



# SAFER Cyber Program Playbook

## 2025-26 SAFER Cyber Program



## 📌 Welcome

Welcome to the 2025-26 SAFER Cyber Playbook. This resource is designed to be your comprehensive guide for building and maintaining a robust cybersecurity program and better understanding the resources and requirements within the SAFER Cyber program.

As a member of SAFER JPA, you are part of a community spanning several hundred California K-12 and Community College organizations with a common mission of defending against an increasingly sophisticated threat landscape. The SAFER Cyber program has been developed and approved by the SAFER JPA Board of Directors to support you on this mission.

The education sector has become one of the most targeted industries for cyberattacks. Ransomware continues to be a devastating trend severely impacting organizations that are not prepared to respond to an advanced persistent threat. Advanced social engineering campaigns leverage a variety of emerging and proven tactics to redirect wire transfers and paychecks, access privileged accounts, and exfiltrate sensitive data. Artificial Intelligence and deepfakes are being incorporated by threat adversaries to creatively target victims and the marketplace for malicious AI tools is growing rapidly.

Yet despite these challenges, districts are not defenseless. This playbook represents the collective wisdom of engagements with fellow districts, lessons from real incidents, and industry accepted best practices and is designed to be an accessible resource for all members.

## 📌 Disclaimer

Please note that this playbook is not an insurance guide and does not constitute promises of coverage or insurance related matters. The purpose of the playbook is to provide members with information related to cyber risk management and the resources available to them.

## 📌 SAFER Cyber Program Mission

The SAFER Cyber Program exists to transform cybersecurity from an overwhelming challenge into a manageable journey. The program has been expanded again for 2025-26 and provides unique services such as:

- Proactive risk identification
- Practical implementation guidance tailored to education environments
- Expert support services at no additional cost to members
- Peer collaboration to share lessons learned across districts

Our goal is to provide the most advanced cyber risk management program in the pooled insurance industry and ultimately, help members to reduce their cyber risk and exposure.

Whether you're a small K-6 with limited IT resources, a large high school district, community college, regional occupation program, or somewhere in between, the SAFER Cyber program services have been intentionally crafted to offer support layers suitable for your organization size and type.

## ▾ SAFER Cyber Program Partners

The SAFER Cyber Program consists of several key organizations that support the cyber risk management process:

### **Keenan & Associates**

Keenan administers SAFER JPA and is the glue amongst all SAFER insurance and support programs.

Jessica Blushi leads emerging risk programs for Keenan including the SAFER Cyber program.

Jessica Blushi  
Vice President  
Keenan & Associates  
jblushi@keenand.com

### **Firestorm Global LLC**

Firestorm Global is the appointed cyber risk consultancy to SAFER JPA.

Members can request support via [SAFER@firestormglobal.com](mailto:SAFER@firestormglobal.com) or [www.firestormglobal.com/SAFER](http://www.firestormglobal.com/SAFER)

### **Cipriani & Werner**

Cipriani & Werner is the assigned breach counsel to SAFER JPA. In the event of a cyber incident, Cipriani & Werner cyber hotline is the members' first point of contact (prior to contacting or communicating with any external stakeholders).

24/7 Cyber Hotline  
1-833-63-CYBER  
cwcyber@c-wlaw.com

### **Incident Response & Forensics Partners**

Leading Incident Response firms, such as Charles River Associates, support the incident recovery process. Breach Counsel will recommend the appropriate firm based on the

specifics of each incident and coordinate engagement with response provider(s).

### **Berkeley Cyber Insurance**

Berkeley is the cyber insurance carrier for the SAFER Cyber program.

### **AIG**

AIG is the carrier for the Cyber Excess program.

Collectively, these organizations work together to support districts in assessing and improving their cybersecurity maturity as well as responding to and recovering from cyber incidents.

## **▮ Firestorm Global LLC Introduction**

Starting in the 2019-2020 policy year, SAFER's members saw a marked increase in cyber claim frequency. With the explosion in claim frequency, the SAFER Board took action to provide expert cybersecurity resources to their members. Firestorm Global was engaged starting in 2024 to aid members in managing their cybersecurity risks. Initially, members who fell short of industry best standards were targeted for support. Subsequently, services were made available to all program members.

Firestorm Global is a trusted cybersecurity services firm specialized in supporting public education institutions. Its services are recognized for providing enterprise best practices while customizing to the unique needs and intricacies of education.

The Firestorm Global team frequently presents to both business and technology leaders via local conferences as well as board and cabinet meetings on topics related to cyber resilience, artificial intelligence, deepfake and advanced social engineering education, and more. Their approach is different than other firms, which combines consulting and code to deliver intelligent services that identify risk that others who are purely software or services will miss.

## **▮ SAFER Cyber Program Overview**

The SAFER Cyber program provides services to members across three (3) integrated service pillars, each addressing unique member needs. The services pillars include:

- Cyber Hygiene Services
- Cyber Resilience Services
- Cyber Risk Management Services

### **Cyber Hygiene Services**

Cyber Hygiene Services are focused on identifying and notifying at-risk members. Firestorm Global has notified members of visible external risk and helped further assess, mitigate and resolve the concerns. Firestorm Global ingests external data on all

members with externally visible telemetry and monitors on an ongoing and best-effort basis. Firestorm Global also performs quantitative analysis on combined member self-reported and external telemetry to identify members with highest need.

