

# CYBER INSURANCE PERSPECTIVES

Focus: Education and Public Sector

June 19, 2023

HACKING DETECTED

INTRUSION DETECTED...

## Our Presenters



Daniel Waldman  
Underwriting Manager  
Starr Insurance Companies



Steve Robinson  
National Cyber Practice Leader  
Risk Placement Services, a division of Gallagher

# Cyber Insurance

**Loss Trends**

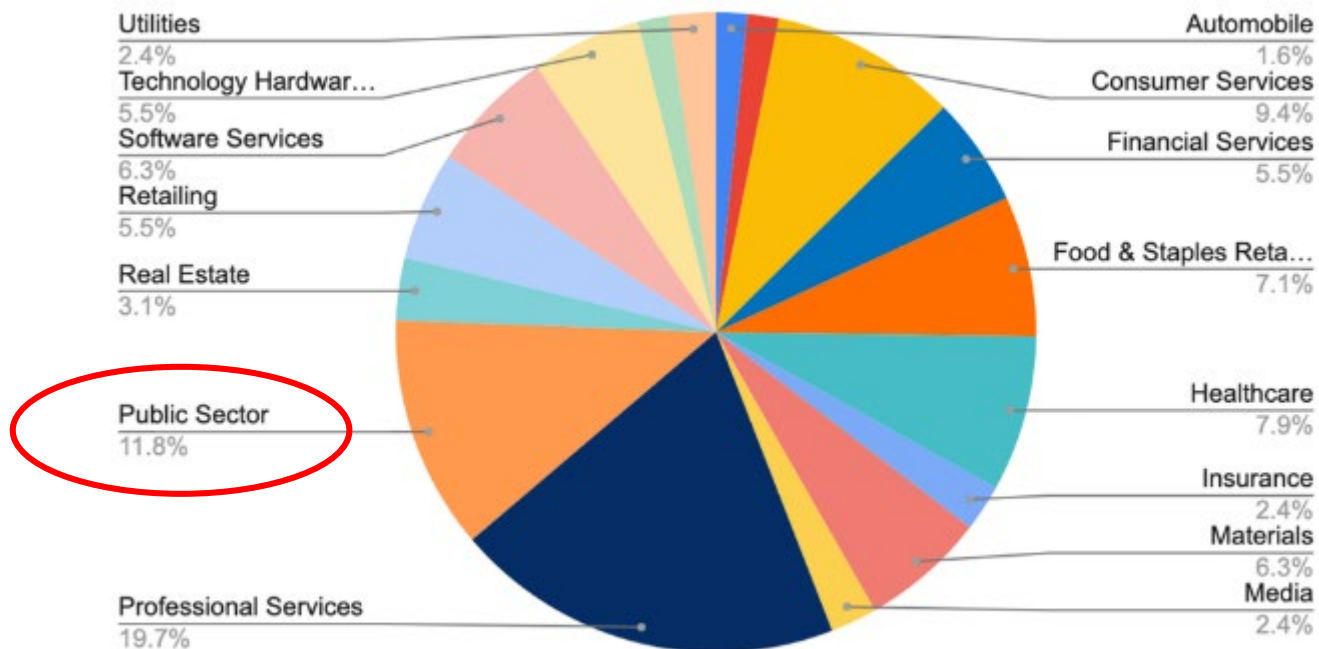
**Market Insights**

**Limits  
Discussion**

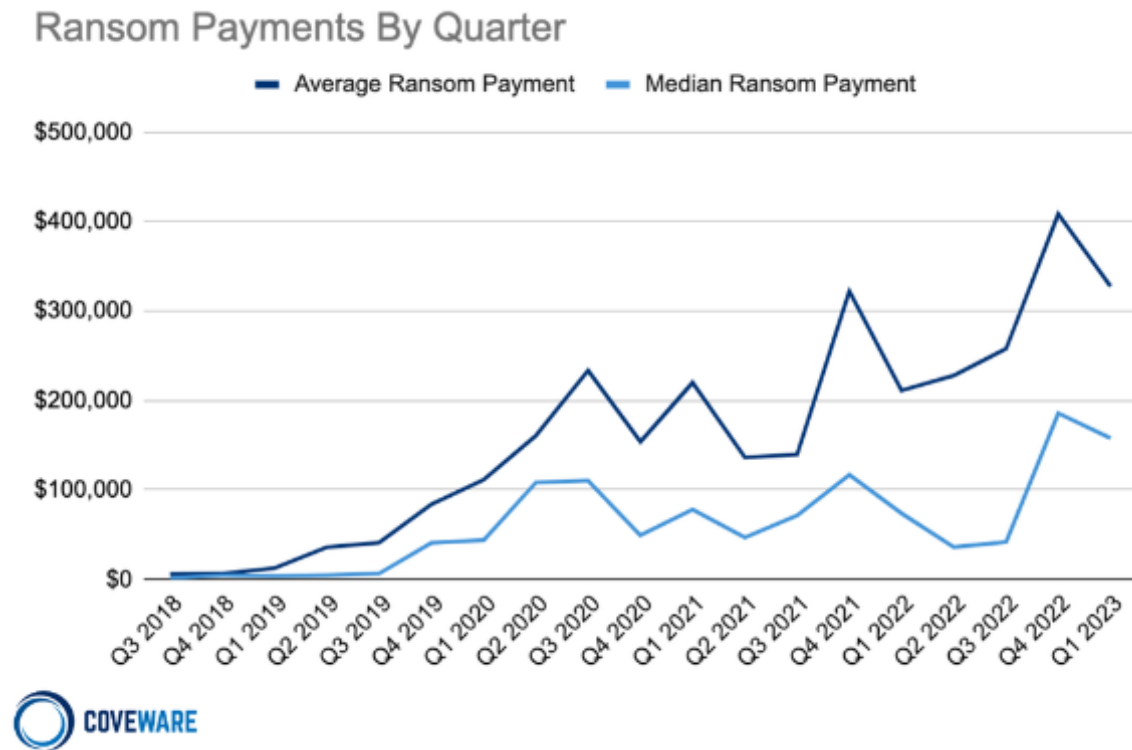
**Why Cyber  
Insurance?**

# Ransomware

Industries Impacted by Ransomware Q1 2023

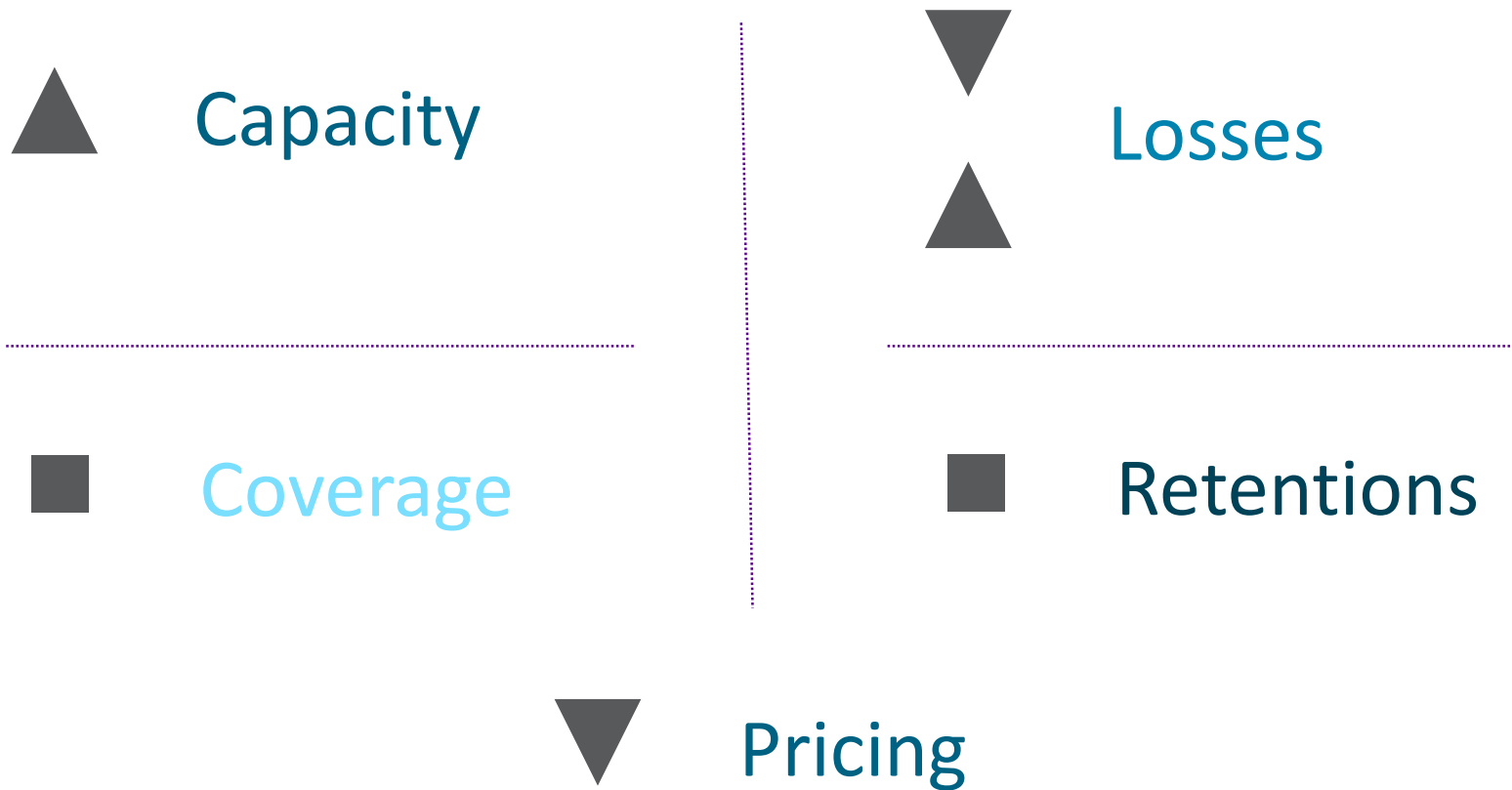


# Ransomware



# 2023 Q3 Update

## State of the Cyber Insurance Market



# Trends in Cyber Insurance Underwriting

Dealing with the threat of systemic risk

- I. Areas in which some cyber insurers are looking to limit their exposure to systemic (wide-spread) risk:
