these costs are increasing.
- Insurance experts now consider the risk of cyber liability losses to exceed the risk of fraud or theft.

Cyber Attacks in the U.S.

- $590 million in suspicious activity related to ransomware in the first six months of 2021.
  - Surpassed the 2020 full year total of $416 million.
- The value of Suspicious Activity Reports (SAR) filed in 2021 surpassed the value of the last 10 years of SARs combined.
- Most SARs are filed by U.S. cybersecurity companies, banks, and cryptocurrency exchanges.

Cyber Attacks in the U.S.

- FinCen Identified 68 ransomware variants in Suspicious Activity Report data.
  - Variant analysis helps identify attackers.
- Top 10 Variants accounted for $217.56 million in suspicious Activity.
- 242 Suspicious Activity Reports on 10 most Frequent variants.

COVID-19

- Uncontrolled cyber security environment
  - Unsecure connectivity
  - Employee access issues
  - Human cyber risks
- Cyber criminals took advantage of human and company vulnerabilities


Recent Cyber Attacks

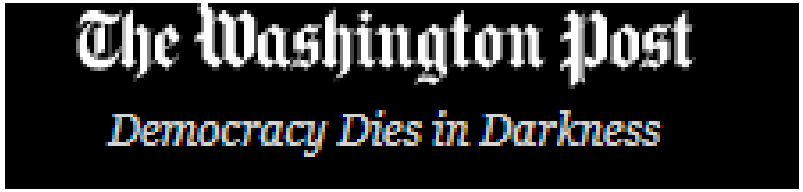
CNA Financial: March 2021

CNA cyberattack in March exposed personal information of more than 75,000 people, filings reveal.

Colonial Pipeline: April 2021

Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate

Kaseya: July 2021



Ransomware attack struck between 800 and 1,500 businesses, says company at center of hack

Robinhood: November 2021

Robinhood: Security breach exposed data of 7 million users

Aon: February 2022

Aon reports cyberattack

Russia

Forbes

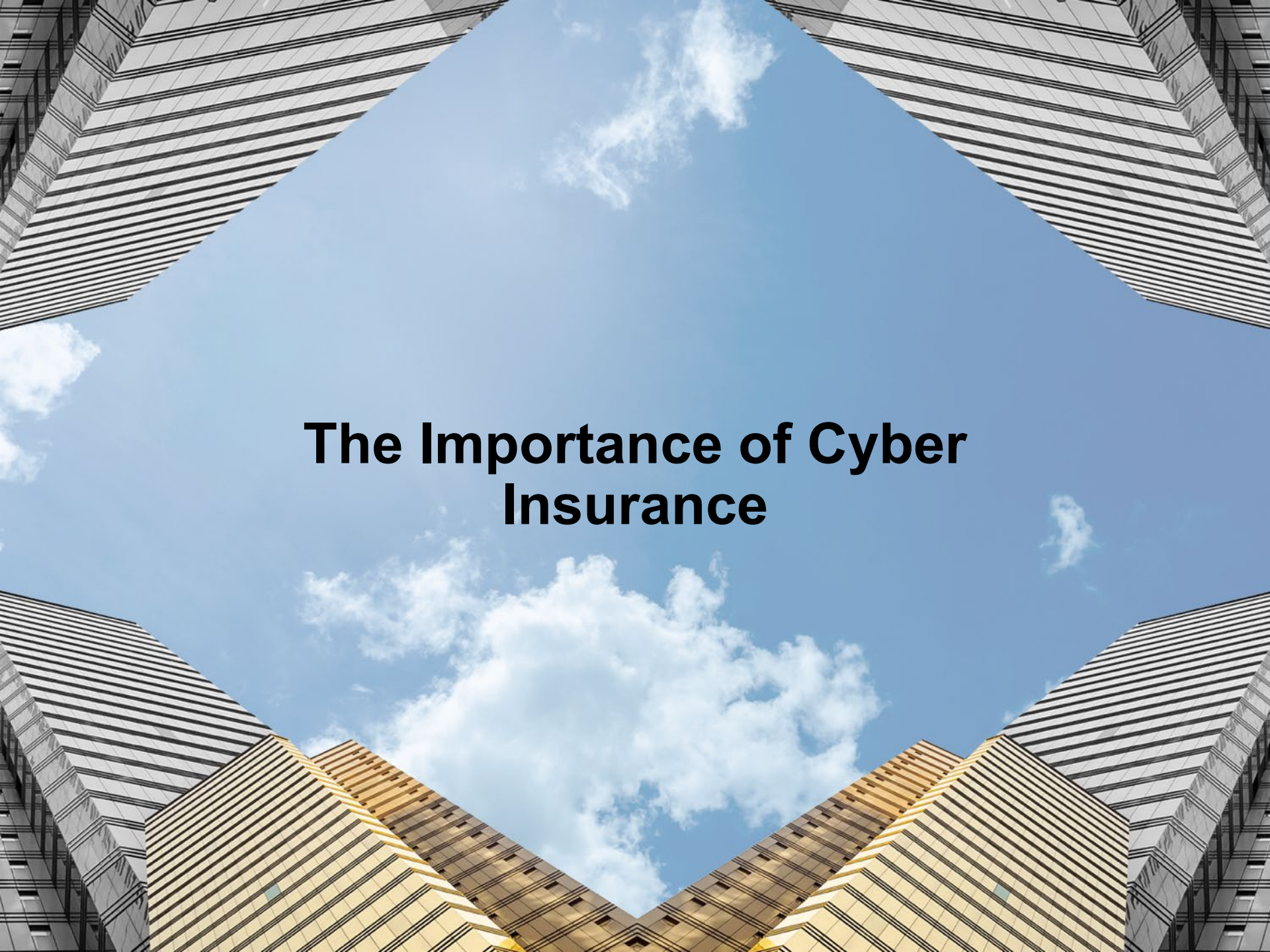
CISA Issues "Shields Up" Warning About Russian Cyber Attacks