Cyber Hygiene Services include:

- Critical risk alerts
- Continuous monitoring
- Program analysis

## Cyber Resilience Services

The Cyber Resilience Services pillar is focused on the people element of cybersecurity. For Cybersecurity Awareness Month in October, the SAFER Cyber program publishes a cyber awareness toolkit for all members to utilize, which includes posters, wallpapers, cyber awareness videos, and more.

New for 2025-26, Firestorm Global is providing employee cyber resilience training for key staff at member districts. These trainings are small group, live format over video designed to educate critical positions, such as cabinet, finance and human resources on identifying and defending against advanced social engineering threats. These trainings are designed to help combat the rise in successful social engineering threats that result in high impact financial fraud.

Additionally, a Monthly Cybersecurity Bytes article is published monthly to all members. Cybersecurity Bytes are intended to be a resource for drip training for end users. We encourage you to send these out to staff to keep cybersecurity as you further develop a culture of cybersecurity within your organization.

Cyber Resilience Services include:

- Security awareness support
- Employee cyber resilience
- Drip trainings

## Cyber Risk Management Services

The Cyber Risk Management Services pillar offers technical services to Information Technology teams to help support assessment, management, and remediation of cybersecurity risk.

We recommend starting with a SAFER Cyber Risk Assessment as an initial entry point, which consists of a \$0 mutual scope of work, 2 ½ hour workshop, external risk analysis and 1 ½ hour engagement readout with comprehensive reporting. Organizations that benefit most from the assessment typically have over 1,000 students with dedicated IT staff.

For members without dedicated IT staff, Firestorm Global provides business-level consultations, small group roundtables, and rapid assessments, which emphasize best-practice recommendations without the technical deep dives.

Large organizations may receive an extended workshop and deeper external analysis to ensure they receive guidance aligned to their size and overall risk potential.

Additional included services include written policies and procedures, incident response planning, virtual tabletop exercises, large vendor risk assessments, 1:1 expert consultations, large RFP reviews, ransomware risk assessments, web application scans, dark web exposure analysis, external attack surface assessments and more.

Cyber Risk Management Services include:

- Cyber risk assessments
- Policies and procedures
- Personalized support

## Engagement Process

Getting started with SAFER Cyber program services is straightforward and simple:

- Request Services
  - Visit [www.firestormglobal.com/SAFER](http://www.firestormglobal.com/SAFER) or email [SAFER@firestormglobal.com](mailto:SAFER@firestormglobal.com)
- Initial Consultation
  - Brief discussion to understand your needs and priorities
- \$0 Scope of Work
  - No-cost mutual scope of work created by SAFER JPA outlining services and timelines
- Service Delivery
  - Expert-led engagement with clear deliverables
- Ongoing Support
  - Continued access to expertise and resources

## Understanding the SAFER Cyber 6 Requirements

The SAFER Cyber 6 represents the minimum cybersecurity requirements established by the SAFER Board of Directors for all member districts. These controls are not arbitrary selections but rather industry-accepted standards that analysis of thousands of breaches has shown these controls to be fundamental to preventing, detecting, and recovering from cyber incidents.

Organizations experiencing breaches are commonly missing one or more of these basic elements. While implementing all six controls does not guarantee immunity from attacks, it dramatically reduces both the likelihood of successful compromise and the



potential impact of any incidents that do occur.

Each control addresses different attack vectors and stages of the cyber kill chain:

1. **Firewalls and Antivirus:** Block known threats at the perimeter and endpoint
2. **Endpoint Detection and Response (EDR):** Detect and respond to threats that evade perimeter defenses
3. **Vulnerability Scanning:** Identify and remediate weaknesses before exploitation across the internal and external network
4. **Multifactor Authentication (MFA):** Prevent credential compromise from enabling system or network access
5. **Security Awareness Training:** Reduce successful social engineering attempts
6. **Immutable Backups:** Ensure recovery from ransomware and similar threats when protection and detection controls fail to safeguard



## Next Generation Firewalls and Antivirus

Modern threats require modern defenses. Traditional stateful firewalls and signature-based antivirus cannot stop contemporary malware, which uses advanced techniques to evade detection.

SAFER members are required to implement credible Next Generation Firewall(s) (NGFW) at each network boundary. All network traffic to/from the internet should be firewall-protected.

Additionally, all capable endpoints operated by the organization should have credible Next Generation Antivirus (NGAV) implemented. This typically includes all PCs, Macs, Windows Servers, and capable Linux Servers.

Common Next Generation Firewall (NGFW) platforms include:

- Palo Alto Networks
- Fortinet FortiGate
- Cisco Secure Firewall
- Check Point Firewall

County Office of Education Options:

Many County Offices of Education (COEs) offer firewall-as-a-service programs that provide enterprise-grade protection at reduced costs through economies of scale. For example, Palo Alto Networks as a Service through your COE can meet all NGFW requirements while reducing management overhead.





Note: Advanced services, such as anti-malware, on next generation firewalls may drastically reduce throughput. When sizing your purchase, ask for the official sizing

guide that lists actual throughput with full services enabled.

