October Is Cybersecurity Awareness Month

Establishing A Vibrant Culture Of Cyber Awareness

Jessica Blushi
Keenan & Associates

Tim Femister
Firestorm Global

October 3rd, 2024

FIRESTORM GLOBAL

Firestorm Global At A Glance

Public Sector Specialized

Mission-Driven Consultancy

Deep Cybersecurity Expertise

Business Risk Oriented

Data Driven Approach

Tim Femister
Principal

Experience

- Principal, Firestorm Global LLC
- CEO, NetXperts | #18 Fastest Growing in US
- VP, C1 | Led $900M business unit
- Sr Dir, C1 | Led Cyber business unit

Highlights

- Forbes | Rising Threat of Cyberattacks on K-12
- Forbes | Encryption Happens Last
- NBC | How To Prevent + Detect a Cyberattack
- Cisco | Are You SASE?

Public Education Is *The* Target

EDUCATION

One reason school cyberattacks are on the rise? Schools are easy targets for hackers

MARCH 11, 2024 · 12:00 PM ET

HEARD ON ALL THINGS CONSIDERED

By Kavitha Cardoza

PRIVACY & SECURITY

Schools Are a Top Target of Ransomware Attacks, and It's Getting Worse

By Lauraine Langreo — August 17, 2023 3 min read

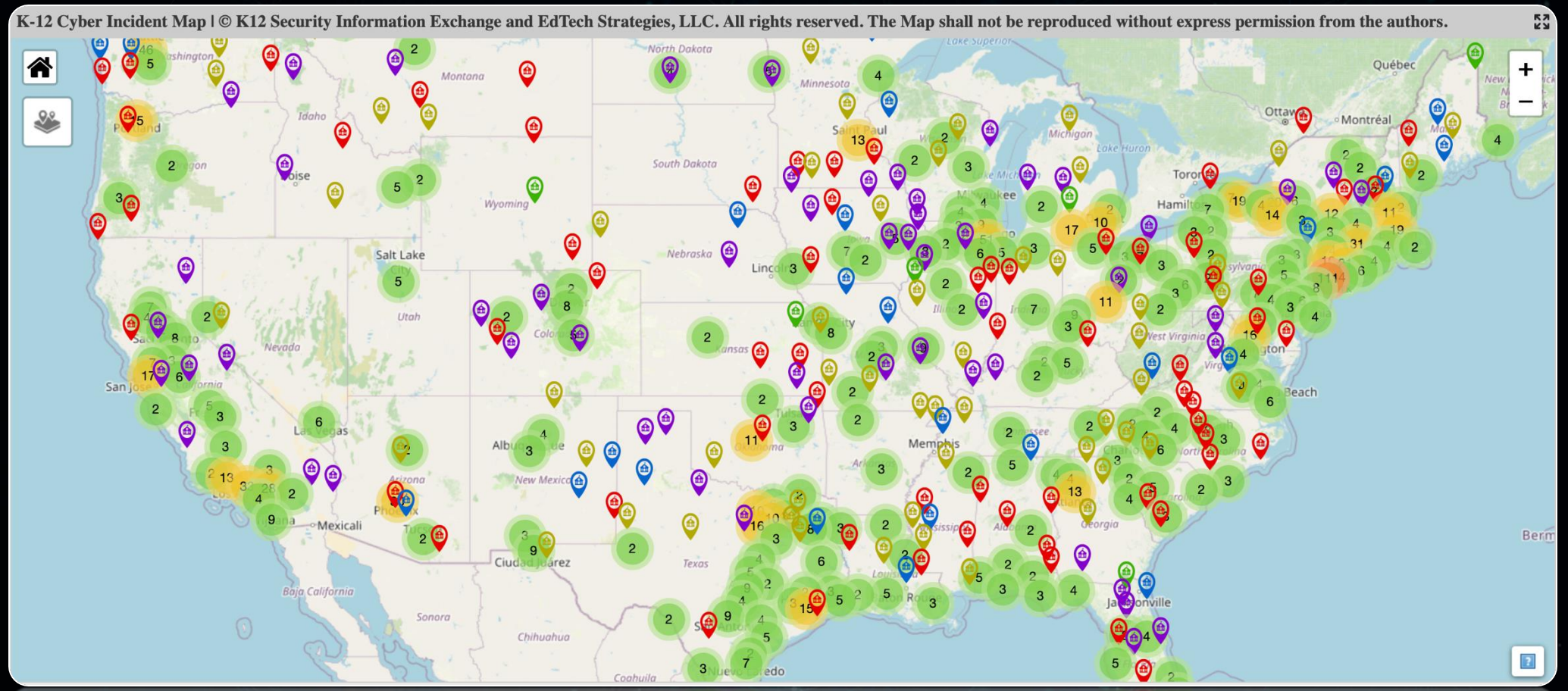
NEWS | SCHOOL (IN)SECURITY | THE BIG PICTURE

Schools Are Now the Leading Target for Cyber Gangs as Ransom Payments Encourage Attacks

