

Increasing Ransomware Attacks Trigger Major Shifts in Cyber Insurance

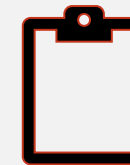
October 6, 2021



Resources available on the MHEC website post-event.



Submit questions in the Q&A.



Please complete our survey.

Cyber Insurance

- Tailored to deliver the right mix of risk transfer and advisory solutions for institutions to
 - ✓ assess,
 - ✓ manage, and
 - ✓ respond to institutional risk
- Policyholders are expected to protect data and systems; these areas will be scrutinized before pricing cyber insurance policies.
- More info: mhec.org/cyber

Today's Presenters from Marsh



Frank Cella



Lindsay Combs



Nicholas Wendell

MHEC Security Services Contracts

- Competitive RFP Process
- Five Product and Service Categories:
 - Security Threat Intelligence Products and Services (TI);
 - Security Information and Event Management (SIEM),
 - Managed Security Services (MSS),
 - Security Consulting Services (Consulting), and
 - Security Awareness Training (training).
- Six contracts awarded, additional contracts pending
- More info: mhec.org/security-services

Contacts for Additional Questions

Property & Cyber
Insurance:

Carla Ahrens

*MHEC Property Program
Manager*

(612) 677-2776

carlaa@mhec.org

Security Services
Contracts:

Deb Kidwell

Consultant

(573) 864-2024

debk@mhec.org

2021 US Education Cyber- Insurance Market Update for MHEC

October 6, 2021

Ransomware epidemic triggers major shift in cyber-insurance –



What risk controls can your institution implement to mitigate cyber-risk and meet the underwriting expectations of insurers?

Challenges Driving the Global Cyber Market Today

Ransomware

- Ransomware perpetrators carry out more than **4,000 attacks daily**
- **One in 3,000 emails** that pass through filters contains malware
- **95 new ransomware families** were discovered in 2019
- The global cost associated with ransomware recovery will exceed **\$20 billion in 2021**
- **Terms being readjusted** to account for this growing trend

Frequency and Severity Beyond Ransomware

- Increasing sophistication and morphing nature of cyber attacks **reshaping loss development patterns**
- An attacker only needs to be successful one time; the insured 100% of the time
- Insurers' rating models did **not accurately predict loss severity**
- **Evolving privacy regulation** mean potential increases in regulatory fines & penalties, wrongful collection/ BIPA claims

Systemic Loss and Aggregation Exposure

- **Difficulties in understanding and quantifying exposure** – one malware can impact multiple organizations around the world
- Increased awareness of aggregation events and supply chain risk, **causing capital volatility** (Solarwinds, MS Exchange, Accellion one after the other)
- Unlike in the past years when the market was soft, insurers are now forced to **price for "systemic event losses"**

Coverage / Product

- Cyber **coverage has broadened significantly** in the past 7 years, e.g. Blanket Dependent Business Interruption cover, no sublimits, and customized policy language, which is now causing concerns for Insurers
- Coverage sustainability is challenged by **deteriorating profitability**

Market Contraction

- Increasingly **conservative limit deployment** in response to increased volatility from large losses and deteriorating financial performance
- Insurers now see the "cyber" product line as **both long tail** (liability, regulatory) as well as **short tail** (ransom demand and breach response expenses).
- There is now a significantly **higher price to obtain capacity**



Cyber Trends

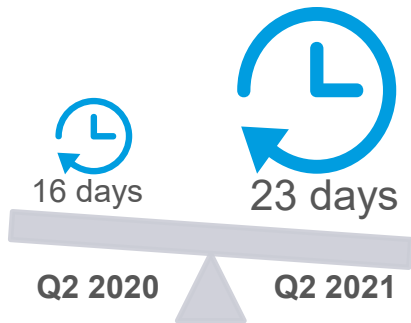
Dominated by ransomware, regulations & supply chain cyber risk



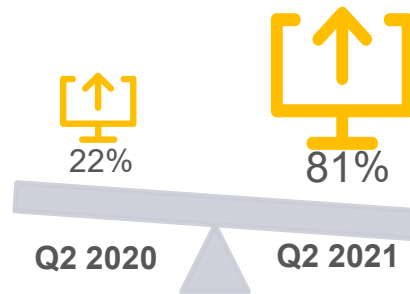
Ransomware attacks continue to increase in frequency, severity & sophistication – impacting orgs of all sizes & industries:

Average downtime:

Cases with data exfiltration:



44% YOY increase



~270% YOY increase

\$ 2021 ransom headlines:
~\$800k average ransom payment

- Large insurer: \$40M paid
- Oil pipeline: \$4.4M paid
- Infrastructure: \$50M demanded
- Food manufacturer: \$11M paid
- Chemical distribution: \$4.4M paid
- Tech hardware: \$50M demanded



Privacy regulations are intensifying and there's still a patchwork approach:







- **GDPR** fines are growing (~\$27M BA, ~\$24M Marriott, ~\$41M H&M)
- **CCPA** (California Consumer Privacy Act) and similar legislation (i.e. VA CDPA) allow for **private rights of action** and require **additional compliance** efforts
- **BIPA** (IL Biometric Information Privacy Act) litigation is **expensive** and is **on the rise** with increased use of biometric identifiers, especially for employee access – driving additional underwriting questions



Supply chain and systemic risk now garner more focus:

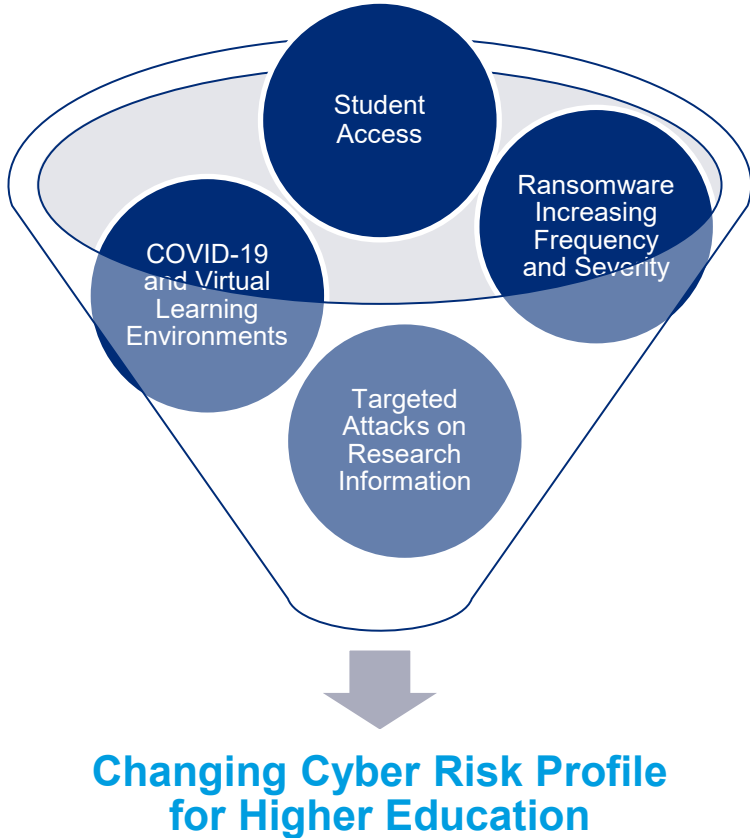
- **Aggregation** exposure a concern for underwriters
- **Systemic loss** – possible cyber risks:
 - **Common vulnerabilities** – in hardware or software
 - **Common dependencies** – vendors (such as cloud providers) and software
- **Cyber events** are driving increased scrutiny: **SolarWinds**, **Accellion**, **Microsoft Exchange**, & **Kaseya**

Cyber Insurance Market Snapshot

<h2>Claims</h2>  <p>Overall claims frequency and severity remains high driven by ransomware. Mild improvement in some categories but overall, loss ratios continue to deteriorate.</p>	<h2>Rates</h2>  <p>Loss environment has resulted in accelerating pricing pressure <u>even on loss free accounts with good controls</u>. Expect rate increases to continue rising through the rest of the year.</p>	<h2>Capacity & Attachment</h2>  <p>Claims activity and future uncertainty have resulted in insurers aggressively managing global capacity and increasing SIRs. Excess pricing increasing at a faster rate than primary, compounding increases.</p>	<h2>Underwriting</h2>  <p>Full application & responses to ransomware Q's are required; carriers using third parties to externally scan environments. Underwriters will inquire about recent systemic/supply chain events & related exposures</p>	<h2>Coverage</h2>  <p>Many carriers scaling back ransomware-related coverages (sublimits or coinsurance), or not offering coverage if poor controls. More scrutiny on contingent business interruption due to systemic risk concerns.</p>
<p>+55% YoY Increase In Loss Ratios, indicating an industrywide underwriting loss for 2020</p>	<p>Aug Cyber Premiums: +112.6% average increase +155% 3rd quartile increase 150%+ looking forward</p>	<p>Aug Cyber Renewals: 21% reduced limits 17% increased limits 62% increased SIRs Driven by insureds minimizing increases & less available capacity.</p>	<p>12 Key Controls & Best Practices are now viewed by carriers as essential</p>	<p> in average BI / CBI waiting periods due to ransomware and supply chain attacks</p>