Common Next Generation Antivirus (NGAV) solutions include:

- CrowdStrike Falcon
- SentinelOne

 **Note:** In the EDR section, it's advised to purchase CrowdStrike Falcon Complete or SentinelOne Vigilance to support managed endpoint detection and response (EDR).

 **Important:** Make sure to deploy NGAV on all available servers and endpoints. Linux and Mac devices are a common gap and savvy threat actors know to look for unprotected infrastructure.

## Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) represents an evolution beyond antivirus, providing visibility and response capabilities that assume some threats will evade prevention.

SAFER members are required to implement leading Endpoint Detection and Response (EDR) to all applicable devices (typically PCs, Macs, Windows Servers and Linux Servers). Endpoint Detection and Response (EDR) solutions include:

- CrowdStrike Falcon Complete
- SentinelOne Vigilance

It is strongly recommended to invest in a credible and market-leading Endpoint Detection and Response (EDR) solution. While many traditional antivirus vendors have rebranded their portfolio to claim they are a true EDR, many fall short of market expectations. While education environments are not Fortune 500 enterprises, we can gain insight from the standardization that large enterprises have made regarding their endpoint protection investments.

## Vulnerability Scanning

Living Off The Land (LOTL) is an increasingly popular tactic used by cyber attackers where they exploit existing legitimate tools and features within a target's environment to maintain persistent access. To counter such threats, vulnerability scanning serves as an essential technique for detecting security weaknesses that could affect both internal and external systems.

SAFER members are required to scan frequently (monthly or better) for vulnerabilities (internal and external). Many organizations aligned to best practices will scan on a daily



or weekly basis and hold weekly meetings to review active vulnerabilities.

Common vulnerability scanning solutions include:

- Tenable Nessus Pro or Expert
- Rapid7 InsightVM
- OpenVAS

Due to both the size of infrastructure and budget constraints of public education, Tenable Nessus Pro is a common solution with a list price around \$4,390 (at the time of writing).

For external scanning, no-cost services are available to public education organizations:

- CISA Cyber Hygiene Services
- K-12 High Speed Network (HSN)



CISA Cyber Hygiene Services: <https://www.cisa.gov/cyber-hygiene-services>



K-12 HSN External Nessus Scanning: <https://www.k12hsn.org/network/network-tools>



**Important:** These services do not satisfy the requirement for internal network scanning, but are great services to leverage.



**Note:** If you are utilizing your County Office of Education (COE) as an ISP, consider inquiring about internal network scanning services. Some COE organizations offer this as a value-added service.



## Multifactor Authentication (MFA)

According to CISA, the use of MFA on accounts makes organizations 99% less likely to be attacked. It is commonly considered the single most effective modern security control available.

SAFER members are required to enforce Multifactor Authentication (MFA) on all critical applications capable of MFA, including email, as well as remote access environments.

Common Multifactor Authentication (MFA) solutions include:

- Microsoft Authenticator
- Google Authenticator
- Cisco Duo
- ClassLink

Multifactor Authentication (MFA) can be susceptible to compromise through phishing, push bombing, SIM swapping, and other techniques. The most secure form of MFA is FIDO-based physical tokens followed by app-based authentication with one-time passcodes or number matching. App-based push notifications without number matching, SMS, and voice are considered less secure MFA options.

Some education organizations struggle to implement MFA based on concerns from various stakeholders. While less ideal, vendors like ClassLink do provide additional secondary authentication measures such as a unique PIN.



**Recommendation:** If MFA is not in place today, start by securing key staff with privileged access, critical applications, and all remote access entry points as soon as possible. Then, continue with a deployment to all applicable users.



**Resource:** Importance of Multifactor Authentication is an available resource document to share with hesitant stakeholders in order to help justify and support the use of MFA across all member organizations.



**Pro Tip:** After MFA deployment, perform a one-time password reset requiring strong, unique passphrases (15+ characters). With MFA protection, these passwords won't need regular rotation unless compromised.



## Security Awareness Training


Even with an unlimited budget, the best security solutions cannot protect against users who willingly hand over credentials, sensitive information, or perform unwarranted changes. Social engineering is a leading contributor to the majority of successful data breaches and its effectiveness will continue to surge with the advancement of artificial intelligence and deepfake technology.

SAFER members are required to have all staff with network access complete annual security awareness training. Key staff who have the potential ability to affect catastrophic change are strongly encouraged to complete an additional level of cyber resilience training to support identification and containment of advanced social engineering threats.

Security awareness training is available to all members via:

- Keenan SafeSchools
- Keenan SafeColleges

Additionally, Cyber Resilience Training is available in small-group, live format training sessions for all members through Firestorm Global. Email [SAFER@firestormglobal.com](mailto:SAFER@firestormglobal.com) or visit [www.firestormglobal.com/SAFER](http://www.firestormglobal.com/SAFER) to request services.

 **Recommendation:** Cybersecurity Awareness Month is October of every year. The SAFER Cyber program has a Cyber Awareness Toolkit available to download for all members. Additionally, organizations like CISA have awareness resources available. Consider emphasizing cybersecurity awareness resources throughout the month.

## **Immutable Backups**


Backups are often considered the last line of defense, or the data of last resort, to ensure proper data recovery and avoid paying a ransom. Immutability and deletion resistance are key elements of a modern backup system that help prevent permanent data loss by blocking attempts to encrypt and delete backup data by ransomware operators.


