

PAVING A PATH OF RESILIENCE



WELCOME

TO THE SOCAL RELIEF ANNUAL CONFERENCE



2025



PAVING A PATH OF RESILIENCE



Behind The Curtain: Exploring The Cyber Threat Landscape



Jessica
Blushi

Vice President
Keenan & Associates



Tim
Femister

Managing Principal
Firestorm Global

Speaker Introductions

Jessica Blushi, CCIC, ARM-P Vice President, Keenan & Associates

- 20+ Years Experience in California Public Sector
- Carnegie Mellon CCIC Program Graduate
- Lead Cyber Program for Keenan Education Clients
 - Program Design
 - Market Negotiations
 - Claims Support
 - Vendor Management
- Frequent Speaker on Cyber Insurance at Conferences and Association Meetings

Tim Femister Managing Principal, Firestorm Global

- Leads cybersecurity firm, Firestorm Global
 - Deep specialization in Public Education
 - Board-ready deliverables
- Former CEO of equity-backed IT services provider
- Prior L2 corporate executive for \$2B IT solutions provider
 - Started Cyber business unit
 - Led \$900M technology solutions portfolio
- Featured in Forbes, NBC, Lifetime, CRN and more
 - Forbes | [Rising Threat of Cyberattacks on K-12](#)

SAFER Cyber Program Overview



400+ Cyber Risk Profiles | 75 Elevated Risk Notices | 20+ Initiated Engagements | 15+ Critical Risk Alerts

Fact or Fiction?

- 1 OpenAI caught Iran using ChatGPT to improve hacking operations
- 2 AI writes more effective phishing emails than humans
- 3 Poor helpdesk hygiene results in \$100M cyber incident in Las Vegas
- 4 Record high \$40M ransomware payment took place in 2024
- 5 A gap in multifactor led to a cyberattack with a \$2.87B financial impact in 2024

Fact or Fiction?

1

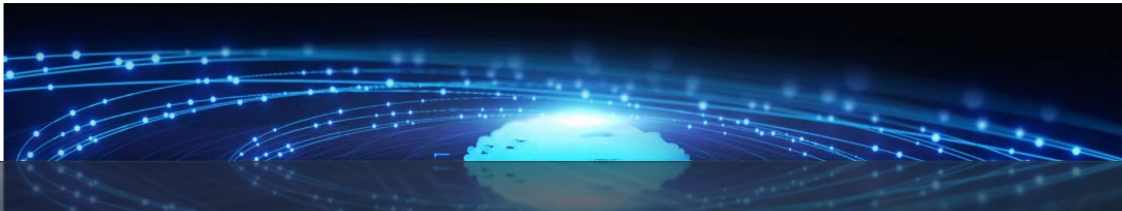
OpenAI caught Iran using ChatGPT to improve hacking operations



