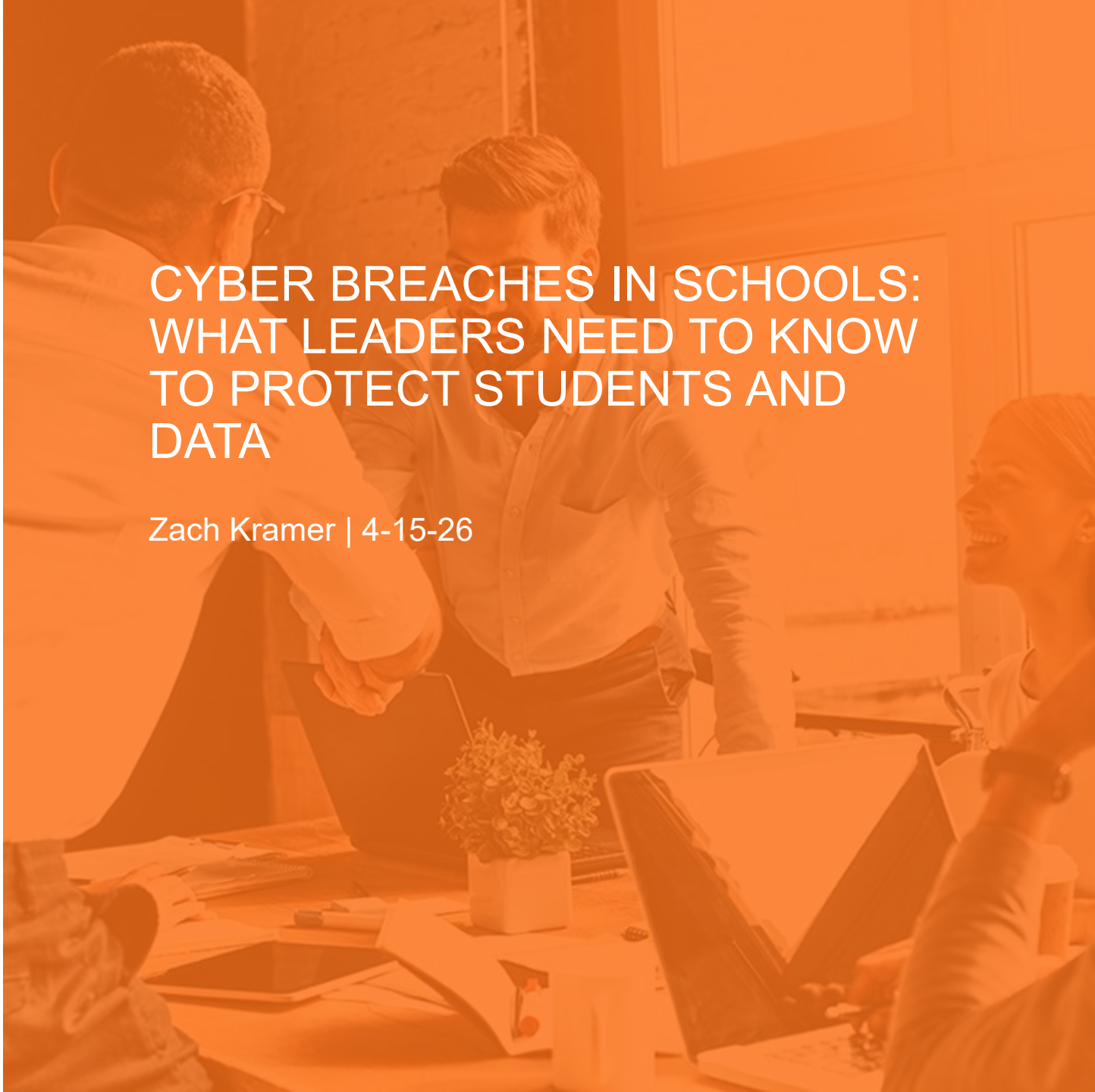
RPS RISK PLACEMENT SERVICES

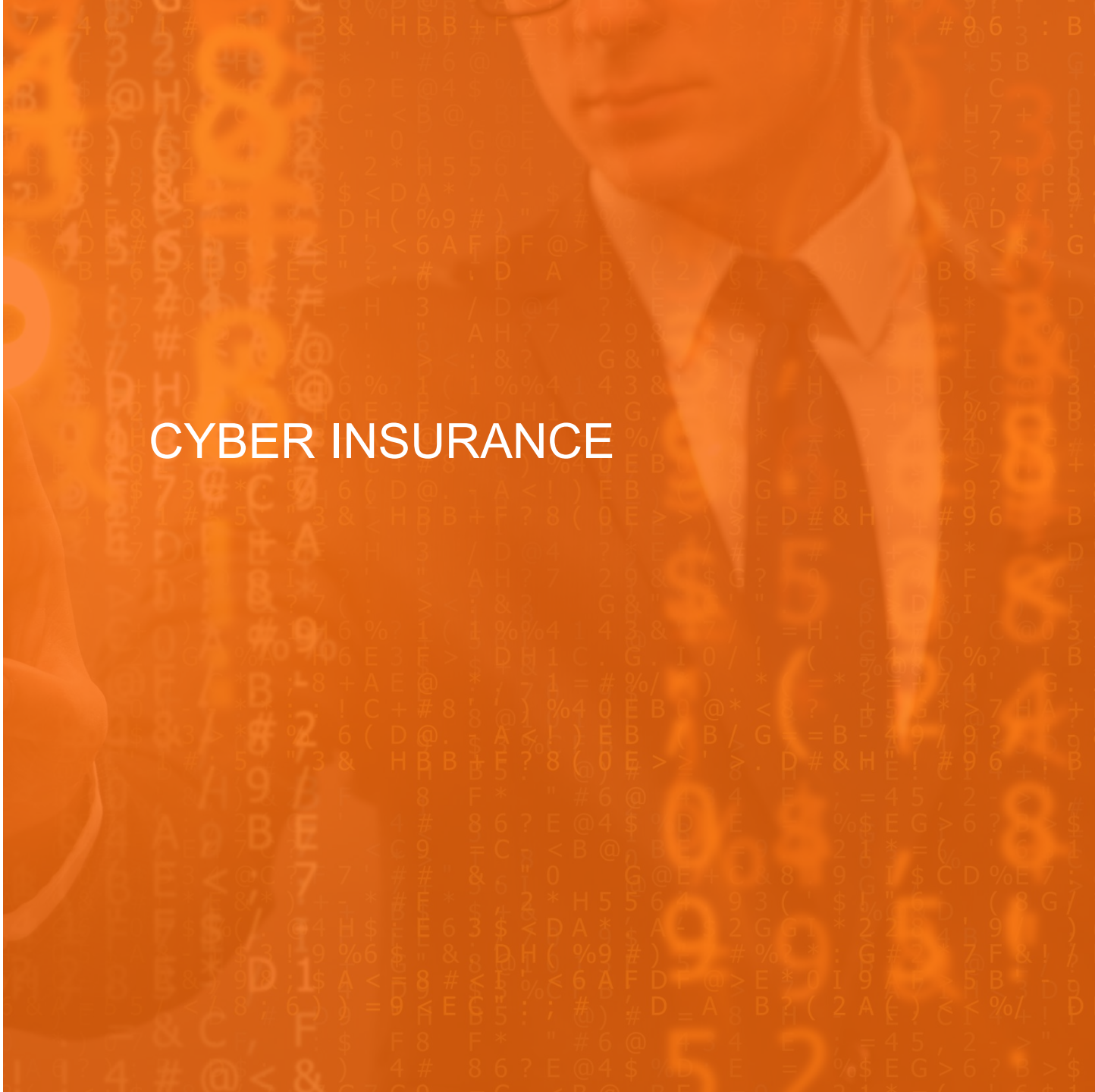
CYBER BREACHES IN SCHOOLS: WHAT LEADERS NEED TO KNOW TO PROTECT STUDENTS AND DATA

Zach Kramer | 4-15-26



RPS RISK PLACEMENT SERVICES

CYBER INSURANCE



Cyber Insurance

An overview of an appropriately designed cyber insurance program

3rd PARTY LIABILITY

Coverage to defend an insured from allegations of liability in the areas of Privacy, Security, Media, and Regulatory.

CYBER RISK MANAGEMENT

Access to resources to help mitigate susceptibility to cyber attacks, including:

- RPS eRiskHub information portal
- Numerous carrier-specific offerings for:
  - Policy & procedure templates
  - Employee training
  - Proactive network defense tools including inbox and browser protection

1st PARTY INCIDENT RESPONSE & CYBER EXTORTION (RANSOMWARE)

Resources to help insureds respond to costly data privacy and security incidents such as ransomware attacks, data breaches, Ddos attacks and more. Coverages include legal assistance, digital forensics, cyber extortion negotiation and ransom payment, customer notification, PR assistance, credit monitoring and call center services.