SAFER members are required to implement an immutable and deletion-resistant backup environment, which should follow a 3-2-1 (at minimum) data protection architecture.


Common Immutable Backup solutions include:


- Rubrik Data Protection with Wasabi Cloud Object Storage
- Veeam Data Protection with Wasabi Cloud Object Storage

 **Important:** Always utilize off-domain accounts for accessing backup environments.

 **Important:** For Wasabi instances, ensure Object Lock is turned on to enable Write Once Read Many (WORM) functionality (immutability function).

 **Important:** When using data protection software on separate physical hardware, ensure physical appliances are hardened to ensure deletion resistance.

 **3-2-1 Architecture:** Data protection strategy that requires at least three (3) copies of data on two (2) different types of media with one (1) copy off-site. This is a classic rule that is now considered a minimum requirement. Modern backup strategies follow a 3-2-1-1-0 or other variations that include items such as air-gapped and error free backups. Additionally, best practice organizations may include physical media backups stored offsite, tape backups, and other methods to ensure the organization can withstand advanced persistent threats.

 **SaaS Backups:** Backing up SaaS data, such as Microsoft and Google, is becoming an increasing trend for data protection. Consider assessing where critical data resides and implement a plan to appropriately protect organizational data.

## Member Services

SAFER members have access to a variety of resources to support their information security journey. The below services encompass Cyber Hygiene, Resilience, and Risk Management Services that members can leverage.

Most members start with the SAFER Cyber Risk Assessment to develop a baseline for their current-state Information Security Program and align additional available member services to consider.

To request services, simply email [SAFER@firestormglobal.com](mailto:SAFER@firestormglobal.com) or visit [www.firestormglobal.com/SAFER](http://www.firestormglobal.com/SAFER).

Program Service	Description
<b>SAFER Cyber Risk Assessment</b>	Personalized report summarizing external findings, compliance gaps, benchmark comparisons, and prioritized remediation guidance.
<b>Written Policies &amp; Procedures Toolkit</b>	Library of editable policy templates tailored to public education institutions, covering the written information security policy, acceptable use agreement, data classification policy, vendor risk management policy and more.
<b>Incident Response Plan (IRP)</b>	Incident Response template detailing roles, responsibilities, and step-by-step actions for responding to security incidents.
<b>SAFER Cyber Playbook</b>	Complete guide for implementing SAFER Cyber 6 controls and recommended practices across member environments.
<b>Virtual Tabletop Exercises (vTTX)</b>	Utilized for incident response planning, scenario-based drills test and strengthen incident response capabilities. Delivered virtually.

Program Service	Description
<b>Large Vendor Risk Assessments</b>	Information security review of major third-party vendors to uncover potential supply-chain risk before contract award or renewal.
<b>vCISO Coaching Sessions</b>	One-on-one or small-group mentoring to guide strategy, policy, and program maturity efforts.
<b>Incident Readiness Reviews</b>	Review and provide guidance around an organization's existing or draft Incident Response Plan.
<b>Ransomware Risk Assessments</b>	Targeted assessments that measure ransomware exposure, control gaps, and recovery readiness.
<b>Large RFP Reviews</b>	Review large Request For Proposals (RFPs) for security inclusivity and concerns as well as strategies for vendor negotiation and budget maximization.
<b>External Attack Surface Assessment (EASA)</b>	Analysis of publicly facing IPs, domains, and services to identify potential exposures an adversary could exploit.
<b>Web Application Scans (WAS)</b>	Security scanning of web applications for potential vulnerabilities and misconfigurations.
<b>Dark Web Exposure Analysis (DWEA)</b>	Review exposure of stolen credentials or data tied to an organization's domain.
<b>Cyber Resilience Training</b>	Role-based training track for finance, HR, cabinet, and other high-impact positions on sophisticated phishing, AI deepfakes, and policy controls. Delivered live in small-group setting or video on demand.

Program Service	Description
<b>Personal Cyber Risk Profiles (Pilot)</b>	Pilot program delivering individualized risk reports that blend external scanning with self-reported data for up to 100 members.
<b>Ask the Expert</b>	On-demand support channel for follow-up questions and deeper guidance on cybersecurity topics.
<b>Cybersecurity Roundtables</b>	Small-group roundtables designed for members that may lack accessible IT resources to ask questions and learn about information security.

## Top Cybersecurity Risks In Public Education

### Targeted and Advanced Social Engineering

*Key staff members are targeted with advanced social engineering tactics to facilitate catastrophic change.*

High-value targets across Cabinet, Finance, HR, IT, and others face sophisticated spear-phishing and social engineering attacks designed to compromise critical systems or authorize fraudulent transactions. Attackers invest significant time researching these individuals through social media, public records, and organizational websites to craft convincing scenarios. Key indicators of vulnerability include limited advanced training for key staff on recognizing sophisticated attacks, and limited involvement in anti-social engineering processes such as regular simulations and tabletop exercises. These targeted attacks often succeed because they exploit trusted relationships and bypass traditional security awareness training that focuses on generic threats.

### Ransomware

*Widespread malware infection leading to data encryption, exfiltration, and backup elimination.*

Ransomware continues to devastate educational institutions through systematic encryption of critical data, destruction of backups, and data theft for extortion purposes. Attackers target schools and colleges knowing they often lack resources for robust cybersecurity programs and depend on their digital infrastructure. Susceptible



organizations tend to lack credible Endpoint Detection and Response (EDR) solutions that can detect and stop ransomware behavior, and basic or limited backup systems that are not immutable, deletion resistant, or stored offline.

