Cyber Insurance
Key Considerations for Higher Education

May 11, 2023

BOND SCHOENECK & KING ATTORNEYS

Today’s Presenters

Gabriel S. Oberfield

Senior Counsel
goberfield@bsk.com
New York, NY

Introduction

- Cyber is one of the most significant risks facing Higher Education and the Insurance Market
  - Risks of liability exposure for cyber are becoming more prevalent.
  - Insurance is the most accepted business practice for risk transference. Accordingly, cyber insurance policies hold more value today than ever.
  - As a result, cyber insurance industry is maturing fast and we all have to keep up.
  - One size does not fit all.

This webinar will review the cyber insurance marketplace and key considerations for higher education institutions in purchasing or renewing cyber insurance policies

Need for Cyber Insurance

- As discussed in prior webinars in our Cyber series, higher education needs cyber insurance to mitigate the risks of cyber attacks due to:
  - Heavy reliance on technology to operate; decentralization,
  - Large volume of personal data,
  - Compliance with growing body of privacy regulations,
  - It’s a contractual requirement (counterparties require it),
  - Your board requires it,
  - Your rating agency requires it for an acceptable bond rating,
  - You have exposure from third-party service providers.

Basics of Cyber Insurance

- Cyber insurance is generally designed to protect against a wide variety of risks:
  - Network security
  - Privacy liability
  - Network business interruption
  - Media liability
  - Errors and Omissions

- Additional coverage available (social engineering, brand reputation damage, replacement equipment)
- Many traditional liability insurance policies now have exclusions for cyber-related risks

Cyber Insurance Underwriting

- The key information needed to assess cyber liability risk is collected in the **insurance application**, which becomes part of the terms of coverage. False statements in the application could void coverage. So first basic rule is to pay careful attention to information submitted in the application. **Dynamic area**
- Mind the gaps.
- Non-Standard Forms.
- Exclusions, policy limits, sublimits, deductibles for each type of coverage.

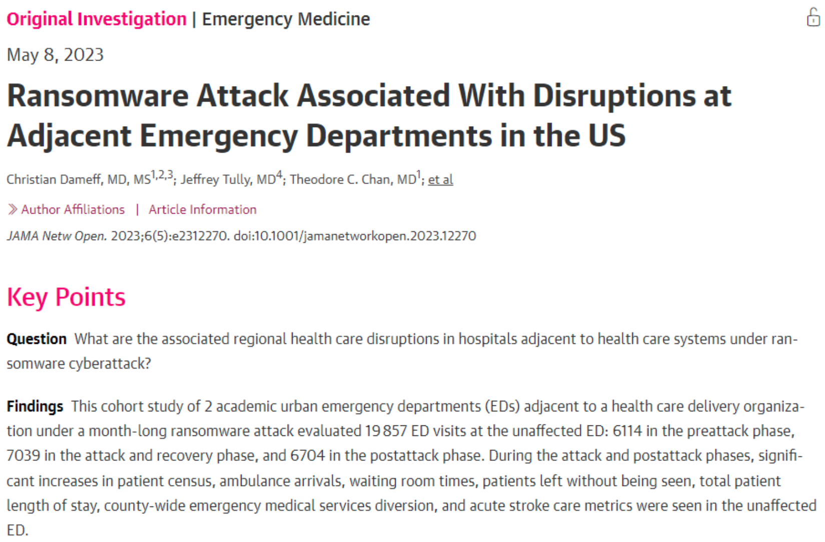
Cyber Insurance Crisis 2021-2022 and its Impact

- Perfect storm of market disruption:
- Frequency of attacks
- Dollar Amount of Losses for each attack
- Migration of workforce to remote work
- Loss coverage ratios too high causing decrease in capacity in the market just when demand was increasing
- Reinsurance capacity was scarce as reinsurers became wary of the large losses
- Growing focus by consumers on their individual rights to privacy and state laws allowing private right of action

Result of Cyber Insurance Crisis

- Premium increases, self-insured retentions increases, coverage limits decreased
- Requirements by insurers to contain policy costs
- Changes to coverage and new exclusions (e.g. crypto, IoT coverage, cloud misconfigurations)
- Increased IT budget for cyber risk management
- C-Suite liability for cyber incidents (D&O insurance)

Yet Cyberattacks Continue –
With Myriad Community Consequences



Original Investigation | Emergency Medicine

May 8, 2023

Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US

Christian Dameff, MD, MS[1,2,3]; Jeffrey Tully, MD[4]; Theodore C. Chan, MD[1]; et al

JAMA Netw Open. 2023;6(5):e2312270. doi:10.1001/jamanetworkopen.2023.12270

Key Points

Question What are the associated regional health care disruptions in hospitals adjacent to health care systems under ransomware cyberattack?