BUSINESS INTERRUPTION

Critical coverage excluded by property insurance that enable the insured to recover lost profits due to an unanticipated interruption in their network, or a network they are dependent upon to do business. Critical data restoration coverage to help ensure operational resiliency in the fastest manner possible, post-attack.

CYBER CRIME

Coverage offerings involving the loss of money, securities or goods in a variety of cyber crime scenarios including:

- Social Engineering
- Funds Transfer Fraud
- Invoice Manipulation
- Services Fraud (Crypto-jacking, telephone & utility fraud, etc.)

RPS

RPS RISK PLACEMENT SERVICES

CYBER CLAIMS

LIABILITY COVERAGES

Coverage Grant	Claim Scenario	Notes
Privacy Liability (Including Employee Privacy)	The insured mistakenly posts the private information of thousands of its customers online. The information contained financial information, social security numbers and account passwords. A class of affected customers sued the insured for damages suffered resulting from the unauthorized release of their information.	
Privacy Regulatory Claims Coverage	A large data breach suffered by the insured drew the attention of State privacy regulators and resulted in defense costs associated with the investigation and a sizeable fine for violation of the State's privacy laws.	- Fines & penalties insured where allowable by law - GDPR wording has been added by name to the definition of "Privacy regulations" - CCPA and IL BIPA are not mentioned by name, but covered by virtue of policy construction (where allowable by law)
Security Liability	An overseas hacking group gained unauthorized access to the insured's network and utilized the network as a host, enabling them to disguise their distributed denial of service attacks against other businesses. The insured was unaware of the intrusion and was presented with a lawsuit for damages suffered by the victims due to the insured's failure to protect the security of their computer system.	
Multimedia Liability	Allegations of defamation contained in a blog produced by the insured's marketing team on their website led to a lawsuit from one of the insured's competitors. Significant costs were incurred to defend the insured in this matter.	- Includes the insured's social media footprint - Includes IP infringement – not patent "Unless such event occurs as a result of a "Security Compromise".
PCI DSS Assessment	The insured suffers a data breach involving the credit card numbers of thousands of their customers. They incur significant fines and expenses to their bank and card association, and, have to pay a Qualified Security Assessor (QSA) to conduct an audit to prove their compliance with the PCI Data Security Standards.	- See expanded definition of "Breach Response Costs", which includes cost of mandatory audit by a Qualified Security Assessor (QSA) and/or cost of a PCI Forensic Investigator to shadow the PFI following a "Security Breach".

FIRST PARTY COVERAGES		
Coverage Grant	**Claim Scenario**	**Notes**
Security Breach Response Coverage	A breach of the insured's systems allowed the perpetrator access to the protected health information of 20,000 current and past patients. The event led to extensive expenses incurred for legal assistance, the hiring of IT forensic investigators, a PR firm, offering identity restoration services, setting up a call center to respond to inquiries, and notification to all of their affected patients.	- No retention for use of Breach Response Counsel - Security Breach Response Coverage is now among the 1st Party coverages with no annual aggregate limit – (coming in Update)
Cyber Extortion	The insured suffers a ransomware attack on their network and is unable to access their servers or their backups. The perpetrator has demanded a ransom the equivalent to $700,000 in bitcoin. The Cyber Extortion insuring agreement pays for the experts to assist and the money to pay the ransom if it is determined that the only means of resolving the situation is to do so.	- Ransomware - Cryptocurrency payment included
Business Income and Digital Asset Restoration	As a result of the insured's network being inaccessible due to infiltration of malware, their ecommerce site was also down, causing significant income loss and extra expenses incurred to establish work-around procedures.	- System Failure - Insured's System - Third Party Systems
Systems Integrity Restoration (aka: "Bricking")	The insured's network is infected by a malicious malware attack, causing many of their physical servers (hardware) to be rendered useless after the event. The Systems Integrity Restoration extension on their Business Income and Digital Asset Restoration insuring agreement allowed them to replace the affected hardware up to a sub-limit. Property damage of this nature is typically excluded from Cyber risk policies.	
Computer System (aka: "Betterment")	After experiencing a particularly malicious virus on their network, the insured determined that a more secure version of their software platform was required, however, the cost to replace the new system was 15% higher than the cost of their existing system. The "betterment" provision in their policy allowed them to do this, up to 25% more than the cost to replace the original system, subject to a sub-limit.	

