Maine Bankers Association

Cyber incident trends & MFA

Portland, ME
April 26, 2023

Presentation by

Today’s topics:

- Cyber incident trends
  - What’s getting attacked?
  - Industry-specific patterns
  - Focus on ransomware
- Multi-factor authentication
  - Common deployment issues
  - Where we see regulations going regarding MFA
  - What are some “gotchas” or things to avoid

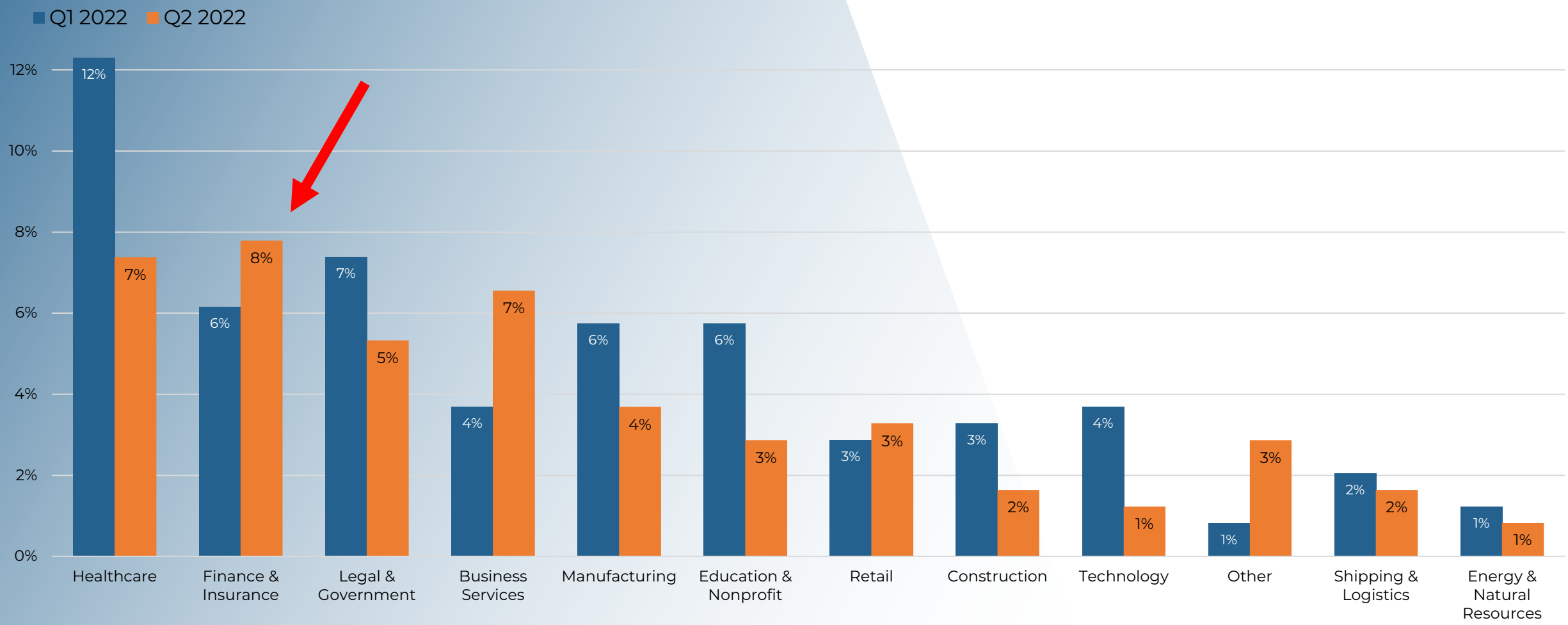
Topic 1 of 2

Cyber Incident Trends

This data summarizes aggregated and anonymized information related to **Incident Response (IR) cyber insurance claims** that Arctic Wolf investigated from January – June 2022