  - Cyber war that accompanies physical/traditional war
  - CVE (Common Vulnerabilities and Exposures)
  - Zero day attacks (such as current MoveIT vulnerability)
  - Pixel and website tracking exclusions
  - Unpatched software
  - End-of-Life software
  - Information Technology/Operational Technology segregation
  - Biometric data collection/use

# Additional Trends of Note

From the front lines of cyber insurance

- A resumed increase in ransomware activity
- Ransomware incidents involving additional threat of disclosure
- Widespread events (ie: Move-IT exploit)
- AI's pending influence in social engineering efficacy
- Dangers of misrepresentation in cyber insurance applications

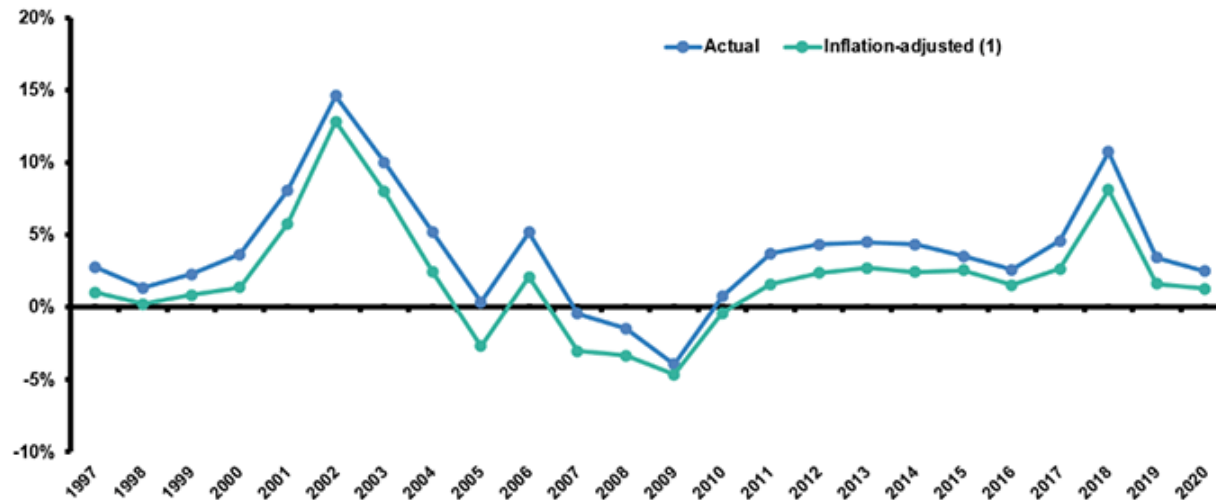
We regret to inform you that coverage under the Policy is not available for the Incident because of a material misrepresentation made by the Insured during the application period that allows Underwriters the right to rescind the Policy. Condition [REDACTED] of the Policy and [REDACTED] law allow an insurer to rescind a policy when: (1) the insured makes an untrue statement of fact or an omission of material fact during the application process, (2) the insured knew the statement was untrue, (3) the insured made the statement with the intent to deceive or recklessly with disregard for the truth, (4) the insurer justifiably relied on the statement, and (5) the false statement actually contributed to the contingency or event on which the policy is to become due and payable. *Chism v. Protective Life Ins. Co.*, 234 P.3d 780, 787 (Kan. 2010) (stating K.S.A. 40-2205(C) imposes the fifth element). As is evident from the facts below, all five elements are satisfied.

