PAVING A PATH OF RESILIENCE

Southern California ReLIEF
Regional Liability Excess Fund

WELCOME

TO THE SOCAL RELIEF ANNUAL CONFERENCE

2025


FIRESTORM
GLOBAL

PAVING A PATH OF RESILIENCE

Southern California ReLiEF
Regional Liability Excess Fund

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

1. Continuous Cyber Risk Monitoring
2. Cyber Risk Alerting
3. SAFER Cyber Risk Assessments
4. Cyber Awareness Resources
5. Ask An Expert Hotline
6. Member Advisories
7. Discounted Cybersecurity Services
8. Cybersecurity Webinar Series
9. Online Cybersecurity Training (Coming Soon)

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

Fact

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

✕ Fiction

2 AI writes more effective phishing emails than humans

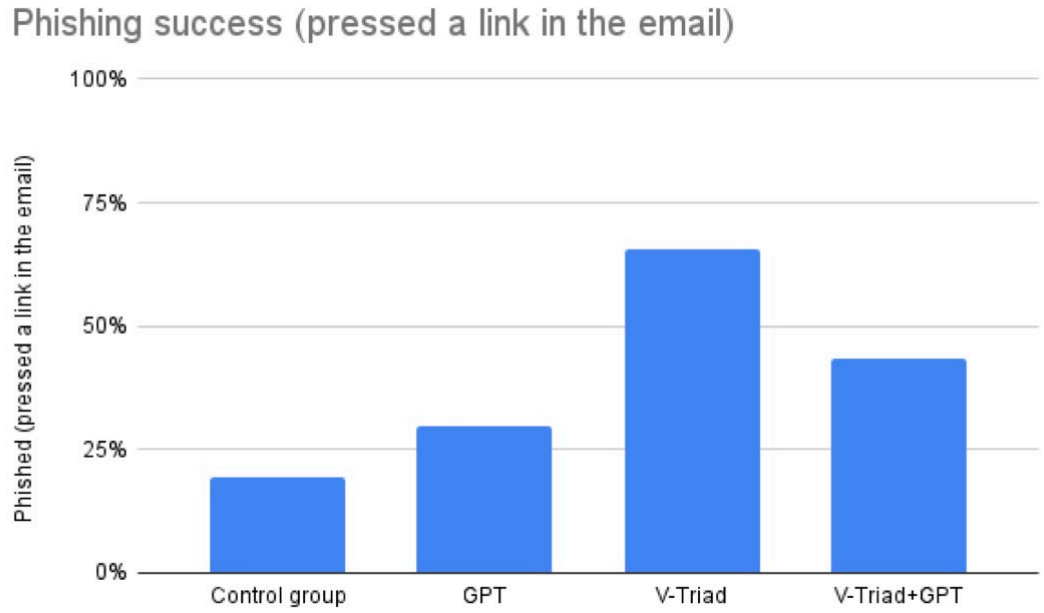
HBR

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



✗ Fiction

2 AI writes more effective phishing emails than humans

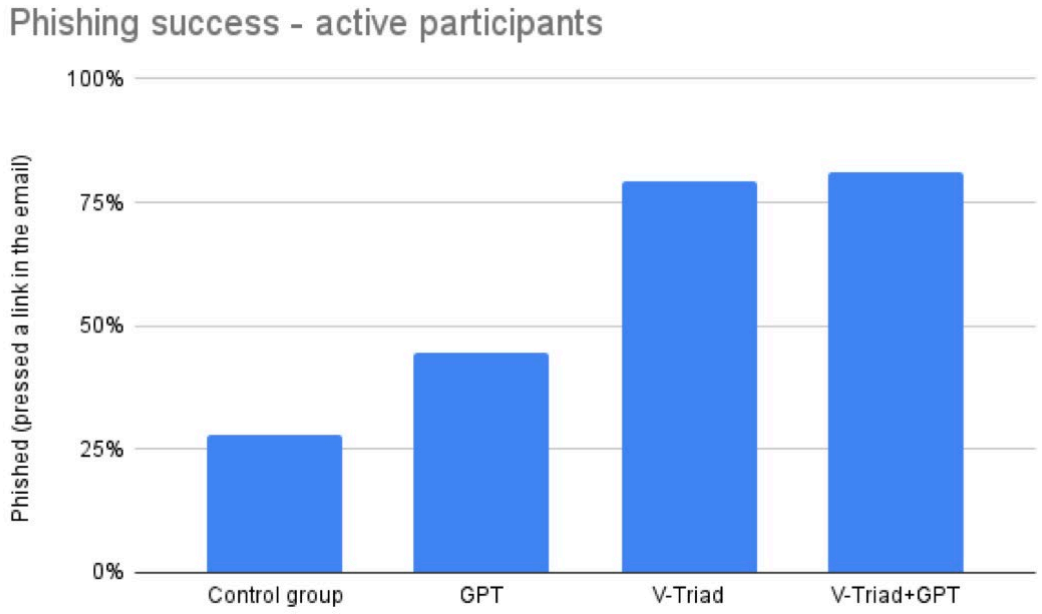
HBR

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



Fact or Fiction?

