Walking the Tightrope of Cybersecurity Risk Management

Presenter

Colin Taggart

Colin.Taggart@plantemoran.com
248-223-3235

Agenda

Top cyber trends

Cybersecurity focus areas for executives

Key takeaways

Recent Incidents

72%

of businesses worldwide were affected by ransomware as of 2023. *Source: Statista*

8 out of 10

Organizations had at least one individual who fell victim to a phishing attempt by CISA Assessment teams. *Source: CISA*

KnowBe4 How a North Korean Fake IT Worker Tried to Infiltrate Us

Ransomware trends

Intelligence gathering

Ransomware crime groups gather intelligence on intended victims, like studying financial statements for an organization's financial position and using the information to scale ransom demands.

Double Extortion

Gain persistence in network to steal data before encrypting and to potentially continue to have a foothold after any recovery

Attacks on cloud service providers

Ransomware writers are now targeting cloud service providers with network file encryption attacks as a way to hold hostage the maximum number of customers possible.

Financial Institution Ransomware and Data Theft

- Only 1 in 10 attacks were stopped before encryption took place.
- Root cause - Exploited vulnerabilities (40%), emails (33%), and compromised credentials (23%) were the three most common entry points for significant ransomware attacks in the financial services sector.
- 43% of financial services organizations paid the ransom to recover their encrypted data.

- Know which of your vendors who will assist with ransomware incidents
- Train teammates and test ransomware scenarios

Source: Sophos News

Common Wire Fraud Attacks

Unexpected Request

Last-Minute Changes to Wire Instructions

Bogus “Problems” on Account Issues

Vendor Account Changes

Social Engineering – Video Call Spoofing

How to Clone Your Voice with AI Voice Cloning?

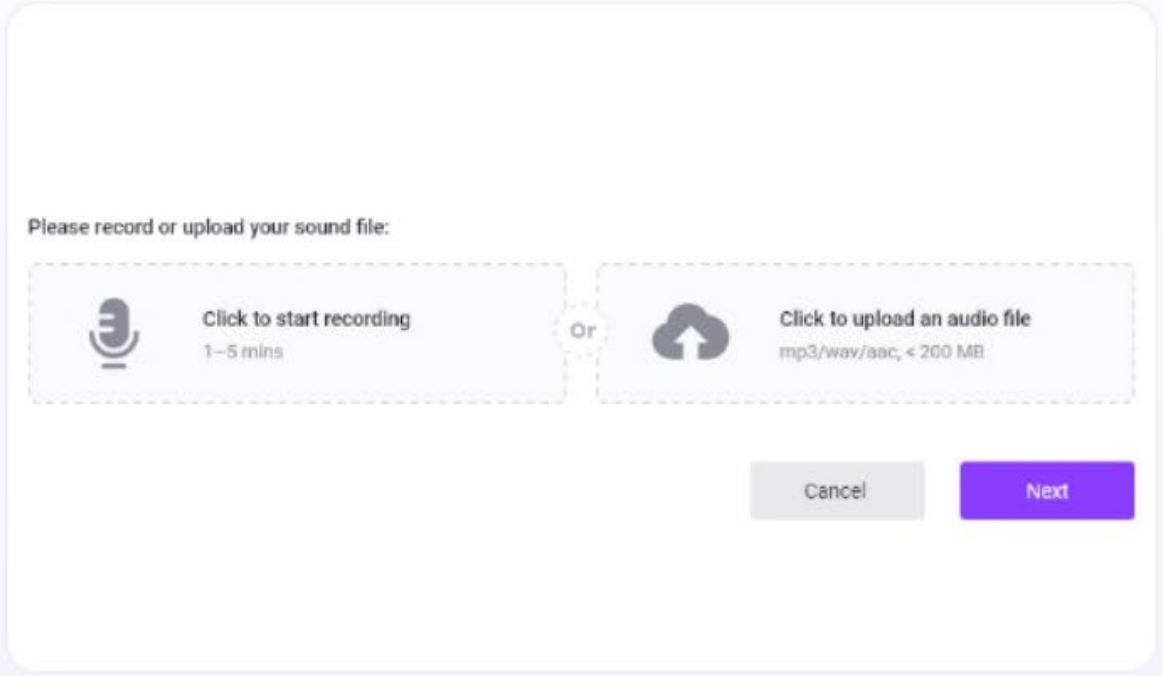
You are now only 3 steps away from cloning any voice and letting them say anything you want.

Open Vidnoz AI Voice Cloning.

Record/Upload Now

Record or upload speaking audio to clone voice.

Preview or download your cloned audio.



Generate your exclusive voice Only $9.99

Upload an audio file as a voice sample to create your exclusive voice with your tone.