## Data Exfiltration

*Data theft by threat adversaries exfiltrating through the corporate network, remote users, and/or cloud apps.*

Sensitive student and staff data is being systematically stolen through multiple vectors including compromised network endpoints, unsecured remote access, and misconfigured cloud storage. This data includes student records containing health information, disciplinary files, and parental data that can be sold on dark web markets or used for identity theft.

## 3rd Party Vendor Risk

*Vendors handling organizational data and/or with privileged access experience a cyber incident impacting the district.*

Educational technology vendors, managed service providers, and other third parties with access to district systems represent a significant and often overlooked attack vector. When these vendors are compromised, attackers gain trusted access to numerous organizations simultaneously making them an attractive target. A strong vendor risk assessment process and methodology as well as internal controls limiting external vendor access and rights provides a strong foundation to weather supply chain problems.

## General Social Engineering

*Creative social engineering schemes, such as phishing, text and voice messages targeting general user population.*

Threat actors cast wide nets using increasingly sophisticated or clever phishing emails, SMS messages (smishing), and voice calls (vishing) to compromise accounts or capture sensitive information. These campaigns exploit current events, seasonal activities like enrollment periods, and emotional triggers. Developing a culture of cyber awareness where security is seen as everyone's responsibility and frequent employee communication about current threats and safe practices are recommended to properly prepare staff and stakeholders.

## AI Risk

*Improper use of AI or utilizing AI outputs as accurate recommendations or source of truth data.*

Staff and students are rapidly adopting AI tools without understanding their limitations, privacy implications, or potential for generating harmful or inaccurate content. In some cases, these platforms are provided to users by the organization without appropriate training. This could include uploading sensitive data to public AI platforms, accepting AI hallucinations as facts, and using AI-generated content without verification. All organizations should articulate policy around AI use that addresses data classification, acceptable use cases, and approval processes as well as provide appropriate training on proper use and limitations.

## **Digital Safety**

*Student safety related concerns including self-harm and cyber bullying occurrences.*

Online platforms and digital communications channels have become venues for cyberbullying, self-harm content sharing, and predatory behavior that directly threatens student wellbeing. These incidents often occur on platforms and devices outside district control but impact the educational environment. Organizations should provide frequent training and communication to all network users as well as evaluate self-harm monitoring solutions that identify at-risk students and users.

## **Living Off The Land**

*Threat actors dwelling within the corporate network carry out significant adversarial impact.*

Sophisticated attackers establish persistent presence within organizational networks, using legitimate administrative tools and stolen credentials to avoid detection while conducting reconnaissance and preparing for major attacks. They may remain undetected for months, learning systems, and identifying valuable data. Key indicators include limited patching capabilities and enforcement that leave known vulnerabilities exposed for exploitation, and limited ability to identify and remediate vulnerabilities through regular scanning and assessment.

## **Account Takeover**

*Accessing internal resources and applications through compromised accounts obtained via stolen credentials.*

Compromised user credentials obtained through phishing, credential stuffing, or password reuse enable unauthorized access to email, financial applications, and

administrative platforms. These takeovers facilitate further attacks, data theft, and business email compromise schemes. The primary indicator is limited use of Multi-Factor Authentication (MFA) on critical applications, leaving systems protected only by passwords that are often weak, reused, or compromised. Without MFA as a second line of defense, a single compromised password often grants full system access.

## 📌 **Current Warnings & Concerns In Public Education**

### **Vape Sensors: Exploit at Defcon**

Security researchers at Defcon demonstrated vulnerabilities in school bathroom vape detection systems. These sensors, designed to detect vaping and alert administrators, were shown to be susceptible to manipulation, including potential use as covert audio recording devices.

Districts should verify their vape detection systems are from reputable vendors with regular security updates and ensure proper network segmentation to isolate these IoT devices from critical systems.

### **Staff Social Engineering: Sensitive Information**

Threat actors are increasingly targeting staff with sophisticated social engineering attacks, particularly around banking information and password reset requests. Common tactics include fake IT support calls requesting password changes, fraudulent emails appearing to be from financial institutions, and phishing attempts disguised as legitimate district communications. Especially look out for Google Forms emailed directly to staff requesting personal information including staff ID, banking, passwords, and more.

Staff should be trained to independently verify all requests through official channels before providing any sensitive information.

### **Advanced Social Engineering: Wire Fraud**

Educational institutions are experiencing targeted wire fraud attempts, often coinciding with large purchases or projects. Attackers research RFP awards, impersonate vendors or administrators, and request payment redirections to fraudulent accounts.

Implement strict verification protocols for all wire transfers, including callback procedures using known phone numbers and multi-person authorization for financial transactions exceeding set thresholds.

### **AI Questionable Advice: Student Self-Harm, Narcotics, Health**

Students are accessing AI chatbots that may provide harmful advice regarding self-harm, substance use, or medical conditions when prompted. While many AI systems have safeguards, determined users can circumvent these protections.

Districts should implement AI content filtering, provide digital wellness education, and ensure counseling resources are readily available. Districts should also adopt AI policies and standards to define acceptable use and allowed models.