While Underwriters have the right to rescind the Policy, they will waive this right if [REDACTED] waives coverage for the Incident, confirms that it has implemented the security protocols it previously misrepresented were in place, and waives coverage for any incident that occurs in whole or in part prior to confirmation that the security protocols are in place. If [REDACTED] is unwilling to do so and rescission is necessary, Underwriters reserve their rights with respect to rescission.

# Additional Trends of Note

From the front lines of cyber insurance

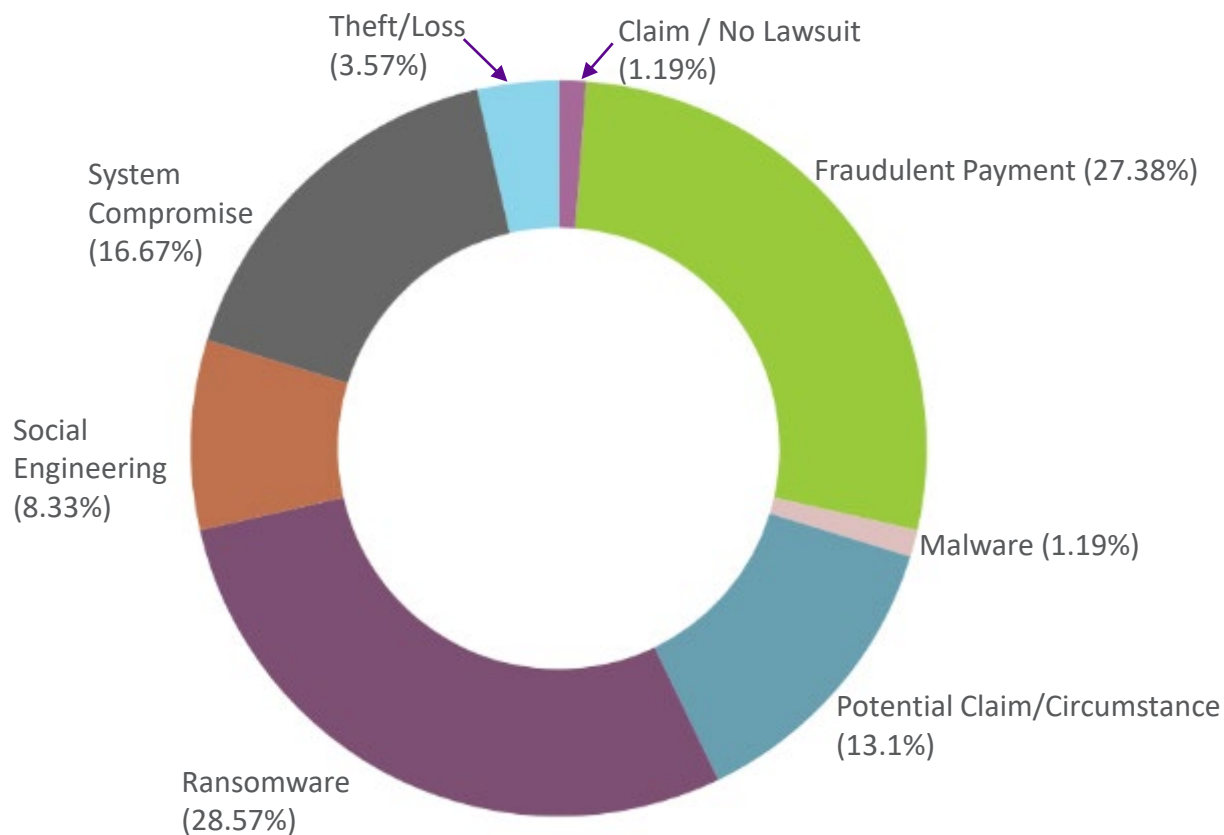
- Many still don't get it – importance of sound back-up practices
- Steeper hills and valleys in cyber insurance market than traditional insurance