New Twist on Common Wire Fraud Attacks

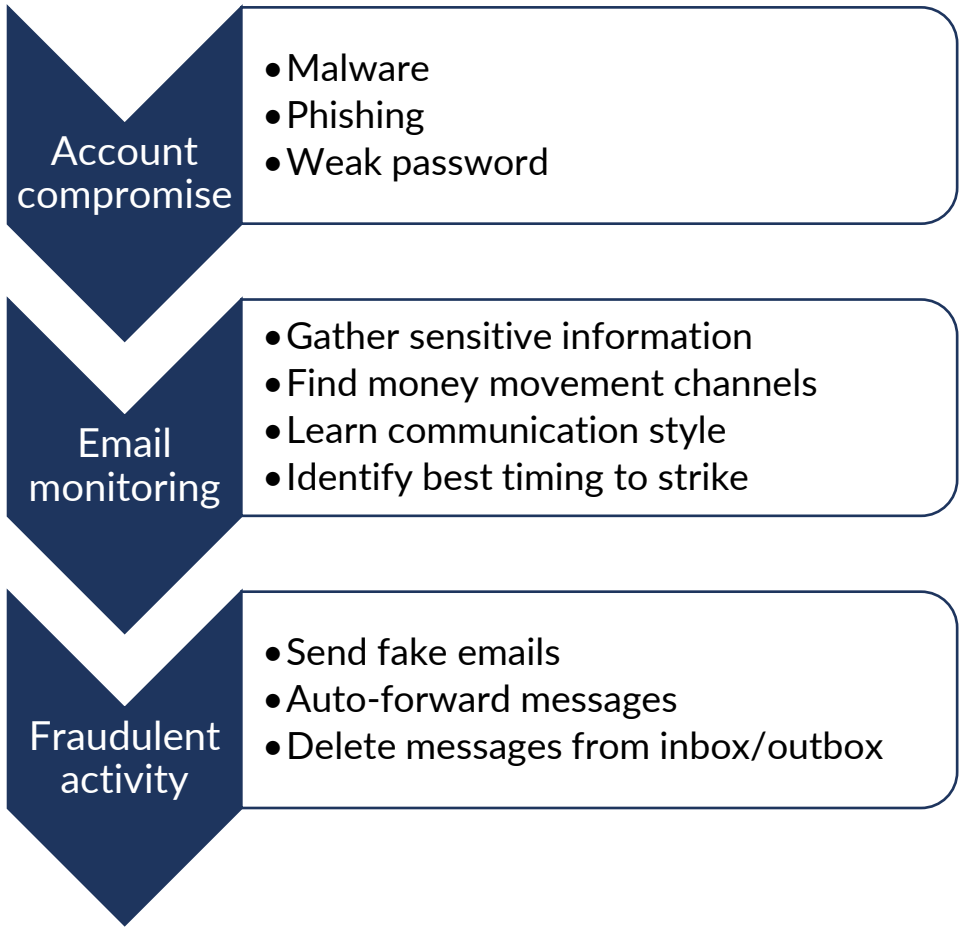
Unexpected Request

Last-Minute Changes to Wire Instructions

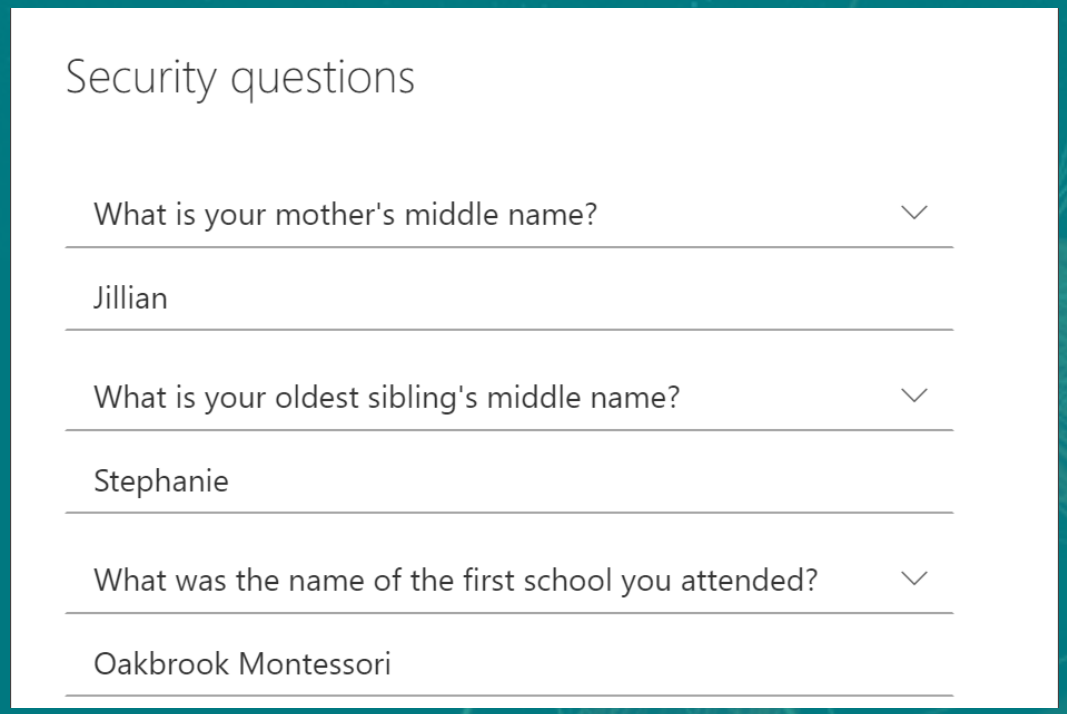
Bogus “Problems” on Account Issues

Vendor Account Changes

Business Email Compromise (BEC)



How secret are answers to security questions?