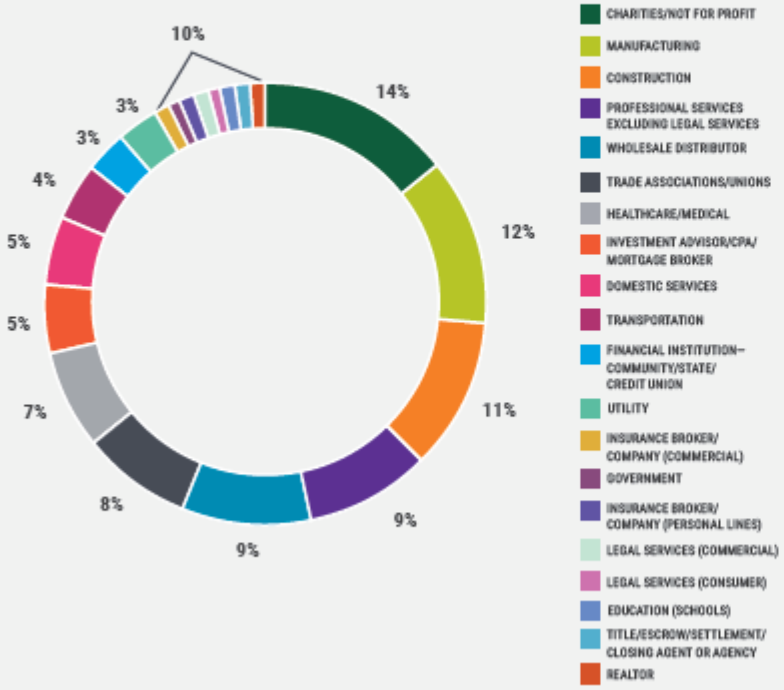
CYBER DECEPTION & ELECTRONIC FRAUD

Coverage Grant	Claim Scenario	Notes
Cyber Deception	CFO receives email from someone purporting to be the company's CEO, directing transfer of $100,000 to a vendor, with wiring instructions. The email was fraudulent. The CFO doesn't verify the email's authenticity and sends the funds - unable to recover the money once discovered that the CEO was being impersonated.	- You will not find the words "Social Engineering" in the policy. It is referred to as "Cyber Deception". - Includes funds held on behalf of others (coming in update) - No call-back requirement
Phishing	The insured's system is hacked and perpetrators, able to familiarize themselves with the company's billing practices, send out fraudulent invoices to customers, re-directing funds to their own account. Insured is unable to collect the receivable due to them because their clients already "paid their" invoice – just unknowingly to the wrong person. Were it not for the insured's failure to adequately protect their system, the loss would not have occurred. This is a first-party loss for the insured.	- Also known as "Invoice Manipulation" , "Reverse Social Engineering" or "Push Payment Fraud" in other policies - Beware of third-party sub-limits offered here by other carriers – should be contemplated under the 3rd party Security liability insuring agreement at full policy limits.
Telephone Hacking	The insured notices excessive long distance charges on their account and discovers their system has been hacked and the perpetrators are utilizing the system to make unauthorized long distance calls.	
Funds Transfer Fraud	An unauthorized third party gains access to the insured's computer system and electronically impersonates the insured, instructing the insured's bank to transfer funds to their fraudulent account.	

Claims

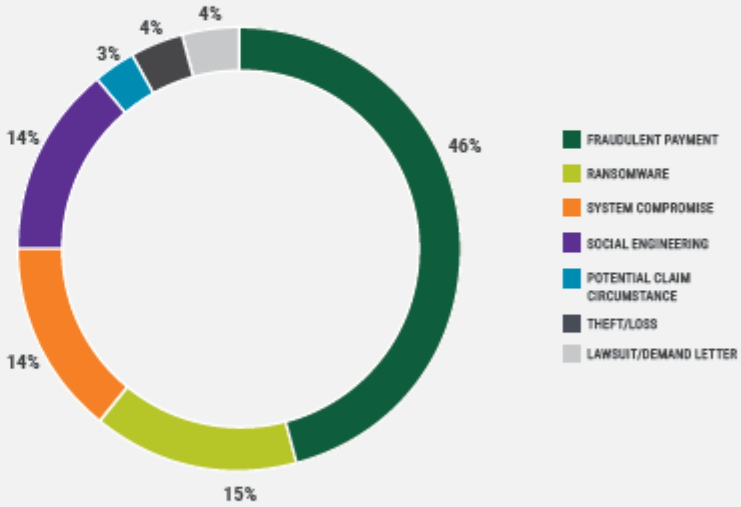
YTD CYBER INCIDENTS BY INDUSTRY

Top three are charities (14%), manufacturing (12%) and construction (11%).