INCIDENTS BY INDUSTRY

Investigations during January – July 2022



RANSOMWARE ROOT POINT OF COMPRIMISE (RPOC) BY INDUSTRY

Q1 & Q2 2022

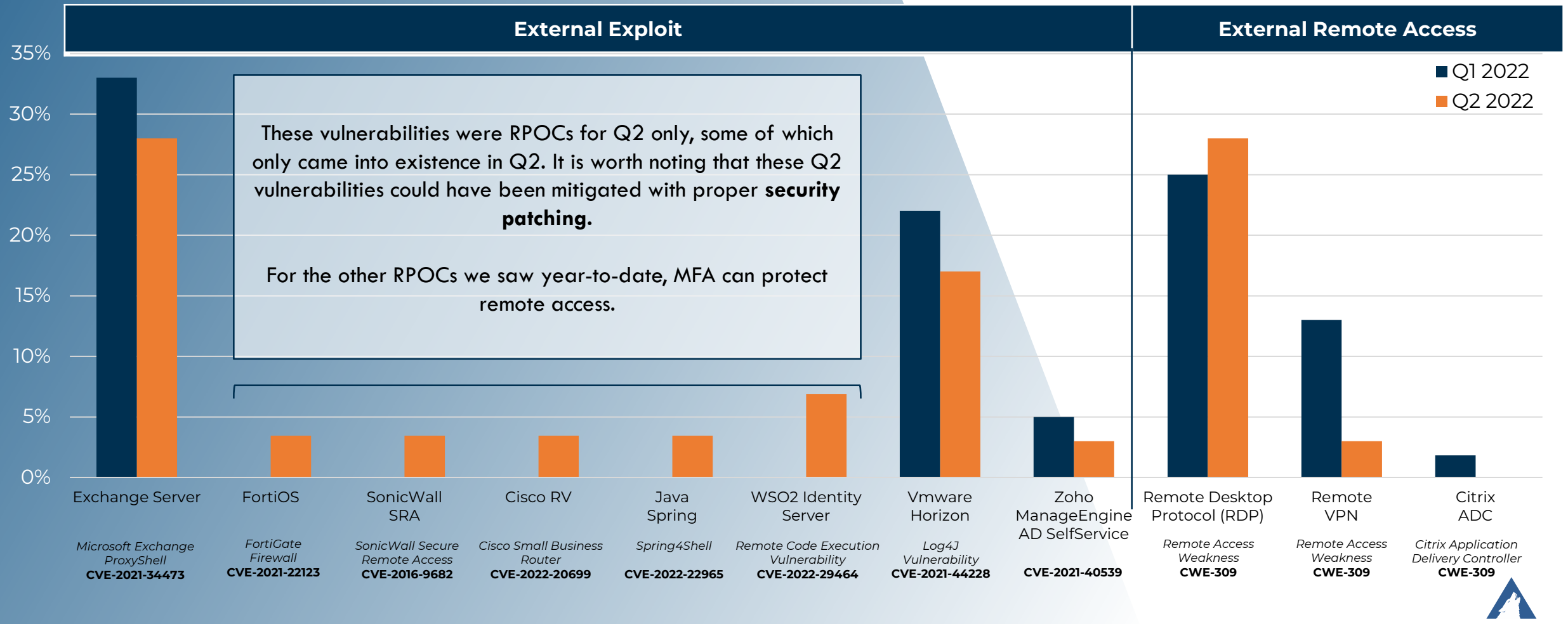
Sorted by Case Volume by Industry

Industry	External Exposure		User Action		
	External Exploit	External Remote Access	Phishing Email	Social Engineering	Drive by Attack
Healthcare	61%	35%			4%
Finance & Insurance	33%	25%	17%	8%	17%
Legal & Government	60%	10%	30%		
Business Services	14%	43%	29%	14%	
Manufacturing	70%	10%	10%		10%
Education & Nonprofit	69%	23%		8%	
Retail	60%	40%			
Construction	50%	25%	25%		
Technology	67%	33%			
Other	100%				
Shipping & Logistics	80%			20%	
Energy & Natural Resources			100%		

RANSOMWARE RPOC BY PRODUCT

Q1 & Q2 2022

Threat actors carried out the majority of attacks via **vulnerabilities** and weaknesses they know how to exploit. The following are products / vendors leveraged in Arctic Wolf cyber insurance incident response work so far this year.



Topic 2 of 2

Multifactor Authentication

MFA weaknesses are the most common cybersecurity gap exploited at financial services companies.