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

Fact

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

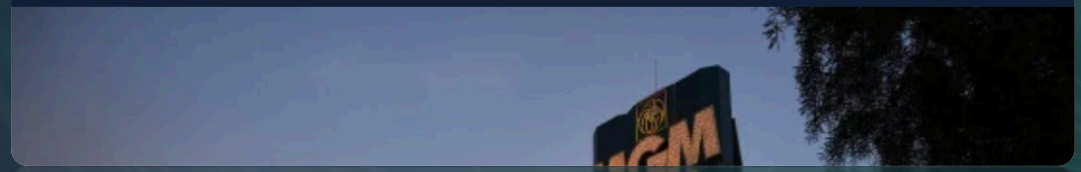
NBC NEWS

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

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

Can You Spot The Phish?

1

Security alert for your linked Google account

G

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

Tuesday, November 26, 2024 at 2:17 PM

To: Tim Femister

Google

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.

VS

2

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

TF

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

Today at 9:29 PM

To: Tim Femister

Tim Femister shared an item

T

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

Hi Tim,

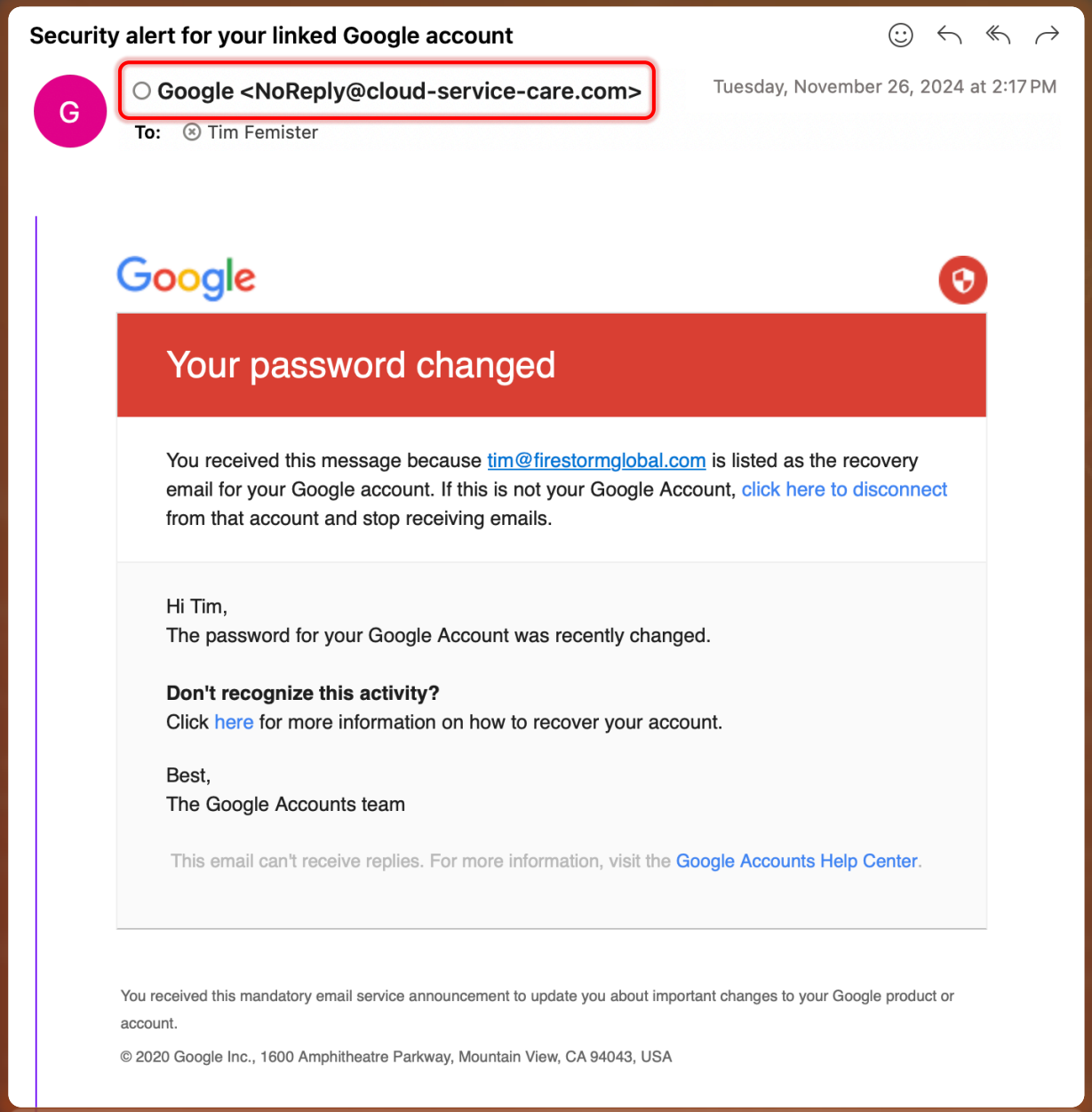
Please download the attached file.