FOX NEWS channel

Ukraine stands up to Russian cyberattacks; Putin could launch revenge attacks against US, expert warns

CNN BUSINESS

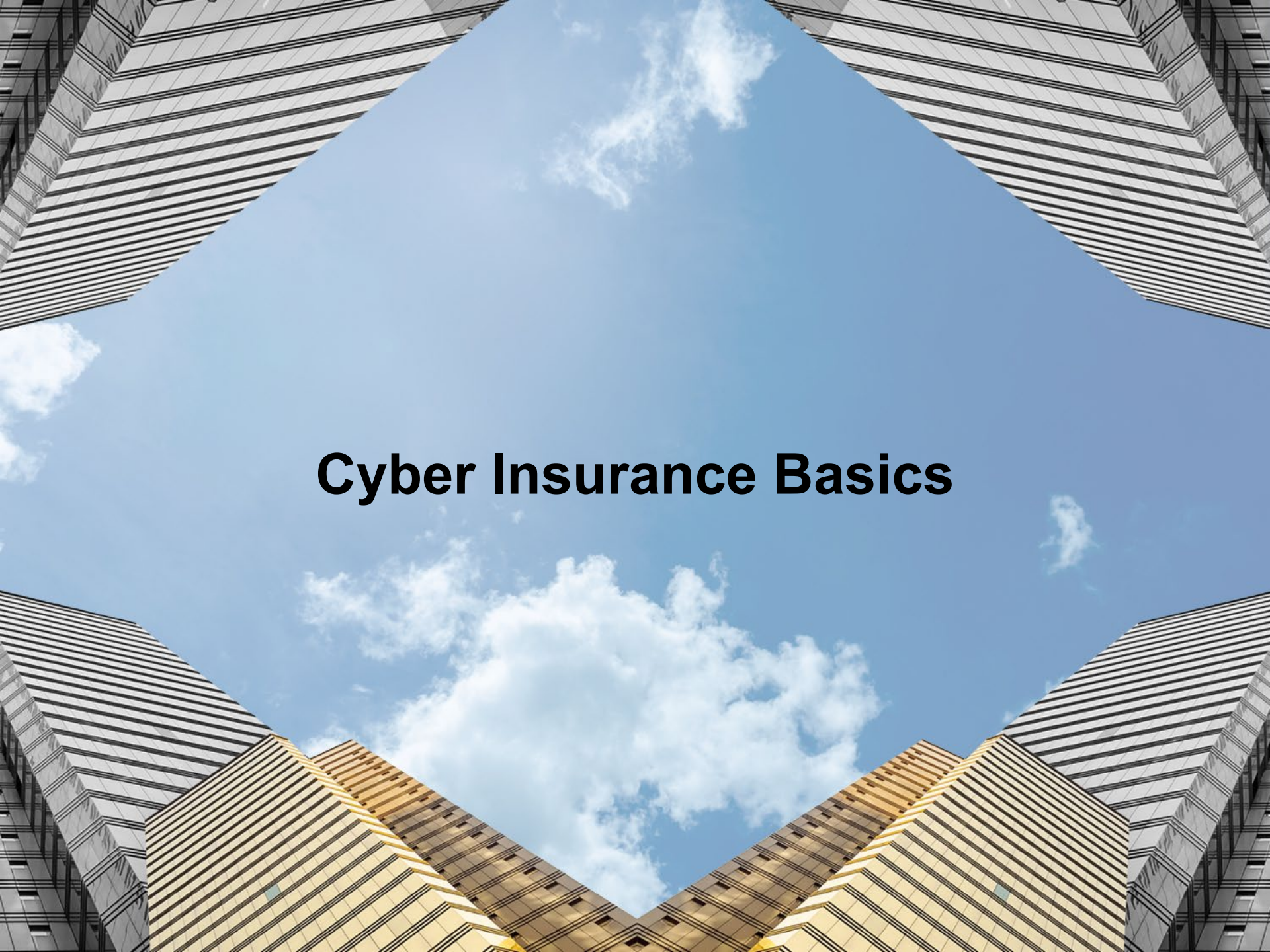
US braces for Russian cyberattacks as Ukraine conflict escalates. Here's how that might play out