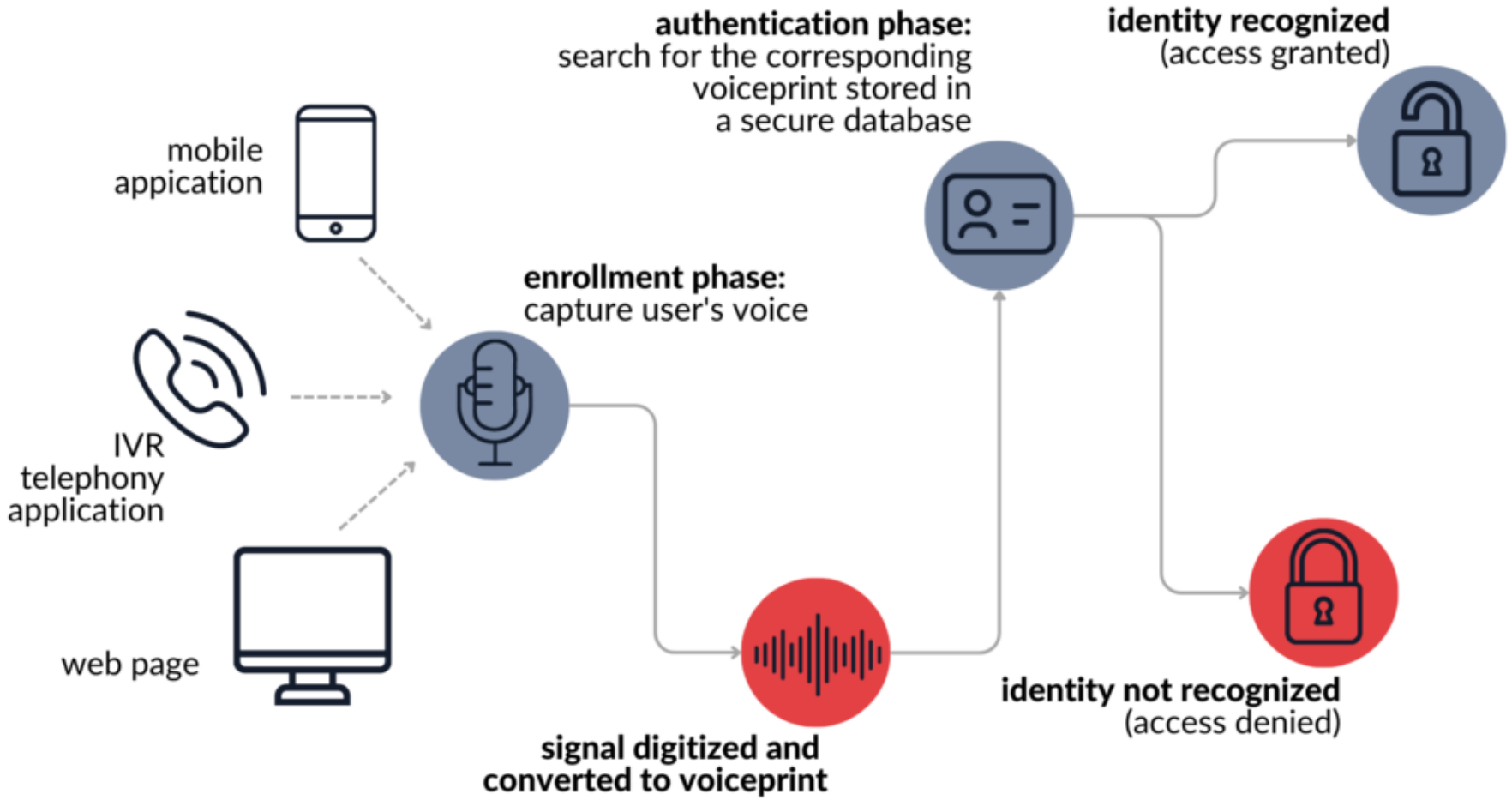
Risk-based authentication

Out of wallet

Out-of-band authentication

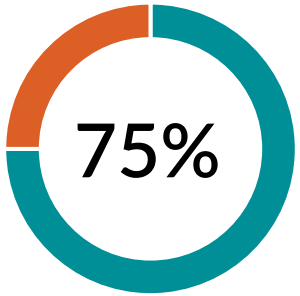
Alerts on failed attempts

Voice Biometrics

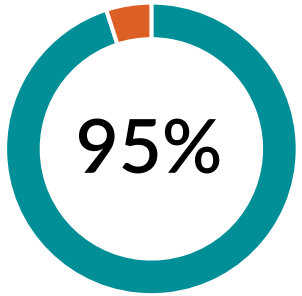


Employee Focused Attacks

Employee Based Incidents

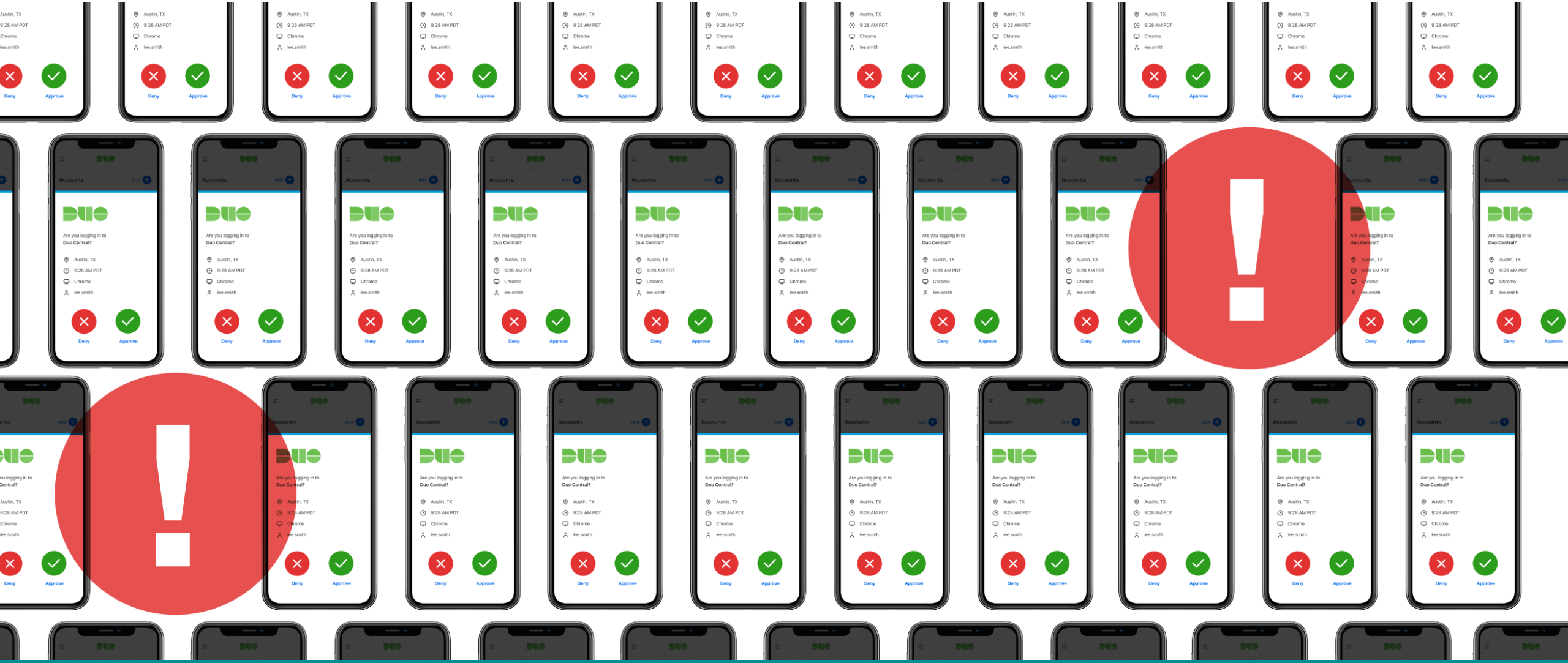


Security breaches due to human error

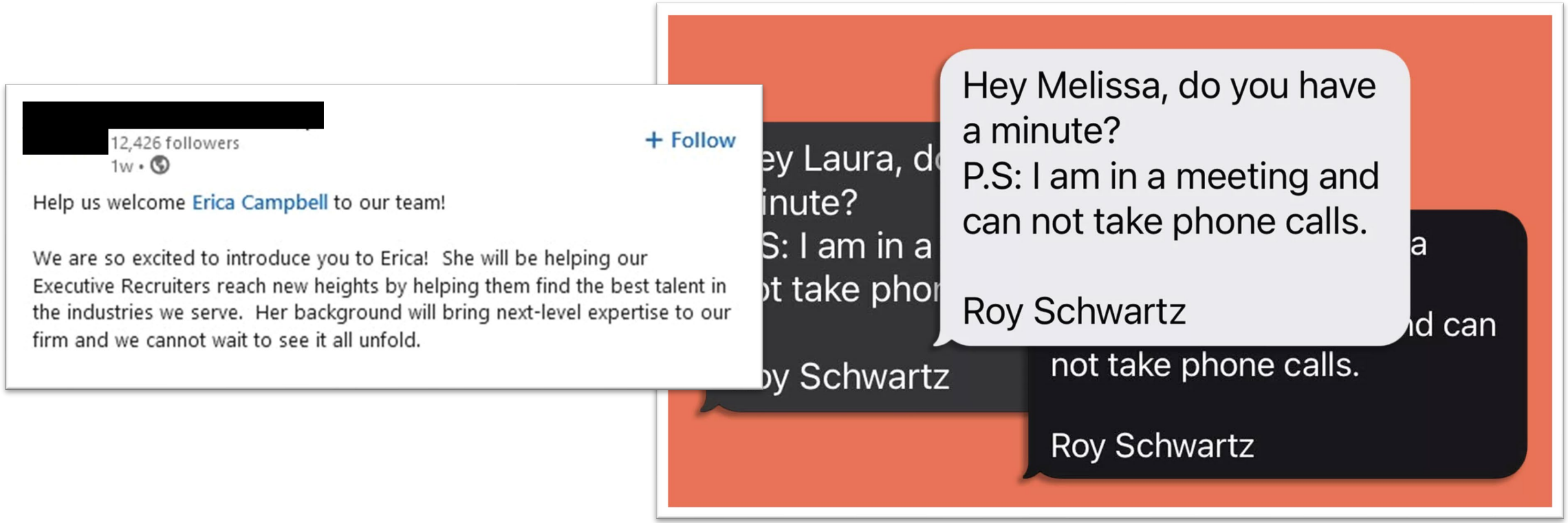


Source: Deltalogix

Social Engineering – Multifactor Fatigue