Thank you.

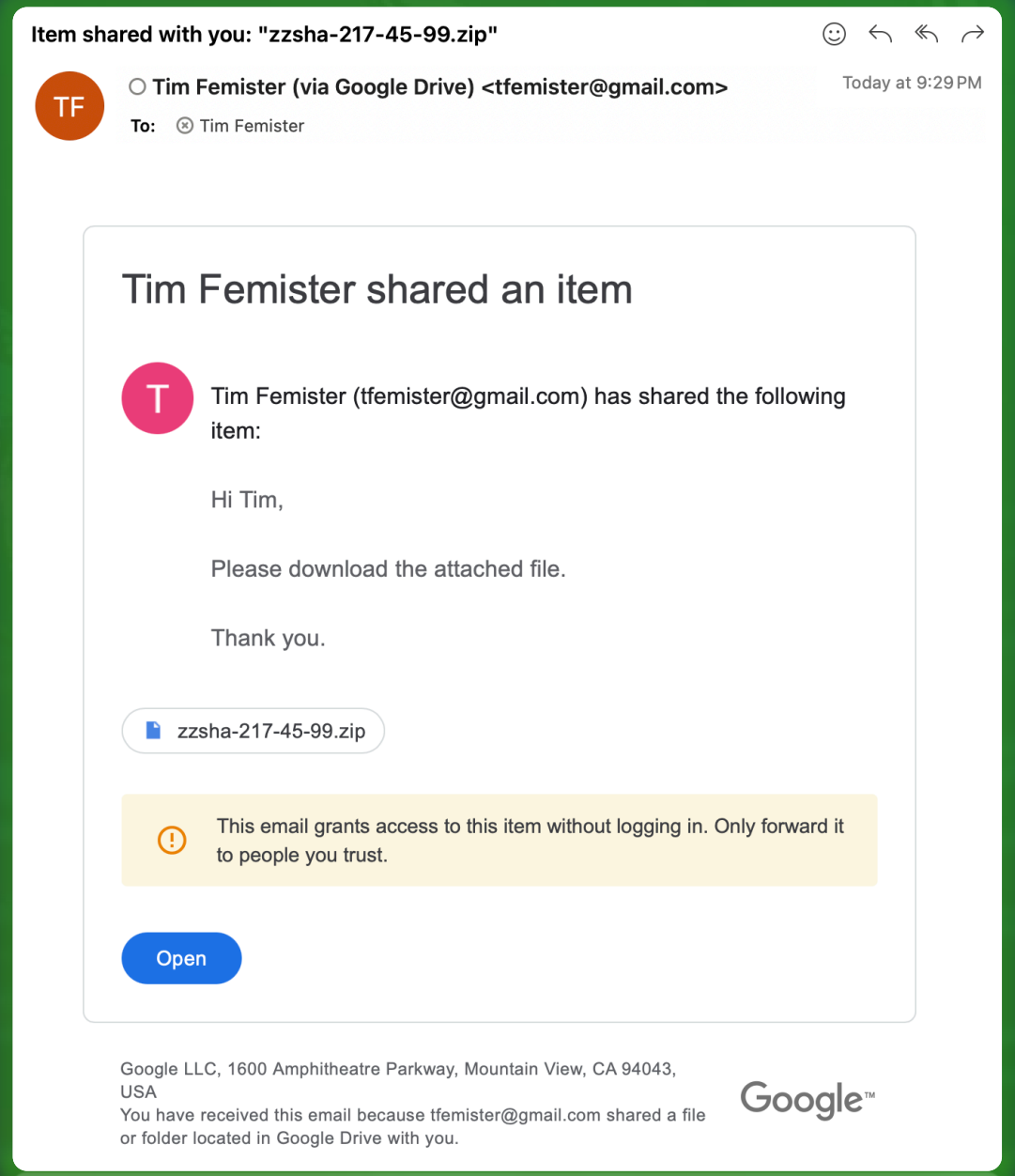
zzsha-217-45-99.zip

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

Open


Security alert for your linked Google account
G
Google <NoReply@cloud-service-care.com>
Tuesday, November 26, 2024 at 2:17 PM
To: Tim Femister
Google
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"
TF
Tim Femister (via Google Drive) <tfemister@gmail.com>
Today at 9:29 PM
To: Tim Femister
Tim Femister shared an item
T
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