OpenAI confirms threat actors use ChatGPT to write malware

By Bill Toulas

October 12, 2024 10:09 AM 4



OpenAI blocks Iranian group's ChatGPT accounts for targeting US election

By Reuters

August 16, 2024 1:42 PM PDT · Updated 4 months ago



Activity	LLM ATT&CK Framework Category
Asking to list commonly used industrial routers in Jordan.	LLM-informed reconnaissance
Asking to list industrial protocols and ports that can connect to the Internet.	LLM-informed reconnaissance
Asking for the default password for a Tridium Niagara device.	LLM-informed reconnaissance
Asking for the default user and password of a Hirschmann RS Series Industrial Router.	LLM-informed reconnaissance
Asking for recently disclosed vulnerabilities in CrushFTP and the Cisco Integrated Management Controller as well as older vulnerabilities in the Asterisk Voice over IP software.	LLM-informed reconnaissance
Asking for lists of electricity companies, contractors and common PLCs in Jordan.	LLM-informed reconnaissance
Asking why a bash code snippet returns an error.	LLM enhanced scripting techniques
Asking to create a Modbus TCP/IP client.	LLM enhanced scripting techniques
Asking to scan a network for exploitable vulnerabilities.	LLM assisted vulnerability research
Asking to scan zip files for exploitable vulnerabilities.	LLM assisted vulnerability research
Asking for a process hollowing C source code example.	LLM assisted vulnerability research
Asking how to obfuscate vba script writing in excel.	LLM-enhanced anomaly detection evasion
Asking the model to obfuscate code (and providing the code).	LLM-enhanced anomaly detection evasion
Asking how to copy a SAM file.	LLM-assisted post compromise activity
Asking for an alternative application to mimikatz.	LLM-assisted post compromise activity
Asking how to use pwdump to export a password.	LLM-assisted post compromise activity
Asking how to access user passwords in MacOS.	LLM-assisted post compromise activity

Fact or Fiction?

2 AI writes more effective phishing emails than humans



2 AI writes more effective phishing emails than humans



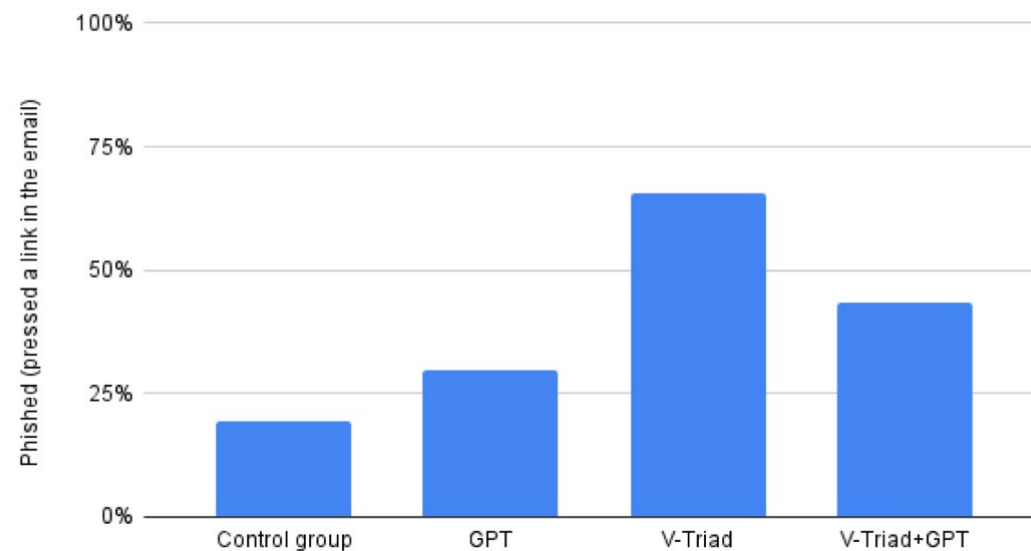
AI And Machine Learning

AI Will Increase the Quantity — and Quality — of Phishing Scams

by Fredrik Heiding, Bruce Schneier, and Arun Vishwanath

May 30, 2024

Phishing success (pressed a link in the email)