Source: NAIC data, sourced from S&P Global Market Intelligence; Insurance Information Institute

# Edu/Public Entity Claims Experienced by RPS Clients

Count by Matter Type: Edu/Public Entity



# Cost of Not Having Cyber Insurance



Source: CFC Underwriting ©2023

Criteria: Based on Education Industry Code @ \$30M annual budget

Estimated Total Cyber Incident Costs	
\$2,710,500	
Compromised Records: 100,000	
Incident Investigation*	\$504,500
Crisis Management*	\$656,500
PCI*	\$25,000
Fines/Penalties*	\$274,500
Ransomware	\$300,000
Data Restoration	\$500,000
Business Interruption	\$450,000

\*In partnership with NetDiligence

Source: Chubb Cyber Index ©2023 Chubb Corporation

Criteria: Industry: Education | Industry Class: Pre-K-12

Annual Revenue: \$30M | Record Count: 100,000



PREVENTING INCIDENTS  
WEATHERING INCIDENTS  
PREPARING FOR THE FUTURE

# SPELL JIF Insurance Policy: Controls by Tier

To be included in Tier 1, districts must utilize the following:



Perimeter Firewall



AV &/or EDR



MFA For Remote Access



MFA For Privileged Access



Tested & Encrypted Backups



A Tested Incident Response Plan



A Vetting Process for 3<sup>rd</sup> Party Vendors

## Tier 1 Terms:

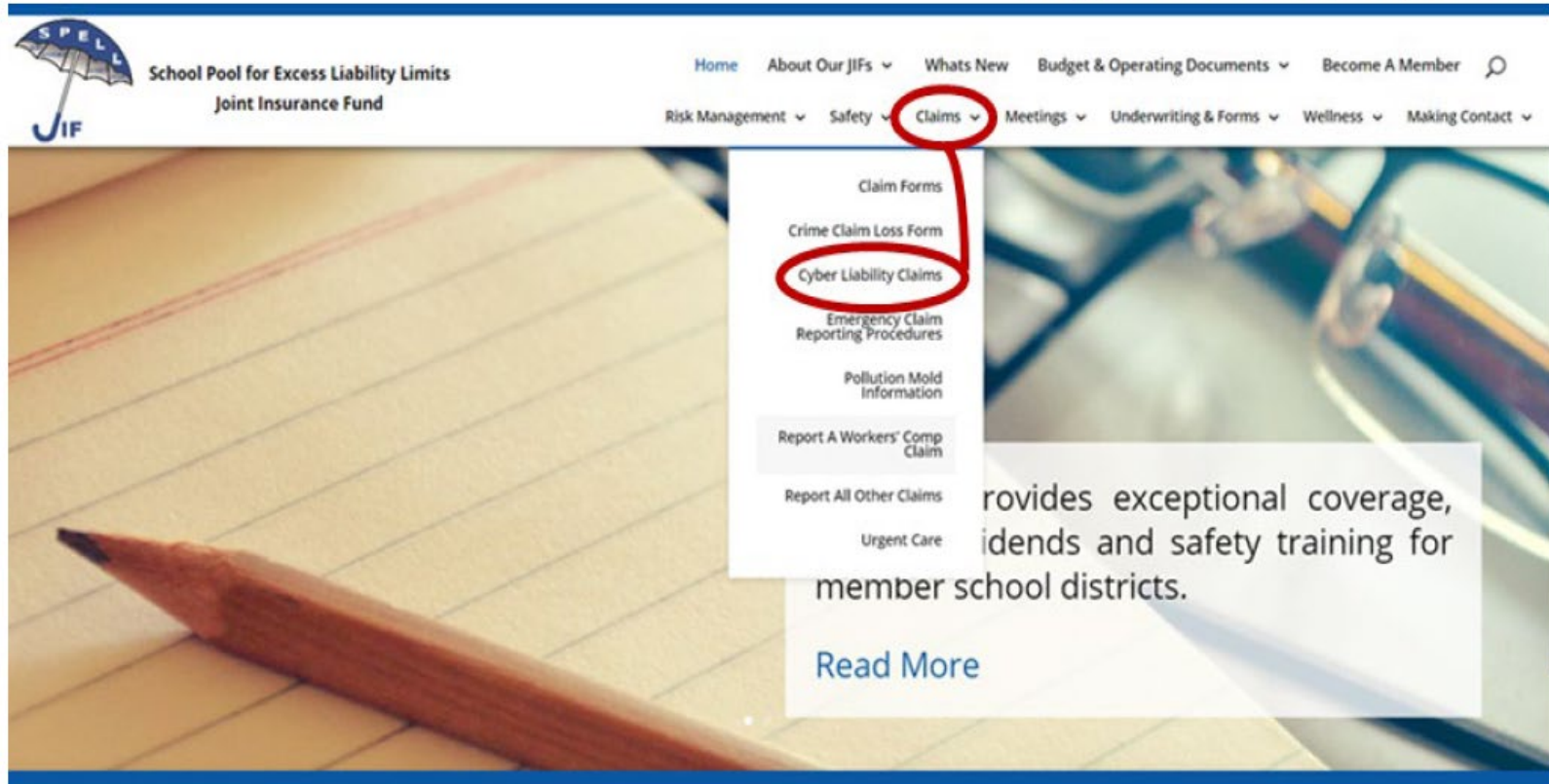
- Utilizes all required controls
- \$50,000 Retention
- 25% Co-Insurance

## Tier 2 Terms:

- Missing one or more of the required controls
- \$100,000 Retention