Can You Spot The Generative AI?

vs

1

vs

2

DARK WEB TOUR

WITH FIRESTORM GLOBAL

NOT FOR PUBLIC DISTRIBUTION

Common Themes Amongst Districts

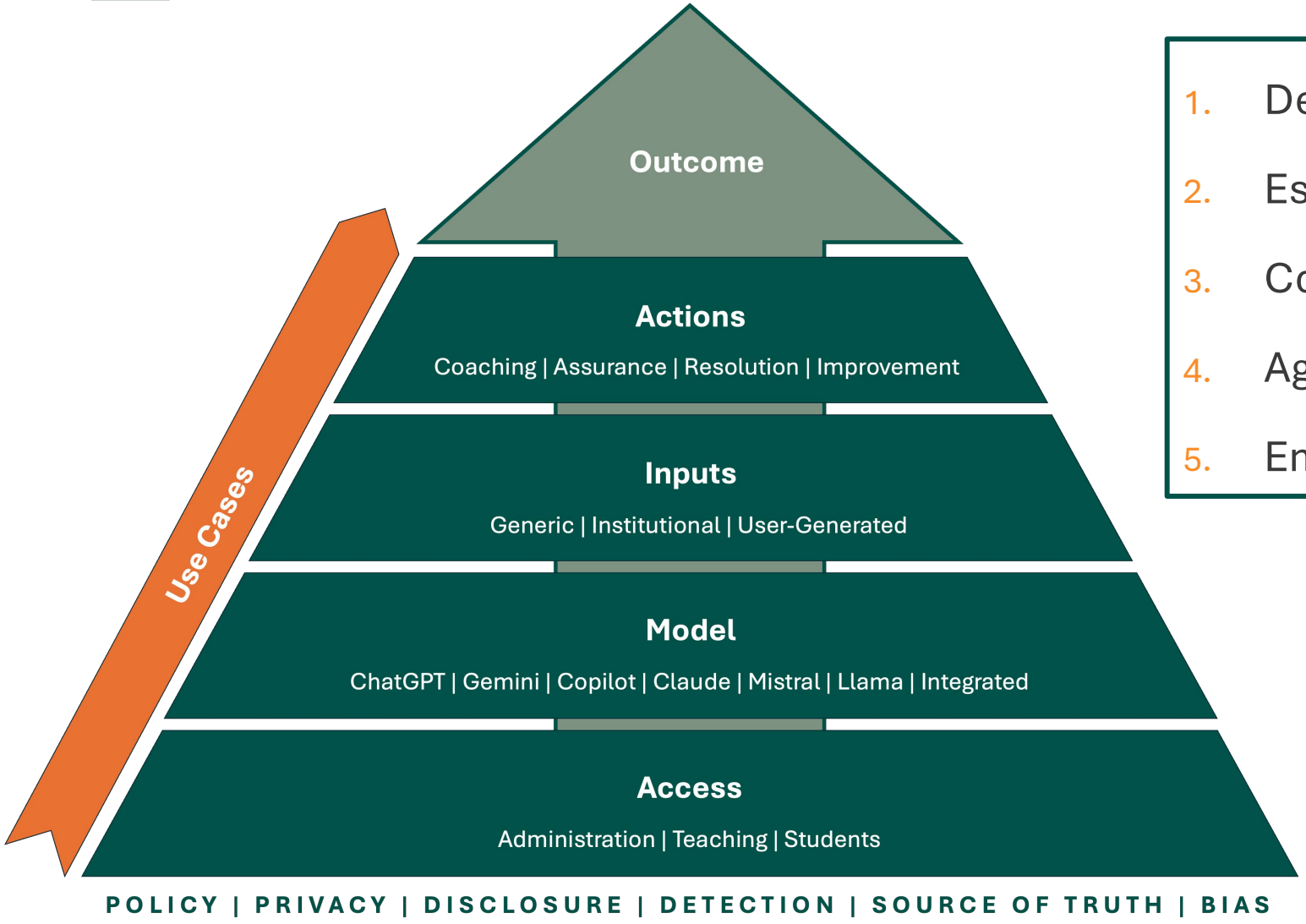
1. Over reliance on **Protection** controls; Under reliance on **Detection** and **Response**
2. Few Districts have implemented an **Incident Response Plan**
3. Lack of awareness training for **high-impact district positions** (e.g. Finance, HR)
4. Limited formality in **help desk policies** governing 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