2 AI writes more effective phishing emails than humans



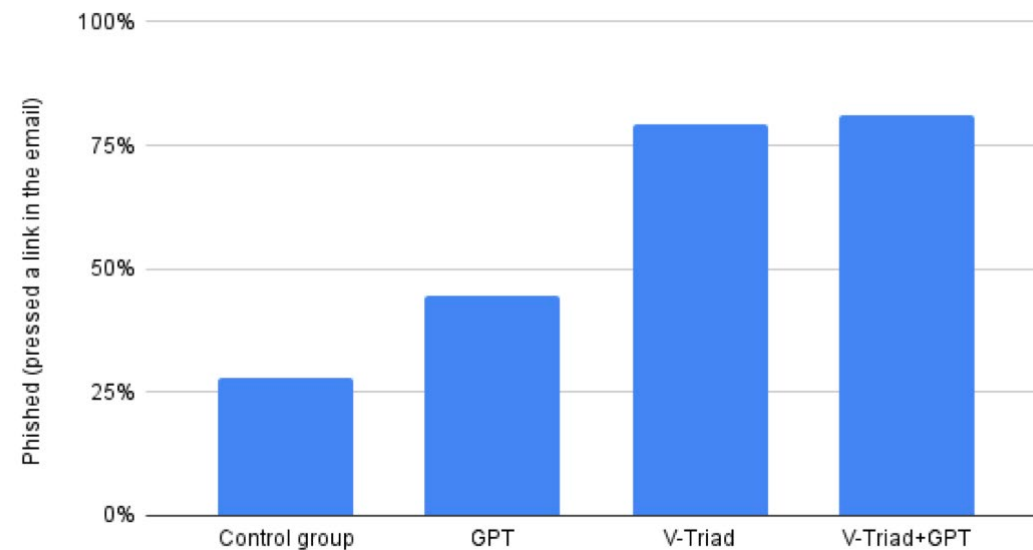
AI And Machine Learning

AI Will Increase the Quantity — and Quality — of Phishing Scams

by Fredrik Heiding, Bruce Schneier, and Arun Vishwanath

May 30, 2024

Phishing success - active participants



Fact or Fiction?

3

Poor helpdesk hygiene results in \$100M cyber incident in Las Vegas





3

Poor helpdesk hygiene results in \$100M cyber incident in Las Vegas

≡ Bloomberg

Subscribe



Technology | Cybersecurity

MGM Resorts Hackers Broke In After Tricking IT Service Desk

- Okta warned about hackers using similar techniques in August
- Group suspected of attack is well known for social engineering



NBC NEWS

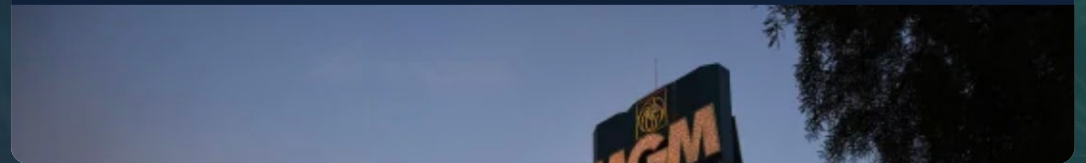
● WATCH LIVE



BUSINESS NEWS

Cyberattack cost MGM Resorts about \$100 million, Las Vegas company says

The company said it deliberately shut down a number of services "to mitigate risk to customer information" after the hack last month.



Fact or Fiction?

4 Record high \$40M ransomware payment took place in 2024



[Home](#) > [News](#) > [Security](#)

'Fortune 50' Company Made Record-Breaking \$75M Ransomware Payment

The payment was sent to a lesser known ransomware group called Dark Angels, according to cybersecurity vendor Zscaler, topping the \$40 million paid by CNA in 2021.

By [Michael Kan](#)

July 30, 2024



Fact or Fiction?

5

A gap in multifactor led to a cyberattack with a \$2.87B financial impact in 2024



Fact

5

A gap in multifactor led to a cyberattack with a \$2.87B financial impact in 2024

BECKER'S
HEALTH IT

Subscribe

Change Healthcare cyberattack costs to reach \$2.87B

Giles Bruce - Wednesday, October 16th, 2024



BUSINESS

Change Healthcare cyberattack was due to a lack of multifactor authentication, UnitedHealth CEO says

The background is a dark blue gradient with wavy, horizontal lines. In the center, there is a detailed illustration of a fish, possibly a bass, facing right. To the right of the fish, there is a large, curved fishing hook. The text "Can You Spot The Phish?" is centered over the fish and hook.

Can You Spot The Phish?