The Education Sector Reports the Highest Rate Of Ransomware Attacks: Survey

FIRESTORM GLOBAL

Public Education Is *The* Target



FIRESTORM GLOBAL

Public Education Is *The* Target

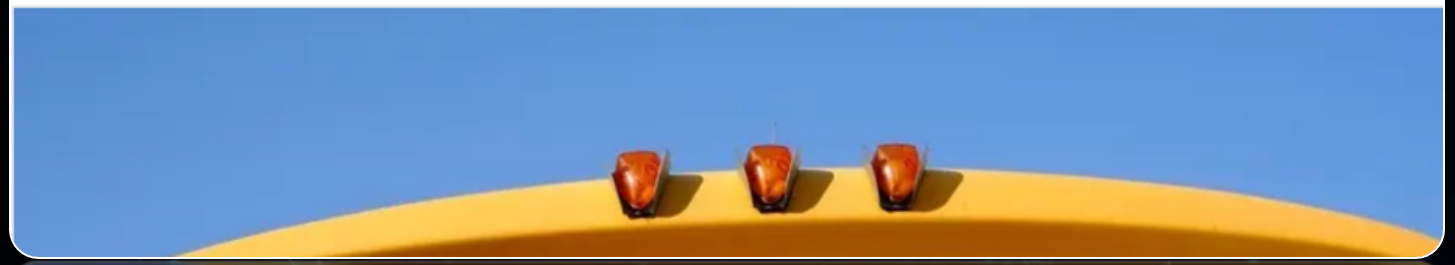
Schools

Hackers Steal $6M Meant For School Bus Contract

"It is unbelievably unethical that someone would steal this amount of money from taxpayers, from children," Mayor Justin Elicker said.

New Haven Independent, News Partner

Posted Thu, Aug 10, 2023 at 4:48 pm ET



- Malware not required for multi-million-dollar cyber attack
- Targeted social engineering campaign convinces district employee to change banking information

FIRESTORM GLOBAL

Public Education Is *The* Target

Hackers email stolen student data to parents of Nevada school district

By **Lawrence Abrams**

October 28, 2023 02:11 PM 0

- Threat actors are seeking to maximize extortion potential – however possible
- Certain cybercriminal syndicates are extorting parents applying added pressure to Districts

FIRESTORM GLOBAL

WE'RE ONLY HUMAN

Human Error Contributed To 68% Of Data Breaches Last Year

FIRESTORM GLOBAL

Cyber Awareness Training Methods

1. Live In-Person Trainings
2. Recorded Videos (Annual, On-Boarding)
3. Phishing Simulations
4. Bite-Sized Communication
5. Webinars
6. Emerging Topics
7. Digital Games and Quizzes
8. Posters, Wallpapers and Digital Collateral

FIRESTORM GLOBAL

Curating A Cyber Education Program

1 District Administration

District Administration	
Awareness Priority	**High**
Risk Potential	• District administrators are prime targets for cyber criminals • Access to financial information, student records and more • Voice of authority with ability to enact change
Communication Frequency	• Quarterly • Ongoing “Drip”
Training Methods	• Live In-Person • Bite-Sized • Emerging Topics • Phishing Simulations
Key Points	• Mandatory reliance on strong fundamentals • Must validate prior to making changes • Hands-on support from technical team for 2nd set of eyes • Reinforce education around finance-related changes

Curating A Cyber Education Program

1. District Administration
2. District Staff

FIRESTORM GLOBAL

District Staff	
Awareness Priority	**Elevated**
Risk Potential	• Ideal target to click on phishing links and download malware • May be less likely to report phishing attempts • May be susceptible to limited social engineering scams
Communication Frequency	• Annual • Ongoing “Drip”
Training Methods	• Webinar • Recorded Videos • Bite-Sized • Phishing Simulations
Key Points	• Focus on strong fundamentals • Embrace role as a human firewall • When in doubt, ask for help

Curating A Cyber Education Program

1. District Administration
2. District Staff
3. **Technical Staff**

FIRESTORM GLOBAL

Technical Staff	
Awareness Priority	**High**
Risk Potential	• Technical staff have wide access to tech systems including password and MFA reset • IT professionals are <u>not</u> inherently Security professionals
Communication Frequency	• Quarterly • Drip • Emerging Topics
Training Methods	• Live In-Person • Webinars • Emerging Topics
Key Points	• Key line of defense to protecting district stakeholders • Educate around latest threat methods • Develop expertise to support district staff in identifying threats

Curating A Cyber Education Program

1. District Administration
2. District Staff
3. Technical Staff
4. **Students**

FIRESTORM GLOBAL

Students	
Awareness Priority	**Increasing**
Risk Potential	• Students are campus technology users • Students face a variety of digital risk and threats while online
Communication Frequency	• Annual • Local Reinforcement
Training Methods	• Recorded Videos • Wallpapers and Posters
Key Points	• Online threats are similar in nature to ”real” in-person risk • Navigate the web carefully and maintain good digital hygiene • Never share information with strangers