The Importance of Cyber Insurance

The Importance of Cyber Insurance

The Importance of Cyber Insurance

- Mitigate Potential Loss
- Threat Protection
- Financial Costs Coverage


Cyber Insurance Basics

How Cyber Insurance Can Help

Cyber Insurance Trends

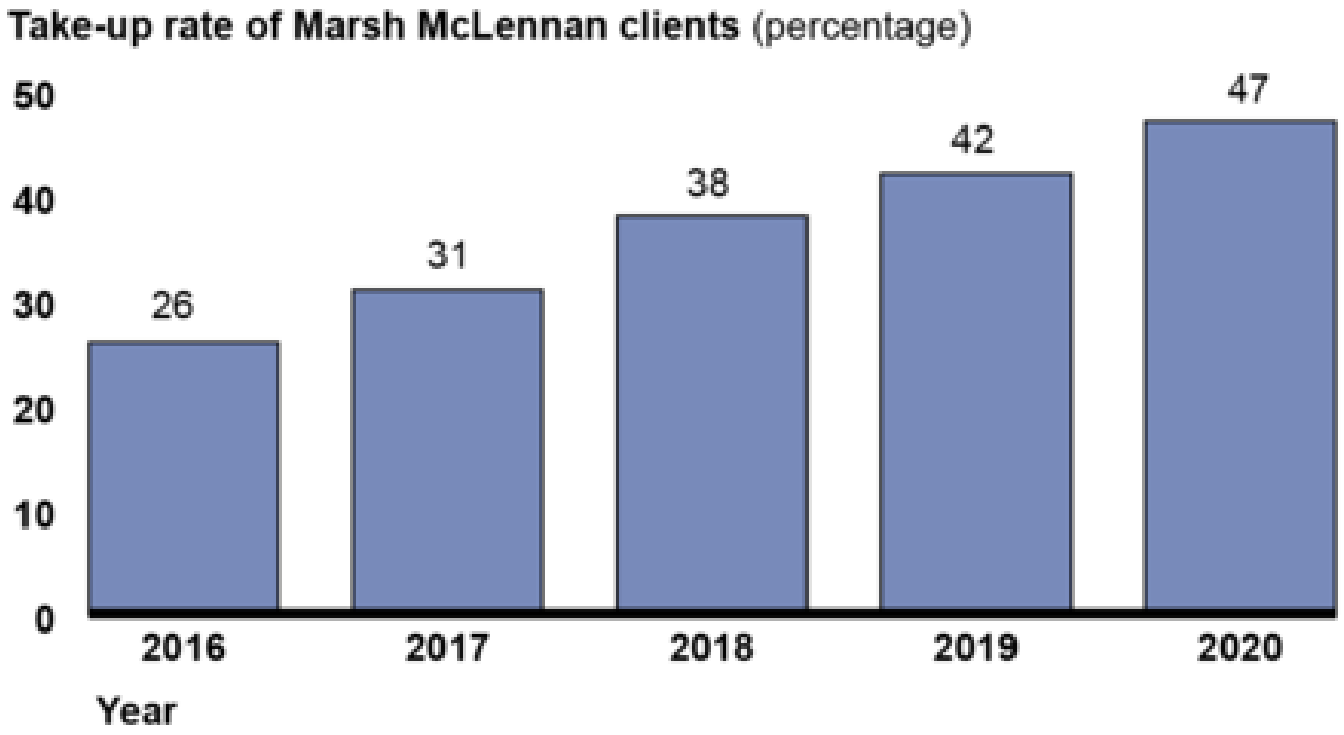
2021 Marsh Report

- Cost of ransomware attacks in U.S. increased by 290%
- Ransomware incidents have increased worldwide by 170%
- Insurers excluding coverage in geographic areas and capping claims.
- Cost of cyberinsurance increased 96%

The Marketplace

- Loss Environment
- Systemic Risk Concerns
- Reinsurance
- Available Capital

Key Trends



Source: GAO presentation of data from Marsh McLennan. | GAO-21-477

What is Cyber Insurance?

- Mitigates a company's cyber risk.
- Covers financial losses following a cyber event.
- Helps with costs associated with remediation.

Emerging Coverage

- Cyber insurance is a new coverage in comparison to most offered by the insurance industry.
- Coverages have changed due to the novel nature of cyber risks.
- Underwriters have limited data to formulate risk models.

Who Needs Cyber Insurance?

Is it a necessity?

- Business with an online component.
- Business that sends of stores data.
- Systems that house private, personal data are also at risk.
- Businesses dependent on computer networks.

4 Myths about Cyber Insurance

- "Cyber insurance never pay claims made"
  - 98% of claims are being paid.
- "If I buy cyber insurance, I won't have to worry anymore about cybersecurity"
  - ABSOLUTELY NOT, cyber insurance is not a "cover all" type of contract, and has specific requirements on cybersecurity.

Source: Verizon DBIR and Insurance Information Institute (I.I.I.) and J.D. Power 2019 Small-Business Cyber Insurance and Security Spotlight Survey

4 Myths about Cyber Insurance

- "I have a data breach endorsement to my Business Owner Policy, therefore I'm covered"
  - Data breach endorsements often don't offer the coverage options and limits that businesses need.
- "I'm on the cloud." Why should I worry about this?
  - Data on the cloud can be compromised during a cyber attack (i.e. Microsoft)
  - When cloud services aren't configured properly, safety gaps can occur (Hackers have sophisticated software to scan the web for those safety gaps)

Source: Verizon DBIR and Insurance Information Institute (I.I.I.) and J.D. Power 2019 Small-Business Cyber Insurance and Security Spotlight Survey

