



SAFER Cyber Resources

Developed In Partnership With: **FIRESTORM
GLOBAL**



**Jessica
Blushi**

Vice President
Keenan & Associates



**Tim
Femister**

Principal
Firestorm Global



Northern
California ReLIEF

SWACC
Statewide Association of Community Colleges



Southern
California
ReLIEF
Regional Liability
Excess Fund





**You Were Specially Invited To Attend,
Thank You For Joining.**

We Recognize The Challenge.

66% of Districts Do
Not Have a Full-Time
Cybersecurity
Position

Lack of Dedicated
Staff **#1** Cybersecurity
Challenge for K-12

47% of Districts Report
Lack of Cybersecurity
Strategy as Top
Concern

SAFER Cyber Program – ‘24-25

Continuous Cyber Risk Monitoring	Monitoring external risk, such as vulnerabilities, open ports, end of support software, and more
SAFER Cyber Risk Assessment	Complimentary risk assessment tailor-made for public education and aligned to NIST – No cost to members
Ongoing Webinar Series	Recurring cybersecurity webinar series to support member development and maturity
Cyber Awareness Month Resources	New resources for Cyber Awareness month in October (Coming Soon)
Updated Cyber Awareness Trainings	Updated cybersecurity trainings in SAFER member portal (Coming Soon)
Discounted Cybersecurity Services	Services include Tabletop Exercises, Leadership Awareness Workshops, Cyber Awareness Trainings, Threat Briefings and more

NO COST TO MEMBERS

SAFER Cyber Risk Assessment

INCLUDES EXTERNAL RISK ANALYSIS

- **Complimentary Cybersecurity Assessment**
- Structured risk assessment **aligned to NIST**
 - Leverages Protect, Detect and Correct framework
- Standard engagement covers 25 categories and 100+ Information Security 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

Engagement Domains Snapshot

The Engagement Domains Snapshot serves to provide an overall rating for the current state maturity of the cybersecurity environment as reviewed through the engagement.

OVERALL MATURITY

Proactive



	CORRECT DOMAINS	LOW MATURITY	HIGH MATURITY
Strategy	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
Protect	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
Detect	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
Correct	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
Govern	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5

Copyright 2024. Confidential Material. All Rights Reserved.

Engagement provided by Keenan as a service to its members.

Protect

Security Training and Awareness

Priority

1 2 3 4 5

Current State

- Security awareness program has not been implemented
- Currently not performing awareness trainings, simulated phishing or similar awareness activities

Associated Risk

Lack of security awareness can lead to users accidentally clicking or downloading malicious content resulting in a significant event, such as a widespread ransomware incident

Maturity

1 2 3 4 5

Target Maturity

- Regularly conducts security awareness training for all users
- Conducts appropriate phishing simulations for staff
- Enables users to report phishing attempts
- Communicates frequently to users about current cybersecurity events for deeper awareness
- Consider leveraging Human Firewall posters or similar items to support awareness

Recommended Remediation

Implement a recurring cyber awareness program incorporating appropriate training and simulated phishing

Framework Alignment

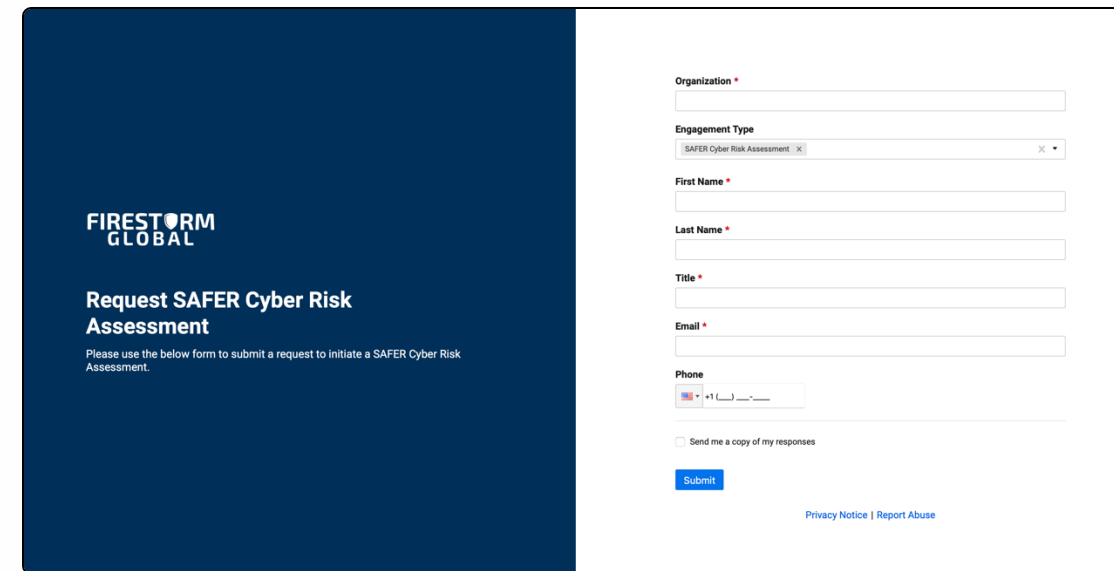
NIST 800-53 AT-2, AT-3

13 Copyright 2024. Confidential Material. All Rights Reserved.

Engagement provided by SAFER as a service to its members.

Getting Started Is Easy

- 1 Register at www.firestormglobal.com/SAFER
→ 24 to 48-Hour Response SLA
- 2 Complete **\$0 Scope of Work**
- 3 Conduct **15-minute Prep Call**
- 4 Schedule **2.5-Hour Workshop** (Remote)
→ Currently Scheduling 1-2 Weeks Out
- 5 Review **Engagement Report** (1-Hour)
→ Readout Available 1-2 Weeks Post-Workshop



The screenshot shows a web form for requesting a SAFER Cyber Risk Assessment. The left side of the form has a dark blue background with the Firestorm Global logo and the title 'Request SAFER Cyber Risk Assessment'. Below the title is a small instruction: 'Please use the below form to submit a request to initiate a SAFER Cyber Risk Assessment.' The right side of the form is white and contains several input fields: 'Organization *', 'Engagement Type' (a dropdown menu with 'SAFER Cyber Risk Assessment' selected), 'First Name *', 'Last Name *', 'Title *', 'Email *', and 'Phone' (with a country code dropdown set to '+1'). There is a 'Submit' button at the bottom of the form fields. At the very bottom of the form, there are links for 'Privacy Notice' and 'Report Abuse'.

Most Common Areas of Risk Amongst Members

57,000+ Alerts Generated (So Far)

- **End of Support Software**
 - Windows Server 2012
 - MySQL
 - Nginx
- **Vulnerabilities**
 - Most Common: CVE-2007-4723
- **Building Control / HVAC**
 - Ex: Tridium Niagara, WebCTRL
- **Database Exposure**
 - Ex: MS-SQL
- **High Risk Services**
 - RDP
 - FTP
 - Telnet
 - SMB
 - VNC

Q&A

Jessica Blushi

jblushi@keenan.com

Tim Femister

tim@firestormglobal.com



Safer Cyber Future **Together.**

Thank You!

Jessica Blushi

jblushi@keenandassociates.com

Tim Femister

tim@firestormglobal.com