YTD CYBER INCIDENTS BY MATTER TYPE

Major types are fraudulent payment (48%), ransomware (15%), system compromise (14%) and social engineering (14%).



4

3rd Party Vendor Breaches

- **PowerSchool**
- **Blackbaud**
- **Crowd Strike**

Key Takeaways

1. The CrowdStrike event was a global warning, underscoring the urgent need for robust cyber resilience strategies in the face of growing cyber threats and vulnerabilities.

2. Though the event was not the result of malicious actors, there are practical lessons for businesses to learn on operational continuity, crisis management and cyber resilience.

3. Businesses should remain vigilant against opportunistic cyber crime following CrowdStrike, as failure to do so may result in a variety of costly exposures.

Cyber Incident Roadmap

What to expect during a cyber claim

Your organization has experienced a privacy/ security incident. Steps of the claims process will vary, depending on the insurer. Here are some things to expect:

What to Do:

1. Call the 24x7 breach hotline provided in your cyber insurance policy. Have the following info ready:
   - What are the names/numbers or internal contacts for IT, HR and legal?
   - What type of cyber/privacy event?
   - What type of information was compromised?
   - Is your system accessible?
   - How many people involved?
2. Written notice to insurer and insurance broker.

What to Expect:

- After initial call, insurer may recommend breach counsel (privacy attorney) assignment.
- If recommended, you will be asked to sign a letter of engagement
  - This is ok!
  - Protects atty/client privilege
  - In your best interest
  - Claims counsel will advise on coverage first

Possible Next Steps:

- Vendors engaged for:
- IT forensics assessment & recommendations
- If ransomware:
  - Are backups viable?
  - If not, Ransom research (OFAC), negotiation, payment - crypto
  - Data restoration
  - Analysis of data breach implications
- If a data breach:
  - Regulatory review
  - Notification
  - Credit monitoring
  - Call center services
  - PR

DO:

- Utilize the resources/vendors provided by your cyber insurance policy
- Report to insurer early in the process, even if unsure
- Preserve forensic evidence whenever possible

DO NOT:

- Go it alone
- Hire your own vendors, attorneys, etc. and expect reimbursement from insurer later
- Notify constituents, students, parents, media without advice from a qualified privacy attorney, PR firm, etc

RPS

Qualifying for Cyber Insurance

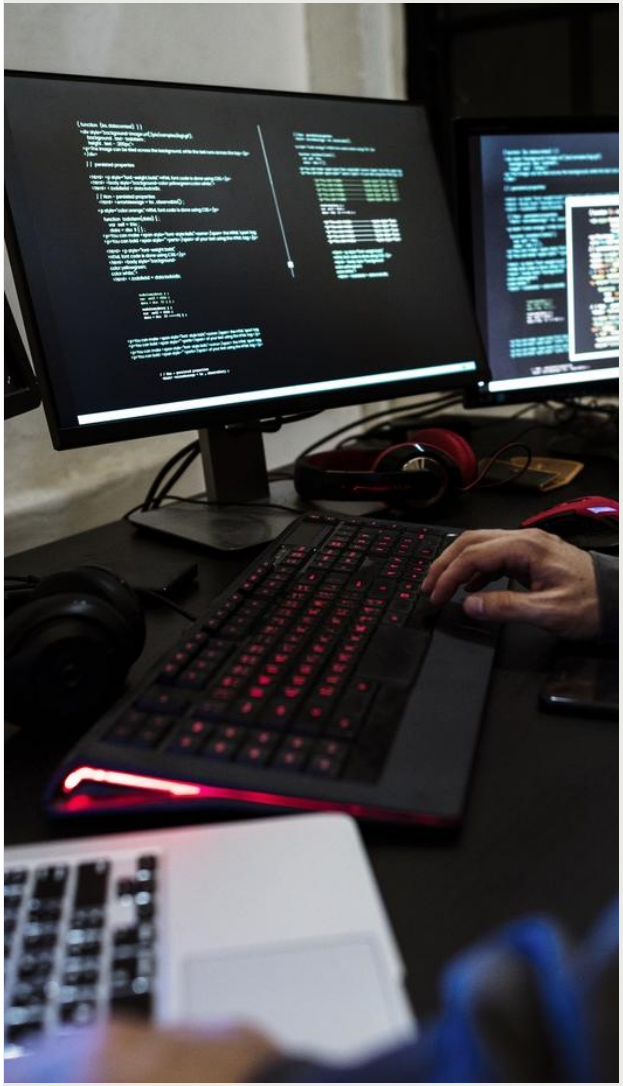
The Cybersecurity Controls Traffic Light System