- 50% Co-Insurance

# Cyber Incident Reporting

Begin at [www.spelljif.com](http://www.spelljif.com)



The screenshot shows the SPELL JIF website. The header includes the SPELL JIF logo (an umbrella with 'SPELL' and 'JIF' text) and the text 'School Pool for Excess Liability Limits Joint Insurance Fund'. The navigation bar contains links: Home, About Our JIFs, Whats New, Budget & Operating Documents, Become A Member, Risk Management, Safety, Claims, Meetings, Underwriting & Forms, Wellness, and Making Contact. The 'Claims' link is circled in red, and a dropdown menu is open, listing various claim types. 'Cyber Liability Claims' is circled in red within this menu. Below the menu, a text box states: 'provides exceptional coverage, identifies and safety training for member school districts.' and a 'Read More' link is visible.

SPELL JIF School Pool for Excess Liability Limits Joint Insurance Fund

Home About Our JIFs Whats New Budget & Operating Documents Become A Member

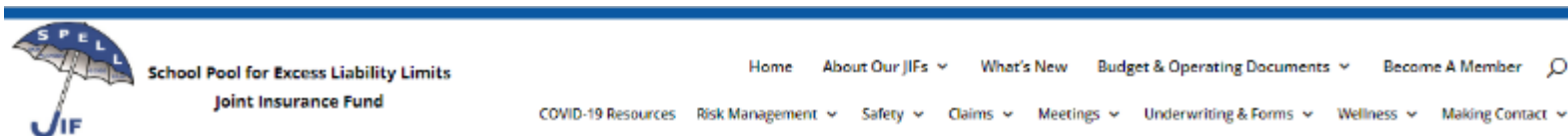
Risk Management Safety **Claims** Meetings Underwriting & Forms Wellness Making Contact

Claim Forms  
Crime Claim Loss Form  
**Cyber Liability Claims**  
Emergency Claim Reporting Procedures  
Pollution Mold Information  
Report A Workers' Comp Claim  
Report All Other Claims  
Urgent Care

provides exceptional coverage, identifies and safety training for member school districts.