Phishing Text/Email Targeting New Hires



Social Engineering Key Controls

Policy

Training

Testing

Reporting/Responding

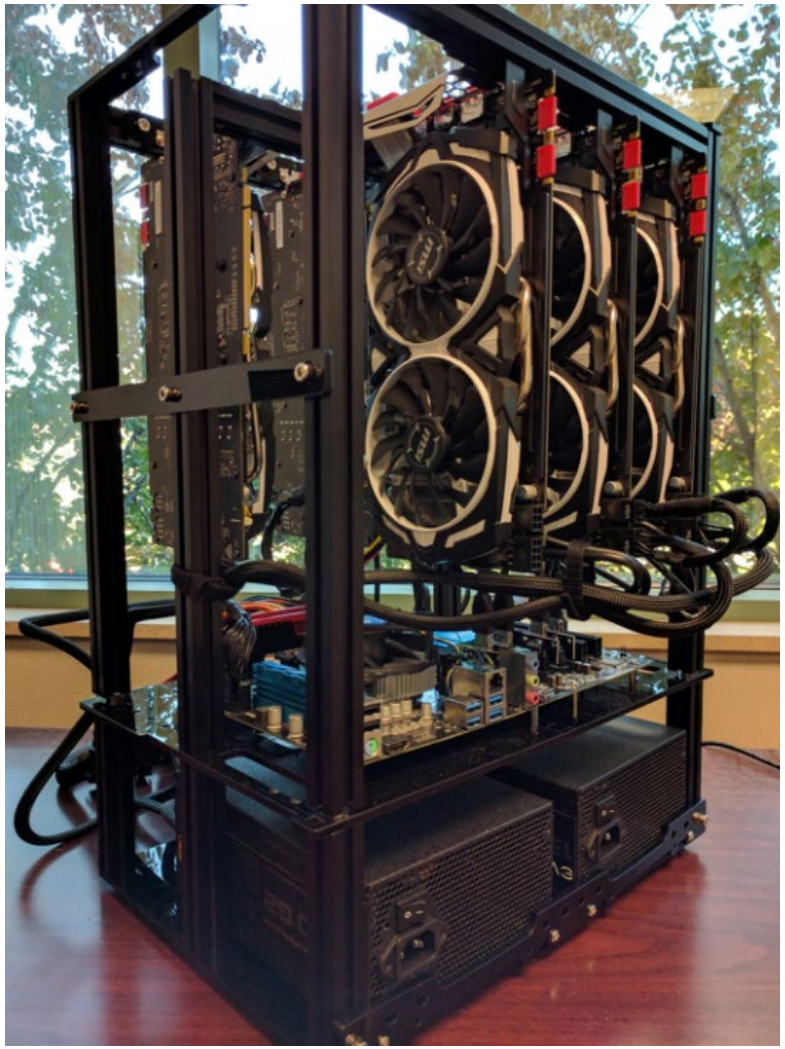
CATCH THE GOLDEN PHISH

Password Compromises

Password re-use – compromised vendors/websites

Weak passwords

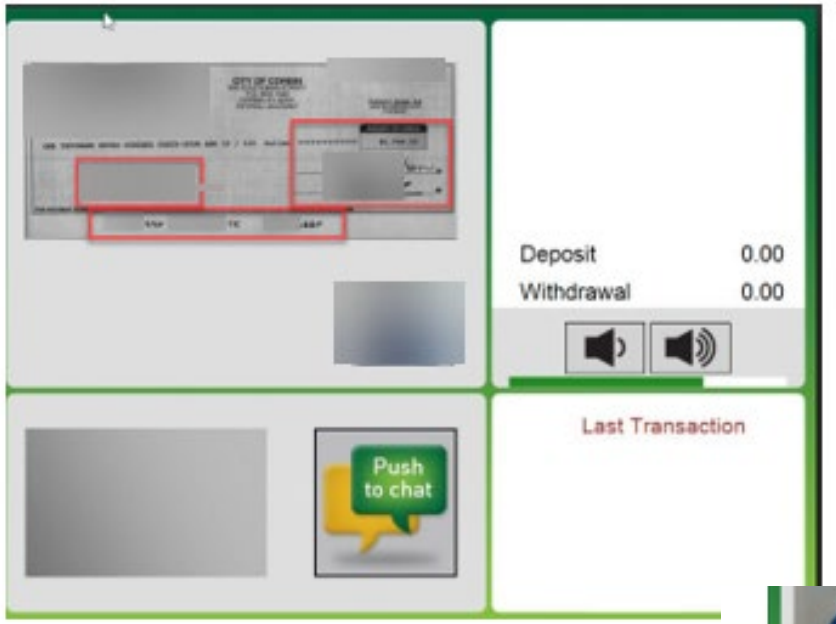
Password managers



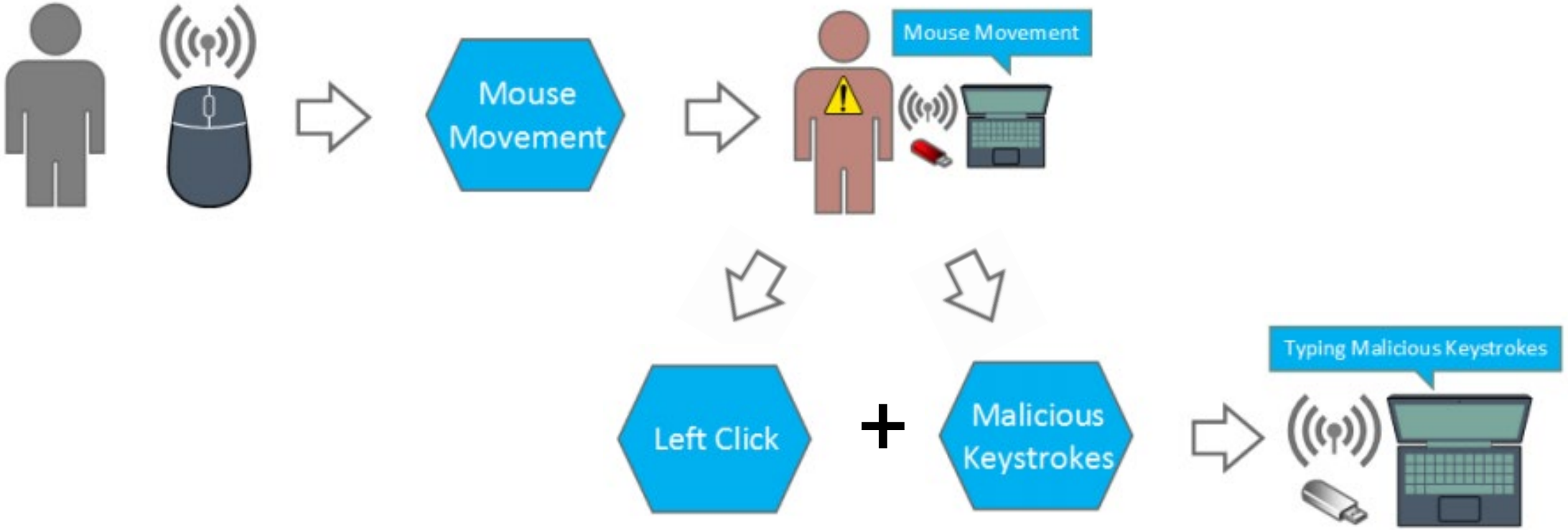
```
PAT
Password Assessment Tool

    Password Analysis
[+] 70 of 444 (15.8%) hashes were cracked.
[+] Results:

Top 10 base words
welcome = 27 (38.57%)
[redacted] = 2 (2.86%)
halloween = 2 (2.86%)
swamy = 1 (1.43%)
zaq1zaq!zaq = 1 (1.43%)
happybirthday = 1 (1.43%)
robinannette = 1 (1.43%)
y0u@r3mysunshin = 1 (1.43%)
nightmare = 1 (1.43%)
snickers = 1 (1.43%)

Password length (length ordered)
12 = 1 (1.43%)
13 = 27 (38.57%)
14 = 17 (24.29%)
15 = 5 (7.14%)
16 = 12 (17.14%)
17 = 4 (5.71%)
18 = 2 (2.86%)
20 = 2 (2.86%)
```