RED **Minimum** standard of security required for underwriters	• Multifactor authentication (MFA) for employee email • MFA for remote access • MFA for privileged accounts/privileged access • Offsite (preferably offline) backups of critical data. • Deploy an endpoint detection and response (EDR) solution on all managed endpoints • Create an audited written plan for patching critical software and hardware
AMBER Requirements over and above red– **more attractive** to underwriters	• Employee cybersecurity training, including phishing simulations • Strong email filtering tools • Privileged access account security measures • End-of-lfie (EOL)/unsupported software and hardware segregated from the network, with plans to decommission in a timely fashion • Cyber-incident disaster recovery/incident response plan, and segmentation of your computer network by operational function, data classification and operational risk
GREEN Requirements over and above amber– **most attractive** to underwriters	• Local domain control turned off on all owned managed endpoints • Password management • Detailed asset footprint of particular service accounts with domain credentials, services and monitoring • Security information and event monitoring (SIEM) tool • Data loss prevention (DLP) tool • Follow an information security framework

RPS

RPS RISK PLACEMENT SERVICES

CYBER STATE OF THE MARKET



Q1 2026 State of the Market

Cyber

Capacity

Capacity remains strong, although the flow of new entrants into the market is slowing. New financing mechanisms to support additional capacity continue to develop. Obtaining appropriate limits for organizations with solid controls risks is still very achievable.

Coverage

Increases in 3rd party privacy liability claims (namely pixel/web tracking/unauthorized collection) are leading to tighter wording on these types of matters. Underwriters are increasingly wanting to know about AI use. Seeing first signs of coverage innovation since pre-2020.

Losses

Loss frequency is still on the rise, driven by business email compromise, wire fraud and ransomware. Companies are less likely to pay ransoms with better recovery preparedness. Threat actors are more likely to extort for threat of information release rather than decryption. Increases in 3rd party litigation and BI claims contribute to longer tails.

Pricing

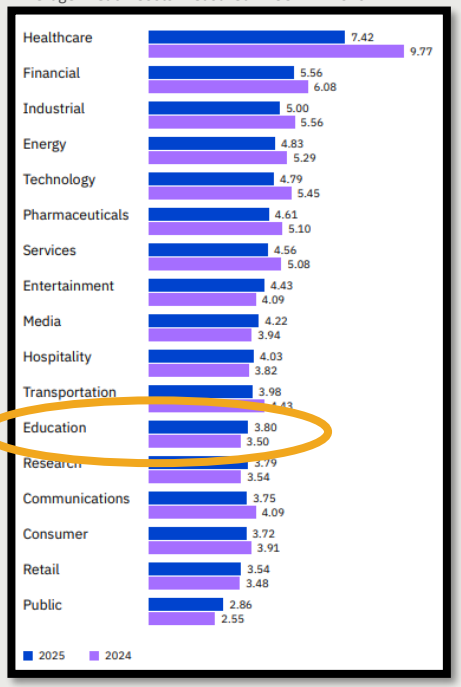
Claims-free insureds experience pricing in the +10% to - 5% range. Flat renewals are still commonplace. Longer tails are contributing to a delayed hardening of the market as these losses continue to develop. We are starting to see change with carriers implementing surgical increases by industry/performance. Large increase in healthcare.

13

Sector Focus: Education

Increasing Frequency. Increasing Severity.
Still a Prime Target.

Average Breach Costs Measured in USD Millions



Source: IBM Cost of a Data Breach Report

24% → Increase in ransomware attacks against schools, colleges and universities in first half of 2025.

Source: Comparitech

Essential Security Controls

Security technology should enable and protect educational activities while remaining as frictionless as possible to users. Key implementations include:

- Multi-factor authentication designed with teacher workflows in mind, understanding that educators often need quick access while moving between classrooms or helping students.
- Backup systems that automatically protect critical data while allowing teachers to focus on teaching rather than manual backup procedures.
- Network design that protects sensitive information while ensuring teachers and staff can efficiently access the resources they need.
- Endpoint protection that focuses on preventing threats without creating barriers to educational software and resources.

Source: 2025 CIS MS-ISAC K-12 Cybersecurity Report: Where Education Meets Community Resilience

Thank You

Zach Kramer

Area Senior Vice President

312 803 5989

Zach_Kramer@rpsins.com