[Read More](#)

# Cyber Incident Reporting



## Cyber Liability Claims

### Types of Losses to be Reported:

- Information Security and Privacy Law Violations
- Data Breaches
- Website Media Content

### Two Step Process to Report a Claim:

In the event of an actual or suspected breach incident, first you must submit your claim by clicking on this link: [SPELL JIF Cyber Incident Report Claim Form](#) and then call the Connell Foley Hotline

**SPELL JIF Policy # 1000600298211 for the Policy Period: 07/01/2022 to 06/30/2023**

### STEP 1: SUBMIT FORM

[CLICK HERE TO SUBMIT THE CYBER INCIDENT  
REPORT CLAIM FORM](#)

### STEP 2: CALL HOTLINE

Connell Foley 24/7 Data Breach Response Hotline

**PHONE: 973-840-2500**

[What is a Breach Coach?](#)

# Chronology of a Cyber Claim

What to Expect

## 1. Internal Preparation

Assemble internal team  
Assess situation  
Review IR plan



### Do NOT:

- Talk to media (yet)
- Hire unapproved vendors
- Compromise forensics footprint

## 2. Report on Website & Call Cyber Insurer

Have team assembled  
Share basic known facts:  
Timeline?  
What type of event?  
What type of information?  
Is network accessible?  
How many people affected?



### Don't be surprised:

- You may have to leave a voicemail – 24x7 response

## 3. Possible Next Steps

Engage breach counsel  
External forensics team  
Ransom negotiators (?)  
Public relations/media  
Customer/citizen notification  
Call center  
Credit/ID monitoring  
Regulatory/law enforcement



### Considerations:

- Clear conflicts
- OFAC check (if ransomware incident)

# School Districts Need Cyber Insurance



Pre-Aligned  
Resources



Operational  
Consistency



Fiscal  
Responsibility



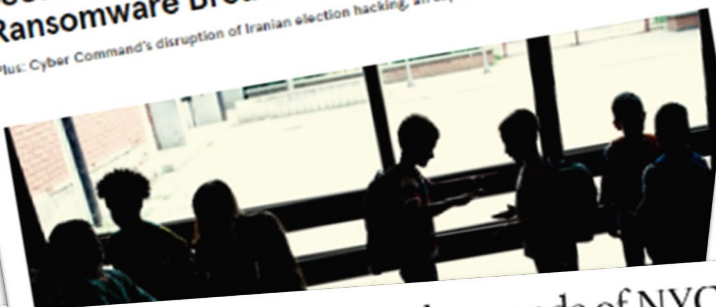
VOTE

Community  
Confidence

# The slow-down was short-lived

## Security News This Week: The Tragic Fallout From a School District's Ransomware Breach

Plus: Cyber Command's disruption of Iranian election hacking, an exposé on child sex trafficking on Metasploit



## Latest MOVEit exploit hits thousands of NYC school students and staff

News  
20 Jun 2022 • 3 min



## Criminal hackers targeting K-12 schools, U.S. government warns

The alert comes after the Los Angeles Unified School District, one of the largest school districts in the U.S., announced late Monday evening that it had been hit by ransomware.

## Ransomware attack closes schools in Nantucket

## Iowa's largest school district confirms ransomware attack, data theft

By Sergiu Gatlan

June 19, 2023 04:16 PM 0



## Brightly says SchoolDude data breach spilled 3 million user accounts

abuse reports,

ator information in an  
community.

## Takeaways

- Threats to schools will continue to occur and evolve
- Virtual Safety needs to be thought of on the same level as other critical dangers (active shooter, sexual abuse, etc.)
- Virtual Safety impacts cyber insurance availability, limits, premium, terms and conditions
- The application process is increasingly important
- The cyber insurance market will begin to harden again – already starting to see signs
- You will become the victim of an attack – will your district invest in prevention, recovery, both, or none?
- As a member of SPELL-JIF – you have much better resources than most of your peers in K-12 education – engage!



Thank You

**Steve Robinson**

Steven\_Robinson@rpsins.com

**Dan Waldman**

Daniel.Waldman@starrcompanies.com