### **AI Source of Truth: Staff Utilizing Hallucination Outputs**

Educational staff are increasingly relying on AI tools for curriculum development, administrative tasks, and decision-making and may not understand the concept of AI hallucinations.

This can lead to misinformation in policy interpretations, flawed data analysis, and cited email correspondence. Establish clear guidelines and training for AI use including a source of truth disclaimer.

### **AI Wearables: Audio and Video Recording without Permission**

Smart glasses, AI pins, and other wearable devices with recording capabilities pose significant privacy concerns in educational settings. These devices can capture audio and video without obvious indicators or can be modified to eliminate manufacturer protections.

Update acceptable use policies to address AI wearables, establish clear zones where recording devices are prohibited, and implement detection protocols for unauthorized recording devices.

### **Microsoft Teams: Threat Actors Messaging via Teams**

Cybercriminals are exploiting Microsoft Teams' external communication features to send malicious messages directly to staff and students. These messages often contain phishing links, malware, or social engineering attempts that appear legitimate because they come through an official platform.

Configure Teams to restrict external communications, implement strict guest access policies, and train users to recognize and report suspicious messages even within trusted platforms.

### **Remote Access VPN: Credential Compromise Utilized On VPN**

Compromised VPN credentials are being actively exploited to gain unauthorized access to district networks. Weak passwords, credential reuse, and lack of multi-factor authentication make educational VPNs attractive targets.

Immediately implement MFA for all remote access, conduct regular audits of VPN access logs, enforce strong password policies, and limit VPN population to bare minimum.

## Deepfakes: Student Creating Deepfake Clones Imitating Staff

Students are using increasingly accessible deepfake technology to create audio and video impersonations of teachers and administrators. These can be used for harassment, spreading misinformation, or undermining authority.

Develop clear policies regarding deepfake creation and distribution, implement digital citizenship curricula addressing synthetic media, and establish policy to validate content authenticity before applying punitive action.

## Grok Spicy and other AI Tools: Inappropriate Image Generation

AI platforms, such as Grok, have released special modes (e.g. Grok Spicy) that will create inappropriate or harmful images. These may include violent content, inappropriate depictions of classmates or staff, or other policy-violating material.

Monitor and restrict AI platforms that allow users to generate inappropriate content. Set policy to clearly define acceptable use of image and video generation technology.

# ▮ Current Warnings & Concerns In Public Education

## Help Desk Hardening

Traditional password reset processes that rely on personal information (birthdate, mother's maiden name, staff ID) are no longer secure. Widespread data breaches have made this information easily accessible to attackers, creating a critical vulnerability in help desk operations. Additionally, voice recognition is being defeated through the use of voice clones.

Cyberattacks making global headlines commonly originate through a help desk associate performing password and MFA reset. This technique has proven highly successful against very large enterprises as well as public education institutions.



Recommended approach:

- **In-Person Verification:** Require physical verification for password or MFA reset. Assigning a Security Site Liaison is a great way to direct employees to a familiar face for quick verification. In this model, the help desk associate contacts the assigned liaison (such as a school secretary) to confirm identity.
- **One-Time Passcodes (OTP):** If physical verification is not possible, send one-time passcodes to the personal email and phone of the requesting individual to support verification.
- **Manager Verification:** If something feels even slightly off (hoarse voice, increased static, audio blips, etc), require help desk associates to seek supervisor support and contact the manager of the requesting individual to verify the request.

## Critical Staff Awareness

Targeted social engineering events are increasing in size, scope, and frequency, especially against key staff with access to sensitive data, financial accounts, or privileged access. Public education organizations are at a distinct disadvantage due to the amount of publicly available information, board documents, online employee directories and more.

Developing a sophisticated social engineering threat based on real contracts with current vendors is simple to accomplish and made easier through AI platforms.

Ensure critical staff have the appropriate training to identify and contain advanced social engineering attempts. Remind staff members that email is only one available vector. Modern threat actors utilize a combination of options like Microsoft Teams, text messages, phone calls, and emails with fake documents, voicemails, and more to develop their attack through a layered approach.

Always make an outbound call to a trusted number before making changes, frequently review organizational policies and procedures, and enforce approval thresholds to limit changes made by singular individuals.

As referenced in the Member Services section, Cyber Resilience Training is available for key staff at all member organizations.

## Incident Response Planning

It is strongly recommended for all members to have a Cybersecurity Incident Response Plan developed, approved, and printed for all executives.

SAFER members have access to an Incident Response Plan template from Firestorm Global as well as an Incident Readiness Review service.

In lieu of a documented plan, print out the SAFER Cyber Claims document, which advises member to contact the Breach Counsel 24/7 Hotline (833-63-CYBER or [cwcyber@c-wlaw.com](mailto:cwcyber@c-wlaw.com)). This is the first point of contact before communicating with any external stakeholders or third parties.

## Technology Purchases

When purchasing new technology, allocate dedicated funding for cybersecurity measures as part of the initial investment rather than treating it as an afterthought. Some educational institutions make the critical mistake of deploying new systems without budgeting for security, then find themselves scrambling for funds to address security gaps after implementation.