Technology Focused Attacks

New Device Vulnerabilities – ITM's



New Device Vulnerabilities – Wireless Mice



Microsoft 365

	Information Worker Plans												Frontline Worker Plans					
	Microsoft 365				Office 365			Enterprise Mobility + Security		Windows 11			Microsoft 365					Office 365
	E3	E5	E5 Security[1]	E5 Compliance[1]	E1	E3	E5	E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F3	F5 Security[2]	F5 Compliance[2]	F5 Sec+Comp[2]	F3[3]
Microsoft 365 apps																		
Desktop client apps[1]	•	•				•	•											
Microsoft 365 for mobile	•	•			•	•	•						Read only	•[2]				•[2]
Install apps on up to 5 PCs/Mac + 5 tablets + 5 smartphones	•	•			•[3]	•	•							•[3]				•[3]
Microsoft 365 for the web	•	•			•	•	•						Read only	•				•
Visio for the web	•	•			•	•	•						Read only	•				•
Microsoft Loop components	•	•			•	•	•						•	•				•
Create and share Loop pages[4] and workspaces	•	•																
Contribute to Loop pages and workspaces	•	•			•	•	•						•	•				•
Microsoft Clipchamp Standard	•	•																
Microsoft Editor premium features	•	•				•	•											
Multilingual user interface for Microsoft 365 apps	•	•				•	•											

[1] Requires Microsoft 365 E3 (or Office 365 E3 and Enterprise Mobility + Security E3).
[2] Requires Microsoft 365 F1/F3 (or Office 365 F3 and Enterprise Mobility + Security E3).
[3] Not available for new customer purchases in Volume Licensing or Web Direct channels.

[1] Includes Word, Excel, PowerPoint, OneNote, Outlook, Access (PC only), and Publisher (PC only).
[2] Limited to devices with integrated screens smaller than 10.9".
[3] Mobile apps only.
4 Any user can create and share pages within a workspace to which they have been invited.

Email, calendar, and scheduling																		
Exchange Kiosk (2 GB mailbox)													See footnote 1	•				•
Exchange Plan 1 (50 GB mailbox + 50 GB archive)					•													
Exchange Plan 2 (100 GB mailbox + up to 1.5 TB archive[2])	•	•				•	•											
Calendar	•	•			•	•	•						•	•				•
Outlook desktop client	•	•				•	•											
Auto-expanding email archive	•	•				•	•									•	•	
Exchange Online Protection	•	•			•	•	•											
Public folder mailboxes	•	•			•	•	•											
Resource mailboxes	•	•			•	•	•											
Inactive mailboxes	•	•				•	•											
Microsoft Shifts	•	•			•	•	•											
Microsoft Bookings	•	•			•	•	•											

[1] Microsoft 365 F1 includes the Exchange Kiosk service plan to enable Teams calendar only. It does not include mailbox rights.
[2] 100 GB initial archive with automatic expansion up to 1.5 TB.

Conditional Access

Dashboard > > Security > Conditional Access

Conditional Access | Named locations

Azure Active Directory

«

Policies

Insights and reporting

Diagnose and solve problems

Manage

Named locations

Custom controls (Preview)

+ Countries location + IP ranges location Configure MFA trusted IPs

Named locations are used by Azure AD security reports to reduce false positives and Azure AD conditional access policies.

Location type : **All types** Trusted type : **All types**

Search names

Name
No named locations found.

Banned Password Lists

All services > Security | Authentication methods > Authentication methods

Authentication methods | Password protection

Azure AD Security

Search

Save Discard Got feedback?

Manage

- Policies
- Password protection
- Registration campaign
- Authentication strengths (Preview)

Monitoring

- Activity
- User registration details
- Registration and reset events
- Bulk operation results

Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: Yes / No

Custom banned password list:

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: Yes / No

Mode: Enforced / Audit

Evolving Regulatory Expectations

Regulatory Updates – August 29

FFIEC Information Technology Examination Handbook

Development, Acquisition, and Maintenance

8/31/25 – CAT Sunset

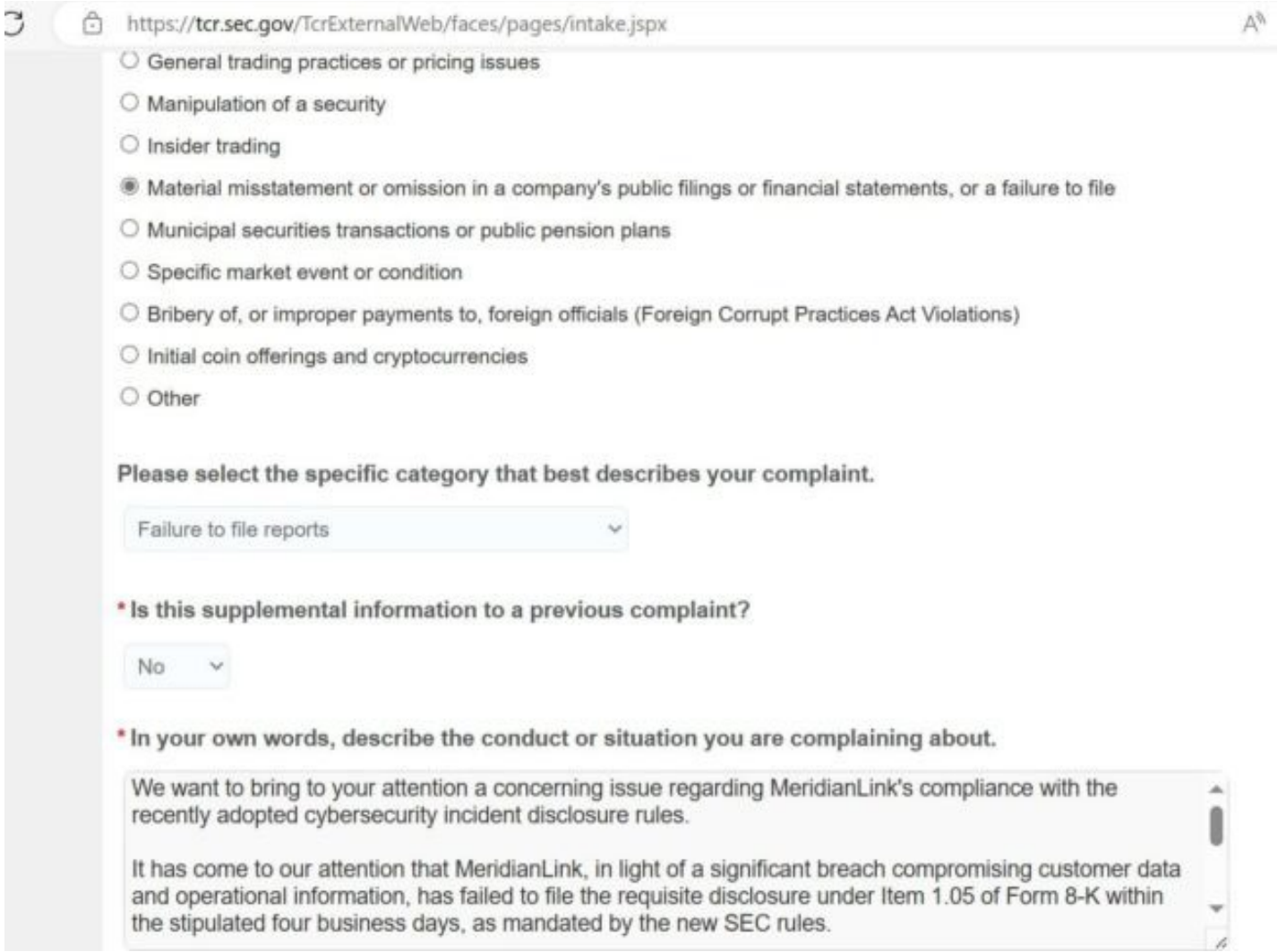
- NIST CSF 2.0
- CISA Cybersecurity Performance Goals
- CRI Profile 2.0
- CIS Critical Security Controls

Regulatory Updates

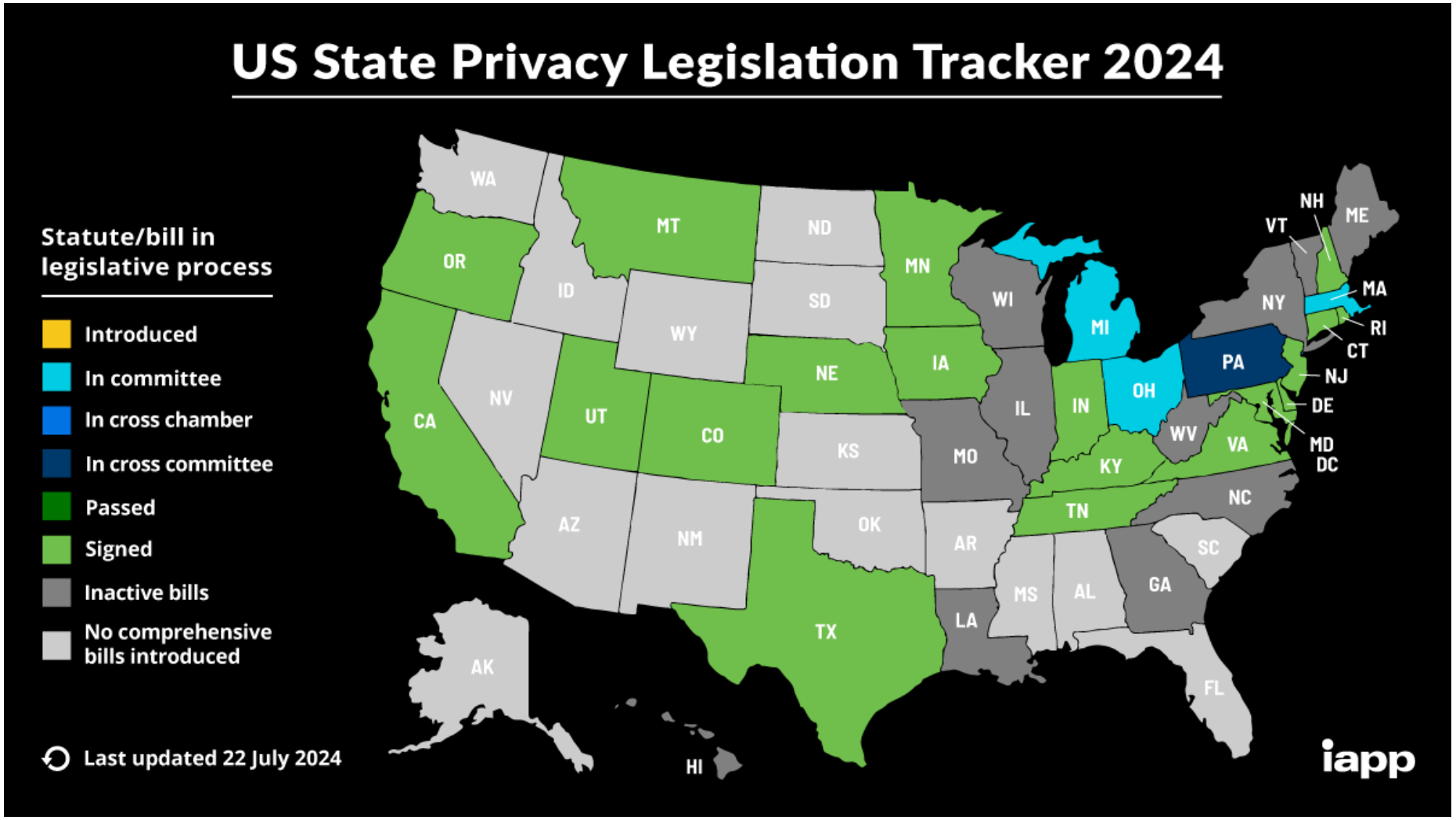
June 2023 - Interagency Guidance on Third-Party Relationships: Risk Management