From January 2020 to July 2021, **64% of entities regulated by DFS that reported a cybersecurity incident had some sort of gap in MFA.**

Over 18.3 million consumers were impacted by cybersecurity incidents reported to the DFS **by** companies with **MFA failures.**

Implementing MFA – The Challenges

Challenge #1: MFA Tool Sprawl

- There are many ways to implement MFA in your organization, whether natively through your applications or by implementing third-party vendor solutions:
  - *SMS/Phone Callback*
  - *Authenticator Apps*
  - *Hardware tokens*
  - *Biometric*

- MFA tool sprawl creates challenges for both the IT/Security team and the end users
  - **IT/Security Team**: No single pane of glass for administrative IAM/MFA management leading to lower security effectiveness

  - **End Users**: Having too many MFA tools/platforms for end users to manage leads to low adoption rate, end user frustration, security workarounds, etc.

- Inventory all software/hardware platforms currently using, or offering, native MFA to understand areas in which MFA sprawl may occur

Implementing MFA – The Challenges

Challenge #2: Lack of Sufficient MFA Coverage

- Misapplication of MFA not only leaves the door open for attackers, but can lead to cyber insurance/compliance issues

- Organizations (at a minimum) **must cover all privileged/high-risk user accounts** with strong authentication to include MFA
  - *This includes internal and external access to directory services (IAM), internal network, and endpoints*
  - *Without this your organization risks attacker privileged account escalation leading to significantly increased incident damage*

- To lower risk and better align to compliance cyber insurance requirements, consider MFA adoption for:
  - **All external user access** to internal network resources and endpoints
  - **All email systems** accessed through the cloud (O365, Google Workspace, etc.)

- With legacy systems, full MFA adoption may not be feasible – in these circumstances, apply compensating controls or consider the possibility of moving certain systems to the cloud

Implementing MFA – The Challenges

Challenge #3: Usability

- End users present a significant challenge to successful organization-wide MFA adoption

- When moving past privileged user account MFA adoption, organization wide rollout can provide MFA usability challenges for end users

- **Usability challenges include**:
  - *Device incompatibility (out of date OS, lack of smart phone, etc.)*
  - *Hesitation to adopt (Slow down current processes, lack of awareness training)*
  - *Poor user experience (lack of training, tool design, etc.)*

- Implementing a proper pre-rollout process is critical to MFA implementation success
  - Users need education, an understanding of *the why*, access to resources to prepare, and most importantly, **time**

Arctic Wolf and MFA

Getting more out of your MFA investment

- Arctic Wolf's **Managed Detection & Response** (MDR) service offering provides 24x7x365 data ingestion and threat monitoring for deployed MFA tools to include *Duo*, *Okta*, and *Microsoft*