Ensure RFPs state appropriate security requirements as included elements, both as part of the solution itself as well as add-on security measures. For example, if purchasing a



new network, ensure security requirements are integrated into the product selection and implementation requirements. This could include mandating certain security features as required elements, such as designing the network for appropriate segmentation with ACL enforcement to limit inter-VLAN communication. Additionally, evaluate add-on security elements to improve security. In the example of a new network, this could include a Network Access Control solution to enforce 802.1X authentication, device profiling, contractor access, and more.



Before releasing an RFP or conducting a technology purchase, ask these questions:

- Have we evaluated available security features and additional licensing, product, or implementation requirements?
- Will this purchase increase our cybersecurity risk?
- What are the best practice security solutions that frequently accompany this purchase?

## Vendor Risk Management

Vendors and supply chain partners have become a constant source of risk for organizations. Any vendor entrusted with sensitive data, network access, system access, or stakeholder communication produces business risk that should be evaluated.

Educational institutions are strongly encouraged to establish a formal process for evaluating how vendors handle institutional data and access network resources before entering into contracts. Organizations will at times discover vendor security weaknesses only after an incident occurs, when sensitive data has already been exposed and remediation becomes significantly more complex and costly. Implementing a vendor evaluation process as part of standard procurement procedures helps identify these issues while there's still time to address them or select alternative vendors.

IT Security Questionnaires are recommended for all technology vendors, with responses reviewed by IT security staff prior to finalizing any agreements. These questionnaires reveal important information about data handling practices and overall cyber hygiene.

Special attention should be given to vendors requesting persistent remote access for support or maintenance purposes. Some vendors expect network access without implementing appropriate security controls such as multi-factor authentication, activity logging, or encrypted connections. Others may still rely on shared credentials across multiple clients or inadequate password management practices.

## Common Technical Gaps

The following gaps are commonly seen in public education and organizations are strongly advised to take appropriate action to mitigate their risk:

## Domain Controller Hardening

- Kerberoasting is a top technique cited in ransomware negotiations by threat actors
- Mandate strong passwords, especially for service accounts and enforce strong encryption
- Learn more: <https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/kerberoasting/>

## Active Directory Monitoring

- Threat actors will attempt to create a new admin account within Active Directory, however traditional AD will not alert to new account creation
- Implement counter measures such as Netwrix (free version available) or custom PowerShell script

## Network Segmentation

- Most public education networks have some existing level of segmentation, however it's important to ensure separate SSIDs do not converge to a single VLAN (e.g. Staff SSID and Student SSID)
- Verify IoT devices including HVAC and building control are properly isolated
- Ensure ACLs are properly applied to limit inter-VLAN communication

## Wired Network Access

- Malicious pass-through and remote access devices are widely available to potential threat actors who may attempt to physically connect to a wired port
- Consider enforcing 802.1X authentication at the wired port level or apply sticky MAC as a port security feature
- Ensure wired VLAN assignment is appropriate for the port location and potential use

## Threat Detection

- It's not uncommon for organizations to emphasize threat protection investments over threat detection in hope of preventing threats at point of entry. However, it's vital to carry an Assume Breach mentality and implement threat detection capabilities that will identify nefarious activity that has bypassed existing protection controls.
- Consider Managed Detection and Response or Managed Endpoint Detection and Response to develop internal detection capabilities

## Log Collection

- Threat actors often spend weeks or months within a network before executing ransomware, leaving digital footprints that can be detected through proper log analysis
- Implement centralized log collection using SIEM solutions or free alternatives like Graylog, ensuring critical systems including firewalls, domain controllers, and authentication systems are included

- Establish baseline logging retention of at least 90 days to support incident response and forensic investigations
- Archive logs after 90 days to low-cost cold storage in the cloud

## Cloud Sharing Policies

- Unrestricted file sharing through cloud platforms creates significant data exposure risks, with threat actors increasingly targeting publicly accessible links and overly permissive sharing settings
- Limit the data types staff and students can share via Microsoft, Google and similar cloud platforms
- Apply data loss prevention (DLP) labels to limit sensitive information sharing

## Access Reviews

- Orphaned accounts and excessive permissions accumulate over time, providing threat actors with potential entry points that may go unnoticed during compromise
- Despite automation workflows to shut down accounts, most organizations have accounts and/or elevated privileges that should not exist
- Conduct quarterly reviews of administrative accounts, service accounts, and terminated employee access across all systems including cloud platforms

## IT Roadmap

- Organizations without strategic technology planning often implement reactive security measures that create gaps and inconsistencies threat actors can exploit
- Develop a 2-3 year roadmap that prioritizes security initiatives based on risk assessment findings and aligns with budget cycles

## Cabinet Cadence

- Regular executive briefings ensure cybersecurity remains a board-level priority and secures necessary resources before incidents occur
- Schedule quarterly updates to leadership covering threat landscape changes, security posture improvements, and required investments

## Risk Assessments

- Many organizations do not conduct regular risk assessments to assess their current posture, gaps, and weaknesses
- Perform annual comprehensive assessments covering technical vulnerabilities, policy gaps, and human factors including social engineering susceptibility
- Leverage the SAFER Cyber Risk Assessment (no-cost to members) to get started

## Network Passwords

- Default or weak passwords on network infrastructure remain a primary initial access vector, with automated tools constantly probing for common credentials
- Utilize solutions like TACACS+ to enforce centralized authentication

- Implement complex passwords on all network devices when logging in directly
- Change passwords on a scheduled basis and when staff departures occur
- Store infrastructure passwords in a secure vault solution with audit logging and enforce multi-factor authentication for access when possible

## Student Passwords

- Avoid storing student passwords in clear-text, especially in later grades
- Do not utilize a student-identifiable password structure
- Ensure mandatory password change happens by 3<sup>rd</sup> or 4<sup>th</sup> grade if passwords are known by staff in early grades

## Free and Low-Cost Services To Consider

### Security Operations Center as a Service

California Dept of Technology SOCaaS

<https://cdt.ca.gov/services/security-operations-center-as-a-service-socaas/>

\*Free SOCaaS, but must use Azure Sentinel for logging. Discounts may be available.