Findings This cohort study of 2 academic urban emergency departments (EDs) adjacent to a health care delivery organization under a month-long ransomware attack evaluated 19 857 ED visits at the unaffected ED: 6114 in the preattack phase, 7039 in the attack and recovery phase, and 6704 in the postattack phase. During the attack and postattack phases, significant increases in patient census, ambulance arrivals, waiting room times, patients left without being seen, total patient length of stay, county-wide emergency medical services diversion, and acute stroke care metrics were seen in the unaffected ED.

Full article available here:
(https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585)

Research published **this week** on the regional effects of ransomware (in healthcare) was published in JAMA Network:

> “The study identified that adjacent hospitals to ransomware attacks may experience resource constraints from increases in patient volumes and ambulance arrivals, as well as increased waiting room times, patients leaving before being seen by a clinician, longer patient stays and increases in critically ill patients such as stroke victims.
>
> “The study's authors suggest that targeted hospital cyberattacks may be associated with disruptions of non-targeted hospitals within a community and should be considered a regional disaster.”

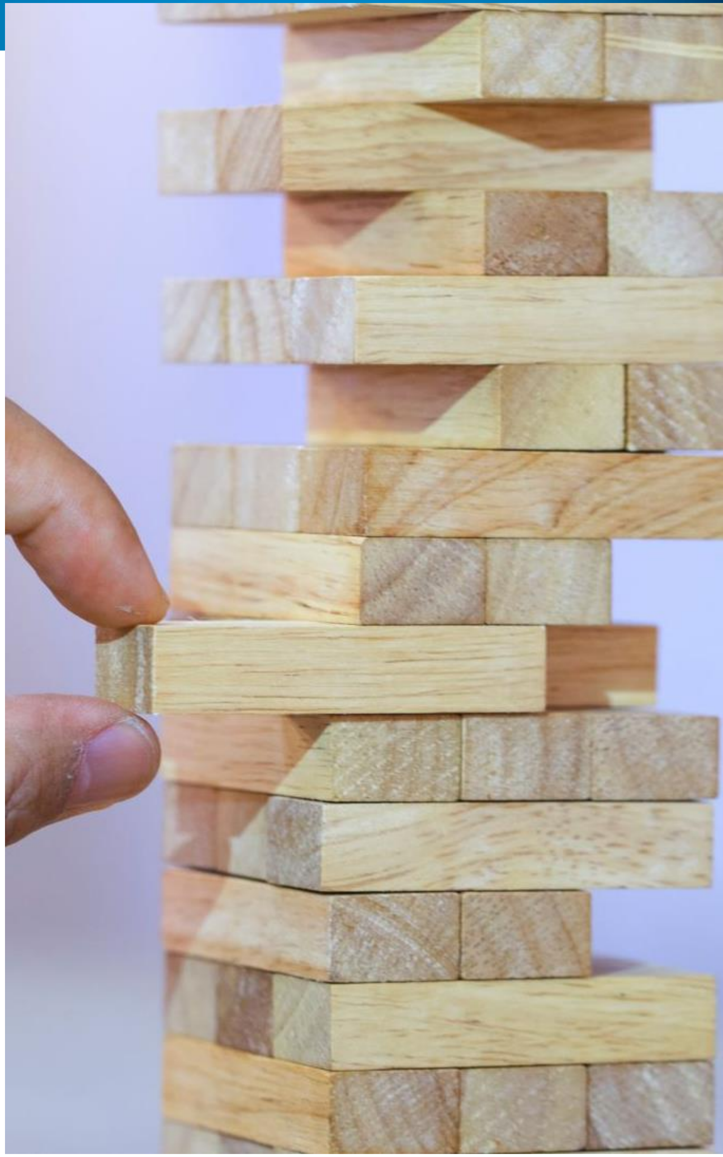
And among IHEs in New York

- In 2021, New York had the highest number of ransomware attacks on schools and colleges, with seven recording, accounting for 10 percent of those recorded, nationally.

- From January 2018 until May 2022, New York schools and colleges endured 21 (publicly disclosed) attacks, affecting 153 schools or colleges, and with the effect of $1.37 billion in costs related to downtime.