Cyber Insurance Market Snapshot – Higher Education

Higher Education Cyber Risk Profile is Evolving



Cyber Insurance Market is Turbulent for Higher Education

- The capacity available for higher education risks is shrinking.
- Rates increases are more severe in the higher education space than the broader cyber marketplace
- Carriers that are willing to offer full ransomware coverage are demanding a premium for it.
- Control differentiation is critical – there are specific controls that the market sees as “minimum standards” – without these controls, some institutions may have trouble finding solutions.

Top Cybersecurity Controls

Insurability is increasingly dependent upon controls

Preparation for underwriting:

1. Get started early!
2. Ensure adequate cybersecurity controls are in place (Cyber Self-Assessment) – where improvements are needed, leverage [Cyber. Catalyst vendors](#).
3. Expect more rigorous underwriting and more detailed questions from underwriters.
4. Without positive responses in the top 12 control categories, coverage offered and insurability may be in question.

Multi-Factor Authentication (MFA) for remote access & admin/ privileged access	Endpoint Detection & Response (EDR)	Secured, encrypted, and tested backups	Privileged Access Management (PAM)
Patch management / Vulnerability management	Logging & monitoring / Network protections	Email filtering & web security	Cybersecurity awareness training / phishing testing
Cyber Incident Response planning & testing	End of Life Systems should be replaced or protected	Hardening techniques including Remote Desktop Protocol (RDP) mitigation	Vendor / Digital Supply Chain Risk Management

Note: Each insurance carrier has their own specific control requirements that may differ by company revenue size & industry class

Cyber Insurance Market Preparation

Develop strategy early to execute on goals

What to expect

How to prepare & execution strategy

Claims

- Ransomware continues to increase; supply chain attacks are of concern; regulatory actions are garnering more focus; and media copyright infringement claims are rising.
- Underwriting actions since beginning of 2021 appear to have some mitigating effect*, but too soon to tell market impact.

Improve security & claims posture:

- Leverage carrier preferred vendors and Marsh Catalyst solutions to improve security posture.
- Update and practice incident response plan specific to ransomware scenario.
- Identify vendor and legal counsel partners you might engage and evaluate against insurer's panel.
- Identify any problematic IP addresses & remote desktop protocols (RDP).

Structure

- **Capacity & attachment:** Expect tower restructuring as carriers limit capacity and change appetite.
- **Coverage:** Clients with lesser cybersecurity maturity should expect potential limitations on coverage – including sublimits, coinsurance or non-renewal.
- **Rates:** Even better than average risks will see increases (new buyers included.)

Explore structure options:

- Demonstrate strong ransomware controls during the underwriting process.
- Prioritize program components & goals: carrier partners, limits, attachment, and consider ability to retain risk.
- Consider alternative terms and conditions to minimize increases & maximize coverage, including increased retentions and alternative limit options.
- Use of insurers in the US, London, & Bermuda may increase terms available.

Under-writing

- Controls most effective at mitigating current risks will continue to garner underwriter focus – it is essential to address potential security gaps **prior to** underwriting to achieve optimal results.
- Excellent controls are now the baseline to access coverage but have little impact on pricing – all clients will see increases.

Provide robust underwriting data:

- Use Marsh Cyber-Self Assessment to minimize need for multiple supplemental applications (includes ransomware Qs & provides additional insights.)
- Ransomware supplemental will still be required. **Critical to get started early!**
- Highlight significant cybersecurity updates & improvements over past year – especially multi-factor authentication (MFA) & endpoint detection and response (EDR.)

Q&A



This document and any recommendations, analysis, or advice provided by Marsh (collectively, the “Marsh Analysis”) are intended solely for the entity identified as the recipient herein (“you”). This document contains proprietary, confidential information of Marsh and may not be shared with any third party, including other insurance producers, without Marsh’s prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party with regard to the Marsh Analysis or to any services provided by a third party to you or Marsh. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. All decisions regarding the amount, type or terms of coverage shall be your ultimate responsibility. While Marsh may provide advice and recommendations, you must decide on the specific coverage that is appropriate for your particular circumstances and financial position. By accepting this report, you acknowledge and agree to the terms, conditions, and disclaimers set forth above.

Copyright © 2021 Marsh LLC. All rights reserved.