### Dark Web Monitoring

Have I Been Pwned with Domain Verification

<https://haveibeenpwned.com>

### External Scanning

CISA Cyber Hygiene Services

<https://www.cisa.gov/cyber-hygiene-services>

K-12 High Speed Network (HSN)

<https://www.k12hsn.org/network/network-tools>

### Open-Source SIEM

Wazuh

<https://wazuh.com>

### Decoy and Early Detection

Canary Tokens

<https://canarytokens.org/nest/>

## Mail, Web and DNS Configuration Analyzer

MX Toolbox

<https://mxtoolbox.com>

## Open-Source Intelligence (OSINT)

Shodan

<https://www.shodan.io>

DeepFind OSINT Tools

<https://www.deepfind.me>

SSL Checker

<https://www.ssl.org>

Talos IP Reputation

[https://www.talosintelligence.com/reputation\\_center](https://www.talosintelligence.com/reputation_center)

DNS Dumpster

<https://dnsdumpster.com>

OSINT Framework

<https://osintframework.com>

## Ransomware Victims and Intelligence

Ransomware.live

<https://www.ransomware.live>

Threat Intelligence Feeds

Cisco Talos

<https://www.talosintelligence.com>

Palo Alto Networks Unit 42

<https://unit42.paloaltonetworks.com>

CrowdStrike

<https://www.crowdstrike.com/en-us/cybersecurity-101/>

## Government Guidance

CISA Stop Ransomware

<https://www.cisa.gov/stopransomware/ransomware-guide>

CISA K-12 Cybersecurity

<https://www.cisa.gov/K12Cybersecurity>

## Dark Web Browsing

Tails Portable Operating System

<https://tails.net>

## What Are Other Members Saying?

SAFER members have found value in leveraging the SAFER Cyber program services. The Keenan and Firestorm Global team can provide named feedback upon request.

*"Partnering with Firestorm Global has been immensely valuable. Their deep expertise in K-12 cybersecurity goes well beyond the standard assessments and evaluations typically offered by others in the field."*

**- Chief Technology Officer, Southern California K-12 District**

*"I enjoyed working with Firestorm Global as they were thorough. They guided us through the review process, answered our questions, and helped us build clear road map to strengthen our security posture."*

**- Chief Technology Officer, Southern California Community College District**

*"Our experience working with Firestorm Global and the SAFER Cyber Risk Assessment has been excellent and truly focused on the realities of K-12... This work has been essential in helping us strengthen our security posture and protect our students and staff."*

**- Senior Director, IT, Northern California K-12 District**

*"Partnering with Firestorm Global for our SAFER Cyber Risk Assessment was a game-changer. Their team brought clarity and confidence to our GLBA compliance efforts, delivering a thorough evaluation aligned with NIST 800-171 standards... Firestorm's professionalism, responsiveness, and deep expertise made them an invaluable partner in strengthening our security posture."*

**- Chief Technology Officer, Southern California Community College District**

*"Working with Firestorm to evaluate our current security posture was a surprisingly pleasant process... The end report was very effective in convincing executive leaders of the school district to dedicate funds and time to better securing all our systems in the district and to become more security conscious."*

**- Chief Technology Officer, Northern California K-12 District**



*"Working with Firestorm Global was a good and worthwhile experience, they provided data on some vulnerabilities to our network, and concrete actions we could take to improve our overall security."*

**- Director of Technology, Central California Community College District**

## **Thank You**

Together, we can make cybersecurity a manageable effort across our public education institutions.

We encourage you to leverage this playbook to drive action by adopting the SAFER Cyber 6 controls, scheduling your no-cost SAFER Cyber Risk Assessment, utilizing the Cyber Awareness Toolkit, and partnering with all departments in your organization to drive sustainable security.

If something goes wrong, remember to engage Breach Counsel first via the 24/7 hotline at 1-833-63-CYBER or [cwcyber@c-wlaw.com](mailto:cwcyber@c-wlaw.com).

Members can request support anytime at [SAFER@firestormglobal.com](mailto:SAFER@firestormglobal.com) or [www.firestormglobal.com/SAFER](http://www.firestormglobal.com/SAFER).

Thank you for protecting your students, staff, and community while embracing a culture of cyber resilience.



**Jessica Blushi**  
Vice President  
Keenan & Associates



**Tim Femister**  
Managing Principal  
Firestorm Global

Questions? Visit [www.firestormglobal.com/SAFER](http://www.firestormglobal.com/SAFER) or email [SAFER@firestormglobal.com](mailto:SAFER@firestormglobal.com) to get support.