1

Security alert for your linked Google account



Google <NoReply@cloud-service-care.com>

Tuesday, November 26, 2024 at 2:17 PM

To: Tim Femister



Your password changed

You received this message because tim@firestormglobal.com is listed as the recovery email for your Google account. If this is not your Google Account, [click here to disconnect](#) from that account and stop receiving emails.

Hi Tim,
The password for your Google Account was recently changed.

Don't recognize this activity?

Click [here](#) for more information on how to recover your account.

Best,
The Google Accounts team

This email can't receive replies. For more information, visit the [Google Accounts Help Center](#).

You received this mandatory email service announcement to update you about important changes to your Google product or account.

© 2020 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

2

Item shared with you: "zzsha-217-45-99.zip"



Tim Femister (via Google Drive) <tfemister@gmail.com>

Today at 9:29 PM

To: Tim Femister

Tim Femister shared an item



Tim Femister (tfemister@gmail.com) has shared the following item:

Hi Tim,

Please download the attached file.

Thank you.

 zzsha-217-45-99.zip



This email grants access to this item without logging in. Only forward it to people you trust.

Open

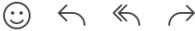
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

You have received this email because tfemister@gmail.com shared a file or folder located in Google Drive with you.

Google™

VS

Security alert for your linked Google account



Google <NoReply@cloud-service-care.com>

Tuesday, November 26, 2024 at 2:17 PM

To: Tim Femister



Your password changed

You received this message because tim@firestormglobal.com is listed as the recovery email for your Google account. If this is not your Google Account, [click here to disconnect](#) from that account and stop receiving emails.

Hi Tim,
The password for your Google Account was recently changed.

Don't recognize this activity?
Click [here](#) for more information on how to recover your account.

Best,
The Google Accounts team

This email can't receive replies. For more information, visit the [Google Accounts Help Center](#).

You received this mandatory email service announcement to update you about important changes to your Google product or account.

© 2020 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

VS

Item shared with you: "zzsha-217-45-99.zip"



Tim Femister (via Google Drive) <tfemister@gmail.com>

Today at 9:29 PM

To: Tim Femister

Tim Femister shared an item



Tim Femister (tfemister@gmail.com) has shared the following item:

Hi Tim,

Please download the attached file.

Thank you.

zzsha-217-45-99.zip



This email grants access to this item without logging in. Only forward it to people you trust.

Open

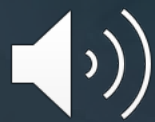
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

You have received this email because tfemister@gmail.com shared a file or folder located in Google Drive with you.



The background of the slide features a dark, teal-toned image. It shows two faces side-by-side, separated by a thin vertical white line. The face on the left is a human woman with light skin and brown eyes, looking directly at the camera. The face on the right is an AI-generated image of a woman with similar features but a slightly different texture and expression. The overall mood is mysterious and technological.

Can You Spot The Generative AI?