September 2023 – Updated Information Technology Risk Examination (InTREx) Procedure

SEC Cyber Incident Disclosure



Regulatory Updates – Privacy Requirements



Cyber insurance challenges

GOVERNANCE, POLICIES AND PROCEDURES

5. Does the applicant have:

a. A documented Incident Response Plan that has been tested (e.g., tabletop exercise) in the last 12 months? Yes ☒ No ☐

b. Documented business continuity and disaster recovery plans that have been tested in the prior 12 months? Yes ☒ No ☐

If "Yes," do they address ransomware attacks, and what are the time objectives and defined roles for the recovery? _Yes, operational recovery of main systems within 24 hours

c. A documented security audit process? Yes ☒ No ☐

d. A Chief Information Security Officer or equivalent? Yes ☒ No ☐

i. If "Yes," internal or external? Internal ☒ External ☒

e. A formal/written Data Retention Policy, which includes email? Yes ☒ No ☐

f. A documented Privacy Policy? Yes ☐ No ☐

g. Does the applicant utilize any of the following security frameworks, standards, or best practices:

☐ NIST	☐ HIPPA Security	☐ COBIT
☐ ISO/IEC 27001	☐ ISF	☐ HITECH
☐ PCI-DSS	☐ FFIEC	☐ Center for Internet Security Cybersecurity Assessment Tools

Others (Please Specify) _____

EMAIL SECURITY

6. Is the Applicant's email server on premises or hosted with a third party?
On premises ☐ Hosted with a third party ☒

7. If with a third party, which vendor? _____

8. Is annual (or more frequent) security awareness training with includes phishing, required for all employees? Yes ☒ No ☐

9. Are employees on an annual or more frequent basis receive security awareness training

10. Does the Applicant allow users to access e-mail when not at a company location? Yes ☒ No ☐

a. If "Yes," then does the Applicant require multi-factor authentication (MFA) for all users? Yes ☒ No ☐

b. Does the Applicant allow access through personal and/or non-company supplied devices? Yes ☒ No ☐

11. Does the Applicant use a product to scan emails for malicious files and/or links? Yes ☒ No ☐

a. If "Yes," which product/tool is utilized? _____
Cybergraph_____

12. Does the applicant utilize an email sandboxing process to test suspicious emails? Yes ☒ No ☐

13. Does the Applicant tag emails from outside of the organization as "external" or similar? Yes ☒ No ☐

14. Does the Applicant use a Data Loss Prevention process/tool for email? Yes ☐ No ☒

15. Does email infrastructure offer SPF/DKIM/DMARC for other companies to ensure the Applicant's messages are legitimate? Yes ☒ No ☐

16. Does your email structure filter messages based on SPF/DKIM/DMARC? Yes ☒ No ☐

17. Does the Applicant use a quarantine and/or other screening process for emails? Yes ☒ No ☐

a. If "Yes," please describe _____
Cybergraph_____

Cyber insurance challenges

20. **Access Control**

a. Does the Applicant require use of MFA for all users for remote access to its network?
b. Does the Applicant require MFA for all access to all cloud-based services or applications used by the Applicant?
c. Does the Applicant require use of MFA for all access to administrator accounts? Note: Administrator accounts are accounts used by users to carry out tasks that require special permissions, such as installing software, managing anti-virus administration, editing information in Active Directory, accessing routers, or provide access to backups.

If "No" to any of a-c above, please provide details below:

_____
_____
_____

d. Does staff with administrator privileges utilize a separate user account when exercising administrative privileges?
e. Does the Applicant allow non-IT employees local administrative privileges?
f. Does the Applicant use a privileged access management solution or other tool to protect privileged accounts?
If "Yes," which product(s)

_____ _____

g. Does the Applicant utilize a VPN for remote connection?

Network Segmentation

a. Is the Applicant's network segmented for security purposes, either virtually or physically? Yes ☒ No ☐

i. If "Yes" then which of the following features are utilized:

☐ DMZs	☒ Hardware Firewalls/internal segmentation firewalls
☐ Industrial Control Systems (ICS) network	☒ VLAN
☒ VoIP network	☐ Access Control Lists
☒ Guest network	☐ Software Defined Perimeter
☐ SDN	☐ PCI Data segregation
☐ Proxy server	☐ Other

mments (Optional): _____
_____

What controls/tools does the Applicant use to protect physical access to the environment?

_____ _____
_____
_____
___

Does the Applicant utilize Operational Technology (OT) technologies and protocols in their operations (e.g., to monitor and control Industrial Control Systems, manufacturing equipment, and supervisory control and data acquisition (SCADA) software)? Yes ☒ No ☐

a. If "Yes," are the Applicant's OT systems segmented from the rest of the environment? Yes ☒ No ☐
b. If "Yes," is the Applicant's OT systems exposed to/accessible from the public internet? Yes ☐ No ☒
i. If "Yes," does the Applicant require MFA for all remote access to OT systems? Yes ☐ No ☐

Takeaways

1. Ongoing training on social engineering – calls, emails, and in-person

2. Support for Bank-wide password manager

3. Implement multifactor authentication –employee, Board, and customer

4. From mice to AI – assess security of new technologies

5. Test incident detection and response capabilities – and involve key vendors

Thank you!

Colin Taggart

Colin.Taggart@plantemoran.com
248-223-3235