Current State of Cyber Insurance…
…*and Trends for the Future*

- The market has shifted profoundly in just 24 months
  - There are new carriers entering the market, which is increasing competition and holding down premium increases
  - That noted: requirements imposed on insureds to have appropriate security protections are a major focus among insurers.



What Are Those Security Protections?

- Cover the key bases:
  - Policies
    - Incident response policy
    - Remote access policy
    - Vendor management policy
  - Make Sure Your Policy Is Robust
    - Some cyber-criminals have been known to review policies of target institutions … and to peg ransom at amounts likely to be paid out

Other Key Attributes for Your Policy

Data breaches (like incidents involving theft of personal information)	Cyber-attacks on your data held by vendors and other third parties.	Cyber-attacks (breaches of your network)
Cyber-attacks that occur anywhere in the world (not just in the United States)	Cyber-attacks determined to be nation-state attackers	Cyber-attacks aided by insiders both intentional and unintentional
Cyber-attacks that lead to extortion (ransomware attacks)	Terrorist acts	Cyber warfare

Source: https://405d.hhs.gov/Documents/tech-vol1-508.pdf#p38

Other Key Attributes for Your Policy – Continued

Test whether your cyber insurance provider will:

- Defend you in a lawsuit or regulatory investigation (called a “duty to defend”)
- Provide coverage more than any other applicable insurance you have
- Offer a breach hotline that’s available every day of the year at-all-times
- Provide access to third-party breach specialists … working on your behalf, not the cyber insurance provider
- Require you to use specific vendors for IR
- Provide coverage for notification costs including printing, mailing, phone centers, and PR assistance
- Loss of business coverage or revenue

Source: https://405d.hhs.gov/Documents/tech-vol1-508.pdf#p38

Stay on Top of the Wave

- Sign up for alerts, track industry knowledge, and stay current

- Regularly assess your vulnerability prioritization

- Explore the services insurers offer in connection with potential policies, e.g., response tools

Avoid Inaction…

…Standing Still Comes with Consequences

- C Suite Liability for Cyber Incidents
  - The U.S. Dept. of Justice and other similar enforcement bodies are starting to hold c-suite leaders accountable for cybersecurity failures at their companies
    - This ties into the importance of D&O – among other upstream protections
    - Managing vendors closely → avoid another liability pathway

Follow the Trends

- Data Privacy laws emerging nationally…

  A. Indiana

  B. Iowa

  C. Montana

  D. Tennessee

  E. Washington My Health Data Act

- These build on policies in place in states, including:

  A. California

  B. Colorado

  C. Connecticut

  D. Utah

  E. Virginia

Standards Specifically Requiring Cyber-Insurance

- No U.S. State has passed legislation requiring a particular group or industry to purchase and maintain cybersecurity or data breach insurance
    - That noted, the nationally emerging privacy requirements suggest that organizations will be expected to take on safeguards, with insurance being logically connected to facilitate operational continuity and recovery

- Some states are offering tax incentives to invest in policies, e.g., Maryland (Maryland Cybersecurity Tax Credit – dating to 2018)
    - New York legislation exploring the same (S4871)
    - Applicability of these incentives to IHEs – not necessarily uniform

Tips for Cyber Insurance Buyers

- Partner with a broker to understand available coverages and secure a policy uniquely tailored for your needs

- Beware of terms…especially *exclusions*
  - *If you've seen one cyber insurance policy, you've seen one cyber insurance policy*

- Protect your organization with a deep enough policy to cover the costs of regulatory enforcement, fines, etc. … think, ahead

- Think about the tiers of insurance you layer in – umbrella policies, stopgap coverage, etc.

- Train, train, train

- Boost your controls – e.g., MFA, network segmentation

Resources

- See, e.g., the work of the ‘405d’ (www.405d.hhs.gov)
  - “The 405(d) Program is a collaborative effort between industry and the federal government to align healthcare industry security practices to develop consensus-based guidelines, practices, and methodologies to strengthen the healthcare and public health (HPH) sector’s cybersecurity posture against cyber threats.
  - “…The 405(d) Program is focused on providing the HPH sector with useful and impactful resources, products, and tools that help raise awareness and provide vetted cybersecurity practices….”

  ○ Recently refreshed resources include:
  - Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP *2023 Edition*)
  - Hospital Resiliency Landscape Analysis

Questions?

Contact Us

Gabriel S. Oberfield

Senior Counsel
goberfield@bsk.com
646-253-2360
New York, NY