Challenges

- Insurers and clients face challenges as cyber attacks are on the rise. These challenges include:
  - Developing cyber insurance products can be hard because insurers don't have much historical data on cyberattack-related costs
  - Determining what's covered can be hard for clients because key terms like "cyberterrorism" don’t have standard definitions

Challenges

- Estimating costs of cyberattacks
- Reliance on data to forecast risks
- New market
- Evolving industry


Cyber Insurance Coverages

Types of Cyber Insurance Coverage

1. Privacy Liability Coverage
2. Network Security Coverage
3. Errors and Omissions Coverage
4. Media Liability Coverage
5. Network Business Interruption Coverage

Privacy Liability Coverage

- Employee and customer information is highly sensitive, and data breaches that expose this data threaten the security of your customers and employees and leave your company vulnerable to liability.
- Company is protected from consumer class action litigation, along with a funding settlement after a data breach or cyber incident.
- May also over legal expenses, penalties, and fines.

Network Security Coverage

- Business email compromises
- Cyber extortion demands
- Data breaches
- Malware infections
- Ransomware

Media Liability Coverage

- Printed advertising
- Online advertising
- Social media posts

Network Business Interruption Coverage

- Fixed expenses
- Lost profits
- Extra costs

Cyber Liability Coverage

Errors and Omissions Coverage

- Protects company from cyber events.
- Covers company when those cyber events hinder services and the ability to fulfill contractual obligations.
- Can also protect against breaches of contract.

Ransomware + Cyber Insurance

- No standard ransomware policy.
  - Coverage varies depending on the insurer.
- Some insurers are accounting for increased risks.
  - Increasing premiums.
- When included in a cyber policy, ransomware coverage has a lower sublimit.
- New products are evolving.


Other Cyber Considerations

Cyber Hygiene Controls

- Multifactor authentications
- Email filtering
- Cybersecurity Training
- Response plans

Cyber Standards

- Backup Practices
- Defensive Software
- Cybersecurity Training
- Response Plans
- Remote Access

Cybersecurity vs. Data Privacy

Cybersecurity	Data Privacy
Intended to regulate interstate commerce standards for security and risk mitigation in cyber commerce	Intended to provide consumers protections in how their data is obtained, used, stored, and protected


Regulatory Considerations

Executive Order 14028

This document is scheduled to be published in the Federal Register on 05/17/2021 and available online at federalregister.gov/d/2021-10460, and on govinfo.gov

EXECUTIVE ORDER
14028
- - - - - - -

IMPROVING THE NATION'S CYBERSECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private

Cyber Incident Notification Act

- Requires CISA to “consult with appropriate private stakeholders” before publishing the rules that will govern the incident-reporting program.
- Requires CISA to determine which companies to include in the regulation, “based on assessment of risks posed” by the disruption of their operations.
- Immunize companies from lawsuits stemming from the data they share with the government.

NAIC Insurance Data Security Model Law

- Establish data security standards for regulators and insurers
- Adopted in 18 states
- Developed in responses to high-profile data breaches of insurers
- Requires insurers to develop, implement, and maintain an information security program, investigate any cybersecurity events, and notify the state insurance commissioner of such events

New York Cybersecurity Requirements for Financial Services Companies

- The rule applies to insurance companies, banks, and other financial services companied regulated by DFS, and requires these entities to adhere to new standards to protect consumers from cyber threats
- Requirements include:
  - Annual Risk Assessment
  - Cybersecurity Policy
  - Third-Party Service Providers
  - Incident Response Plans

State Regulations

California: CPPA and CPRA

Wisconsin: 2021 Wis. Act 73

Virginia: Consumer Data Protection Act (CDPA)

Colorado: Colorado Data Privacy Act

Florida: Data Privacy Law

Value of Cyber Insurance

- Risk Financing
- Business Continuity
- Risk Prevention
- Crisis Management

Questions?

Contact

Fred E. Karlinsky

Shareholder & Global Chair,
Insurance Regulatory &
Transactions Practice

Greenberg Traurig, P.A.

(954) 768-8278

Karlinskyf@GTLaw.com