Curating A Cyber Education Program

1. District Administration
2. District Staff
3. Technical Staff
4. Students
5. **Parents and Community**

FIRESTORM GLOBAL

Parents and Community	
Awareness Priority	**Opportunistic**
Risk Potential	• As threats evolve, parents and community members should understand how to support online safety
Communication Frequency	• Annual
Training Methods	• Local In-Person • Webinar
Key Points	• Understand what your children are accessing online • Establish good parental controls • Recognize online scams and phishing to keep your household safe

Rely On Strong Fundamentals To Stay Safe

- Check The Sender Address
- Don’t Click Links Or Attachments From Unknown Senders
- Evaluate Tone, Grammar And Syntax
- Place An Outbound Call To A Trusted Number
- Watch And Listen For Out Of Place Occurrences

Remember: When In Doubt, Ask For A Second Set of Eyes 👀

FIRESTORM GLOBAL

Reinforce Best Practices

1. Report, But Do Not Forward Phishing Messages
2. Never Send Money Without Verification (Call Trusted Numbers)
3. Use Strong, Unique Passwords (👍 Password Managers)
4. Keep Software Updated (Especially Security Updates 🚨)
5. Utilize Multifactor Authentication Wherever Possible

FIRESTORM GLOBAL

SAFER Cyber Awareness Resources

ww2.keenan.com/safer-cybersecurity-awareness

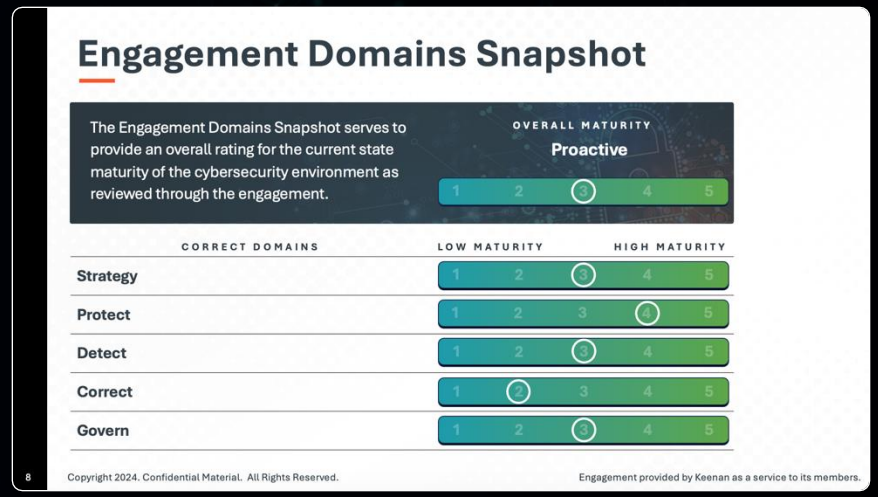
- Cyber Awareness resource kit available for download
  - Video
  - Posters
  - Wallpapers
  - Virtual Background
  - Presentation
- SAFER Cyber Program resources

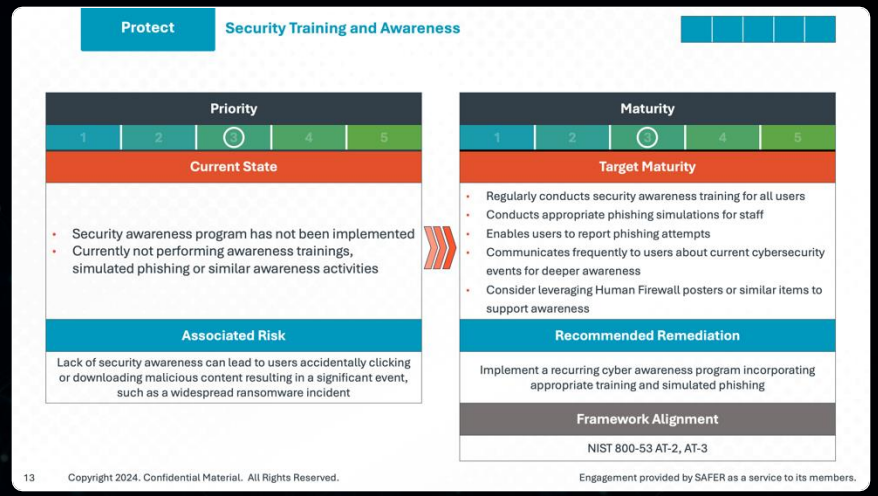
NO COST TO MEMBERS

INCLUDES EXTERNAL RISK ANALYSIS

SAFER Cyber Risk Assessment

- **Complimentary Cybersecurity Assessment**
- Structured risk assessment **aligned to NIST**
- Standard engagement covers 100+ topics
  - **2.5-hour engagement** followed by **1-hour readout**
  - ~40 slide engagement report with clear, concise recommendations
- Initiate engagement at www.firestormglobal.com/safer
- **Questions?** Email SAFER@firestormglobal.com





FIRESTORM GLOBAL

Q&A

Jessica Blushi
jblushi@keenan.com

Tim Femister
tim@firestormglobal.com

www.firestormglobal.com/SAFER

ww2.keenan.com/safer-cybersecurity-awareness

Thank You

FIRESTORM GLOBAL