1



vs



2



1



vs

2





DARK WEB TOUR

WITH FIRESTORM GLOBAL

NOT FOR PUBLIC DISTRIBUTION

Common Themes Amongst Districts

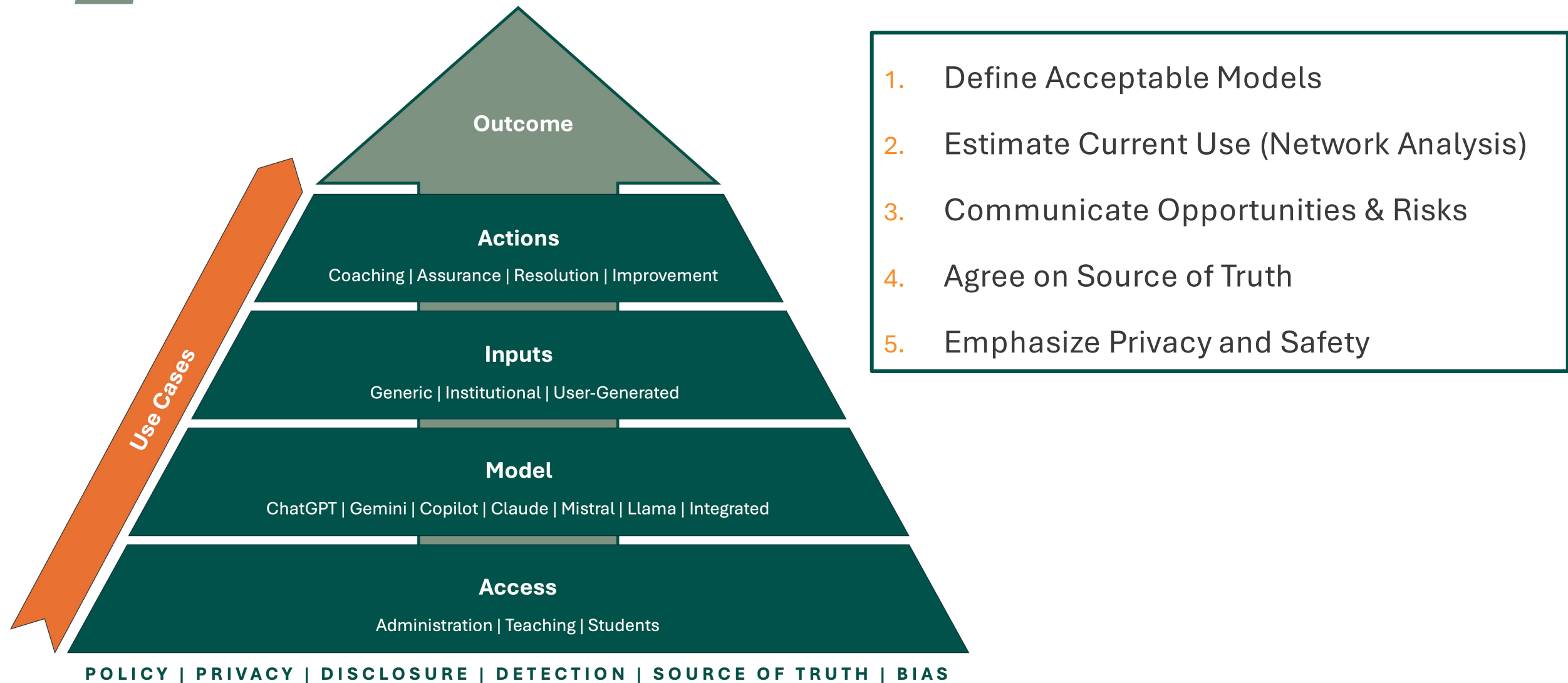
1. Over reliance on **Protection** controls; Under reliance on **Detection** and **Response**
2. Few Districts have implemented an **Incident Response Plan**
3. Lack of awareness training for **high-impact district positions** (e.g. Finance, HR)
4. Limited formality in **help desk policies** governing password and MFA reset
5. **Backup** and **endpoint** best practices are hit and miss
6. Gaps are common in **multifactor authentication**, if implemented at all
7. Scanning for **vulnerabilities** is conducted few and far between, or more often not performed at all

AI TOUR

WITH FIRESTORM GLOBAL

NOT FOR PUBLIC DISTRIBUTION

AI Considerations for Public Education



Executive Considerations For Reducing Cyber Risk

Treat Information Security As A Movement, Not A Moment

- 1 Evaluate cybersecurity risk as business risk
- 2 Instill and promote a culture of cyber awareness across all staff
- 3 Prioritize cybersecurity as an organizational imperative
- 4 Empower a single point of contact to protect information across the organization
- 5 Ensure Information Security has a seat at the table to report regular updates

SAFER Cyber Risk Assessment

Complimentary Cybersecurity Assessment

- Complete Information Security Review
- Board-ready Deliverables
- Full External Analysis
- Aligned to Industry-Standard Frameworks

Get Started: www.firestormglobal.com/safer

Questions? Email SAFER@firestormglobal.com

Executive Overview: SAFER Cyber Risk Assessment

Firestorm Global conducted a **SAFER Cyber Risk Assessment** aligned to industry-standard frameworks capturing comprehensive qualitative information through structured discovery and quantitative data based on externally visible risk telemetry.