1. Define Acceptable Models
2. Estimate Current Use (Network Analysis)
3. Communicate Opportunities & Risks
4. Agree on Source of Truth
5. Emphasize Privacy and Safety

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

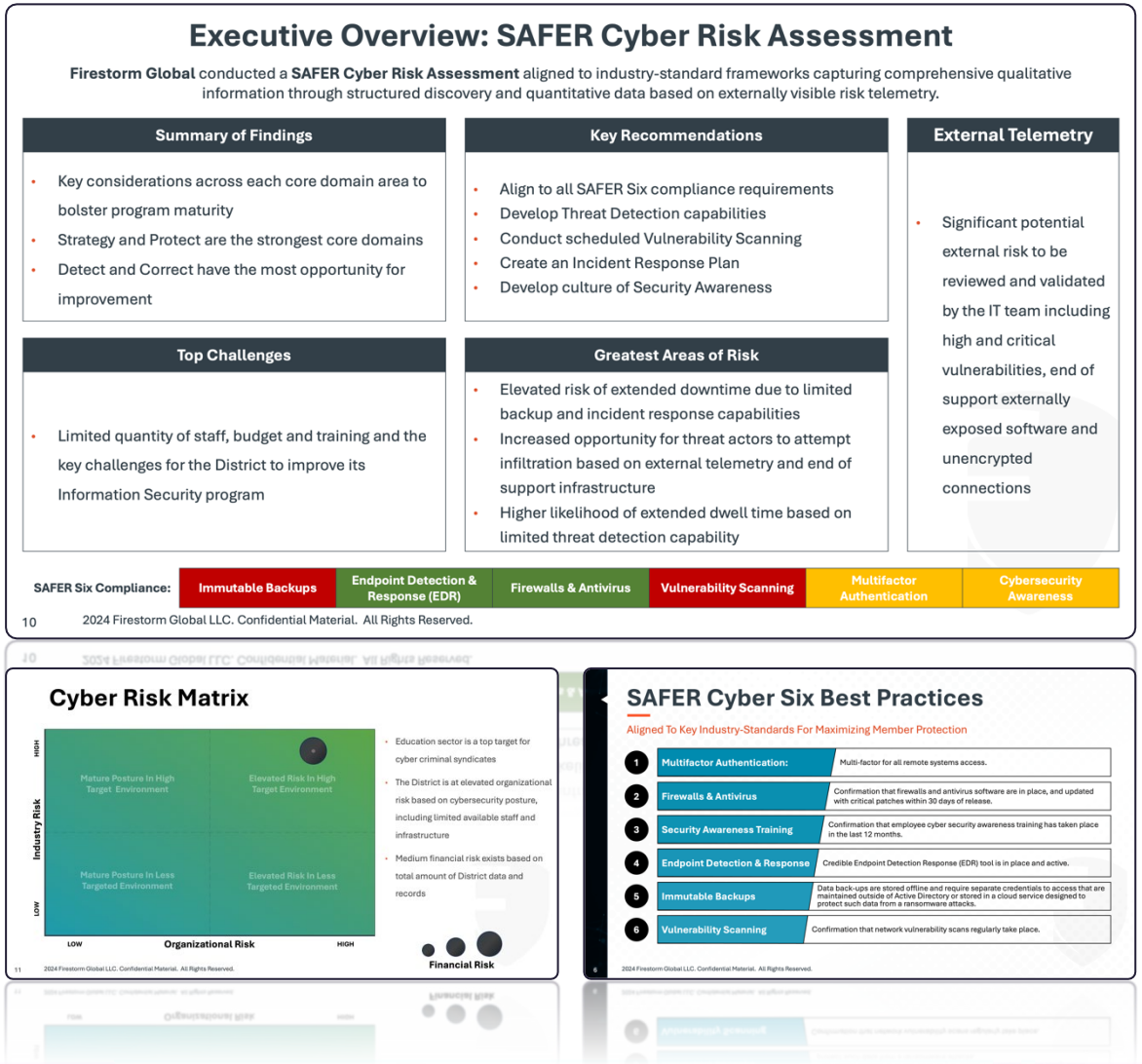
SAFER Cyber Risk Assessment

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



Thank You

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

Tim Femister | **Managing Principal** 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