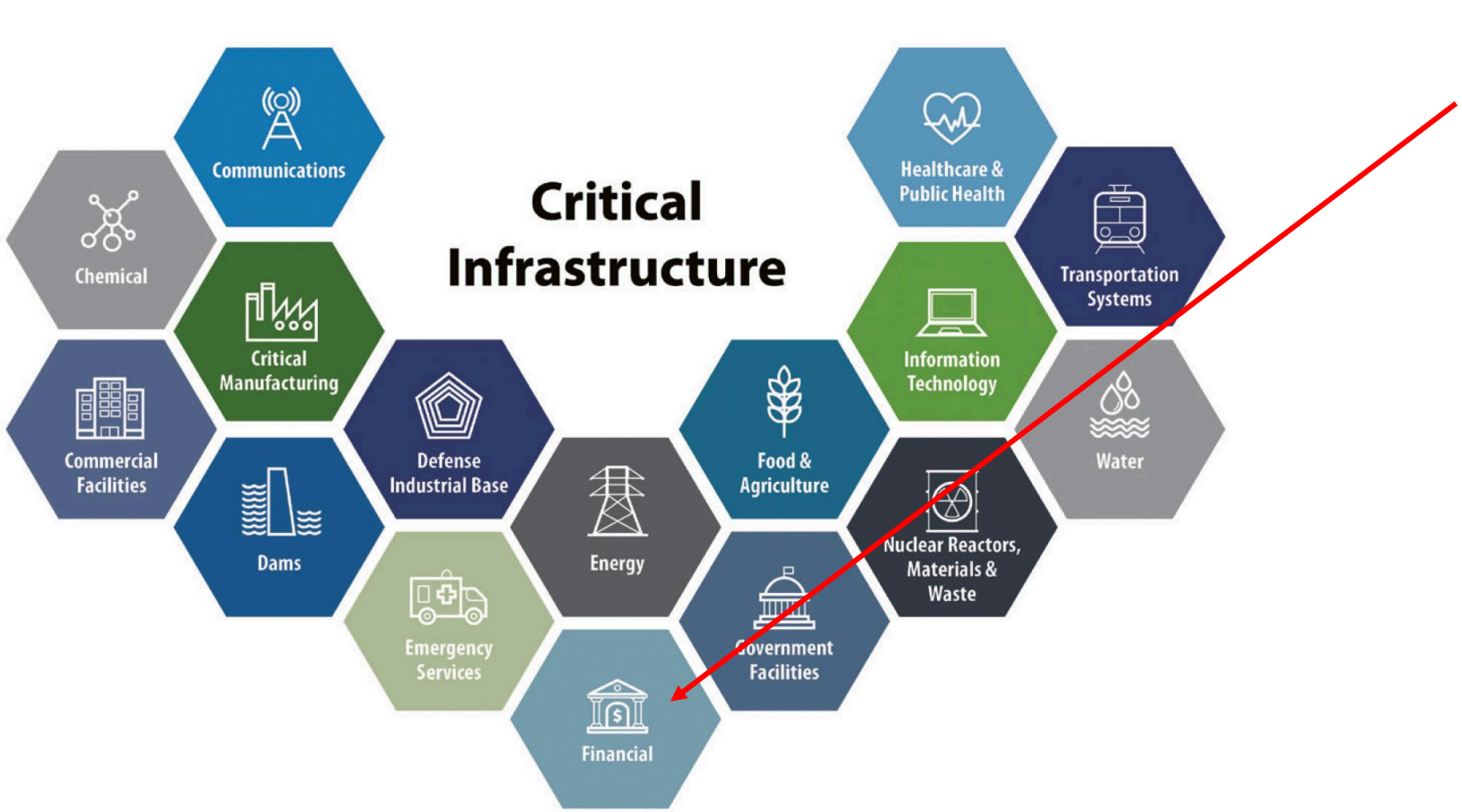
- With single pane of glass data ingestion and alerting, Arctic Wolf can identify MFA attacks to include (non-exhaustive):
  - *MFA Fatigue*
  - *Restricted Country Login*
  - *User/Admin MFA Deactivation*
  - *Fraudulent Login Attempts*

- The assigned **Concierge Security Team** (CST) act as strategic guidance advisors while guiding clients down a guided Security Journey to include:
  - *Security Posture in Depth Reviews (SPiDRs) focused on current/future MFA deployment*
  - *Ongoing, unlimited security guidance and security best practice recommendations*
  - *Inclusion of compliance frameworks to ensure proper adherence and audit readiness*

United States Critical Infrastructure

- *“There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have debilitating effect on security, national economic security, national public health or safety, or any combination thereof”*

Critical Infrastructure: Financial Services



© US Cybersecurity & Infrastructure Security Agency (CISA)

- **Financial Services Sector:**
  - *Depository institutions*
  - *Credit and financing organizations*
  - *Providers of the critical financial utilities and services that support these functions*

Proposed Amendments in New York

- Conduct systematic scans or reviews at least weekly (vs. bi-annually)
- Increased CISO responsibilities – Authority to make binding decisions about cybersecurity program
- Independent cybersecurity audits (not an audit by the person doing the work)
- MFA for all privileged accounts

Source: https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2_text_20221109_0.pdf

Discussion Question

What's your biggest struggle with multi-factor authentication

a) Unsupported/legacy systems
b) Incomplete MFA rollouts
c) Reliance on insecure MFA methods like SMS *
d) Other

*The FBI recommends against using phone numbers for two-factor authentication.

THANK YOU

FOR FOLLOWUP, PLEASE CONTACT:

JEFF MILLER

518-390-2534 (CELL)

JEFF.MILLER@ARCTICWOLF.COM