Summary of Findings	Key Recommendations	External Telemetry
• Key considerations across each core domain area to bolster program maturity • Strategy and Protect are the strongest core domains • Detect and Correct have the most opportunity for improvement	• Align to all SAFER Six compliance requirements • Develop Threat Detection capabilities • Conduct scheduled Vulnerability Scanning • Create an Incident Response Plan • Develop culture of Security Awareness	• Significant potential external risk to be reviewed and validated by the IT team including high and critical vulnerabilities, end of support externally exposed software and unencrypted connections
Top Challenges	Greatest Areas of Risk	
• Limited quantity of staff, budget and training and the key challenges for the District to improve its Information Security program	• Elevated risk of extended downtime due to limited backup and incident response capabilities • Increased opportunity for threat actors to attempt infiltration based on external telemetry and end of support infrastructure • Higher likelihood of extended dwell time based on limited threat detection capability	

SAFER Six Compliance:

Immutable Backups

Endpoint Detection & Response (EDR)

Firewalls & Antivirus

Vulnerability Scanning

Multifactor Authentication

Cybersecurity Awareness

Cyber Risk Matrix

Education sector is a top target for cyber criminal syndicates

The District is at elevated organizational risk based on cybersecurity posture, including limited available staff and infrastructure

Medium financial risk exists based on total amount of District data and records

SAFER Cyber Six Best Practices

Aligned To Key Industry-Standards For Maximizing Member Protection

1	Multifactor Authentication:	Multi-factor for all remote systems access.
2	Firewalls & Antivirus	Confirmation that firewalls and antivirus software are in place, and updated with critical patches within 30 days of release.
3	Security Awareness Training	Confirmation that employee cyber security awareness training has taken place in the last 12 months.
4	Endpoint Detection & Response	Credible Endpoint Detection Response (EDR) tool is in place and active.
5	Immutable Backups	Data back-ups are stored offline and require separate credentials to access that are maintained outside of Active Directory or stored in a cloud service designed to protect such data from aransomware attacks.
6	Vulnerability Scanning	Confirmation that network vulnerability scans regularly take place.

Thank You



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



Tim | **Managing Principal**
Femister | Firestorm Global
tim@firestormglobal.com

SAFER@firestormglobal.com | www.firestormglobal.com/SAFER

Resources

- <https://www.bleepingcomputer.com/news/security/openai-confirms-threat-actors-use-chatgpt-to-write-malware/>
- https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf
- <https://www.reuters.com/technology/artificial-intelligence/openai-blocks-iranian-groups-chatgpt-accounts-targeting-us-election-2024-08-16/>
- <https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html>
- <https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html>
- <https://www.pcmag.com/news/fortune-50-company-made-record-breaking-75m-ransomware-payment>
- <https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams>
- <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10466545>
- <https://www.bloomberg.com/news/articles/2023-09-16/mgm-resorts-hackers-broke-in-after-tricking-it-service-desk>
- <https://www.bleepingcomputer.com/news/security/black-basta-ransomware-poses-as-it-support-on-microsoft-teams-to-breach-networks/>
- <https://www.forbes.com/sites/larsdaniel/2024/10/30/hackers-posing-as-it-support-on-teams-new-ransomware-scam-targeting-your-workplace/>
- <https://www.ic3.gov/PSA/2024/PSA241203>
- <https://www.beckershospitalreview.com/cybersecurity/change-healthcare-cyberattack-costs-to-reach-2-87b.html>
- <https://apnews.com/article/change-healthcare-cyberattack-unitedhealth-senate-9e2fff70ce4f93566043210bdd347a1f>