Cybersecurity for Small Business

CALIFORNIA
PSYCHOLOGICAL
ASSOCIATION

CPA Division I Practice Conference 2024:
Using New Digital Technologies to Support Our Practice

Sam Bowne

Nov 9, 2024

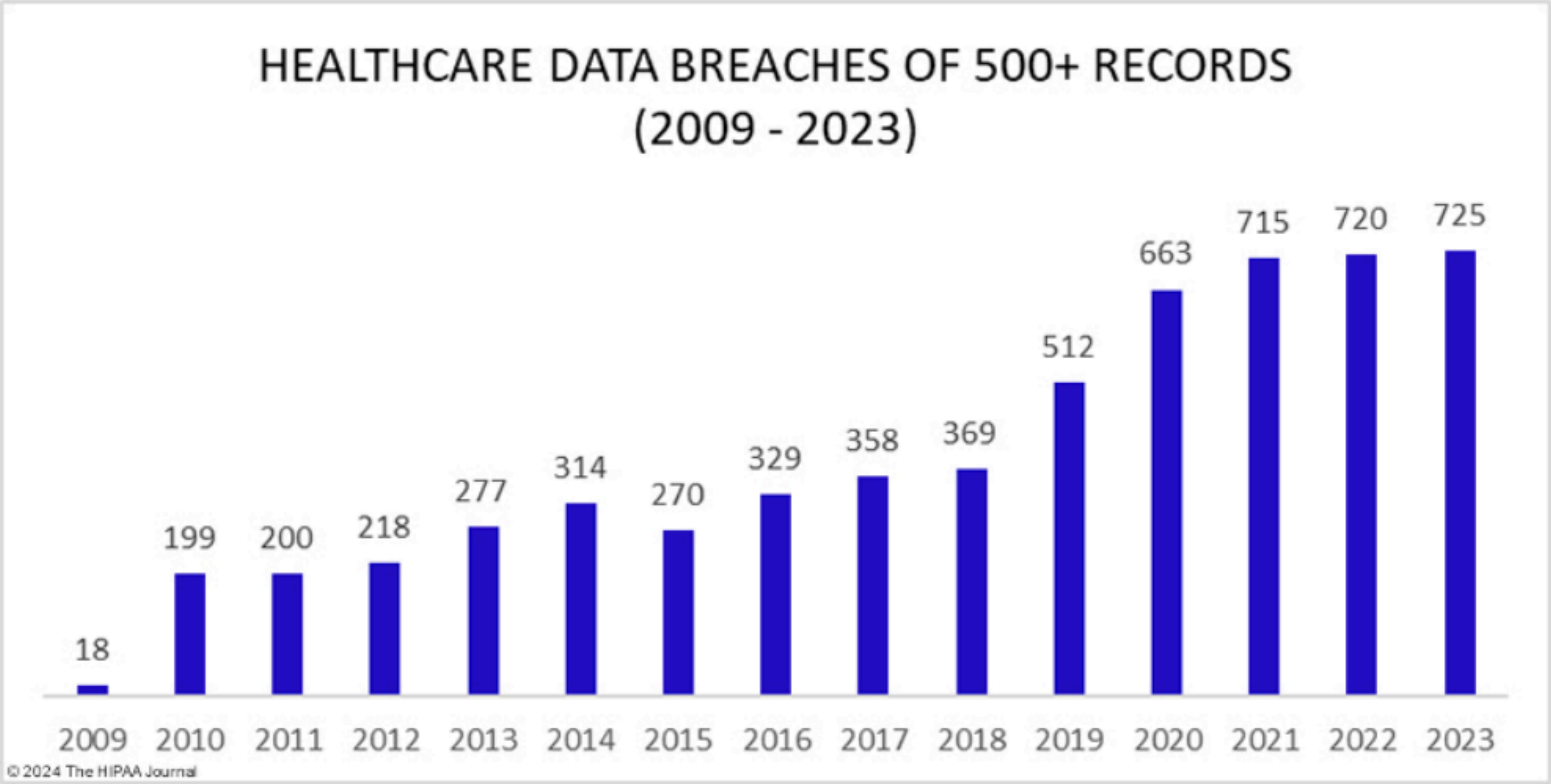
Whoami

- Sam Bowne, PhD
- Instructor at City College San Francisco
- Corporate consultant for Infosec Decoded
- Web: samsclass.info
- Email: sam.bowne@infosecdecoded.com
- Mastodon: sambowne@infosec.exchange

Introduction to this Presentation

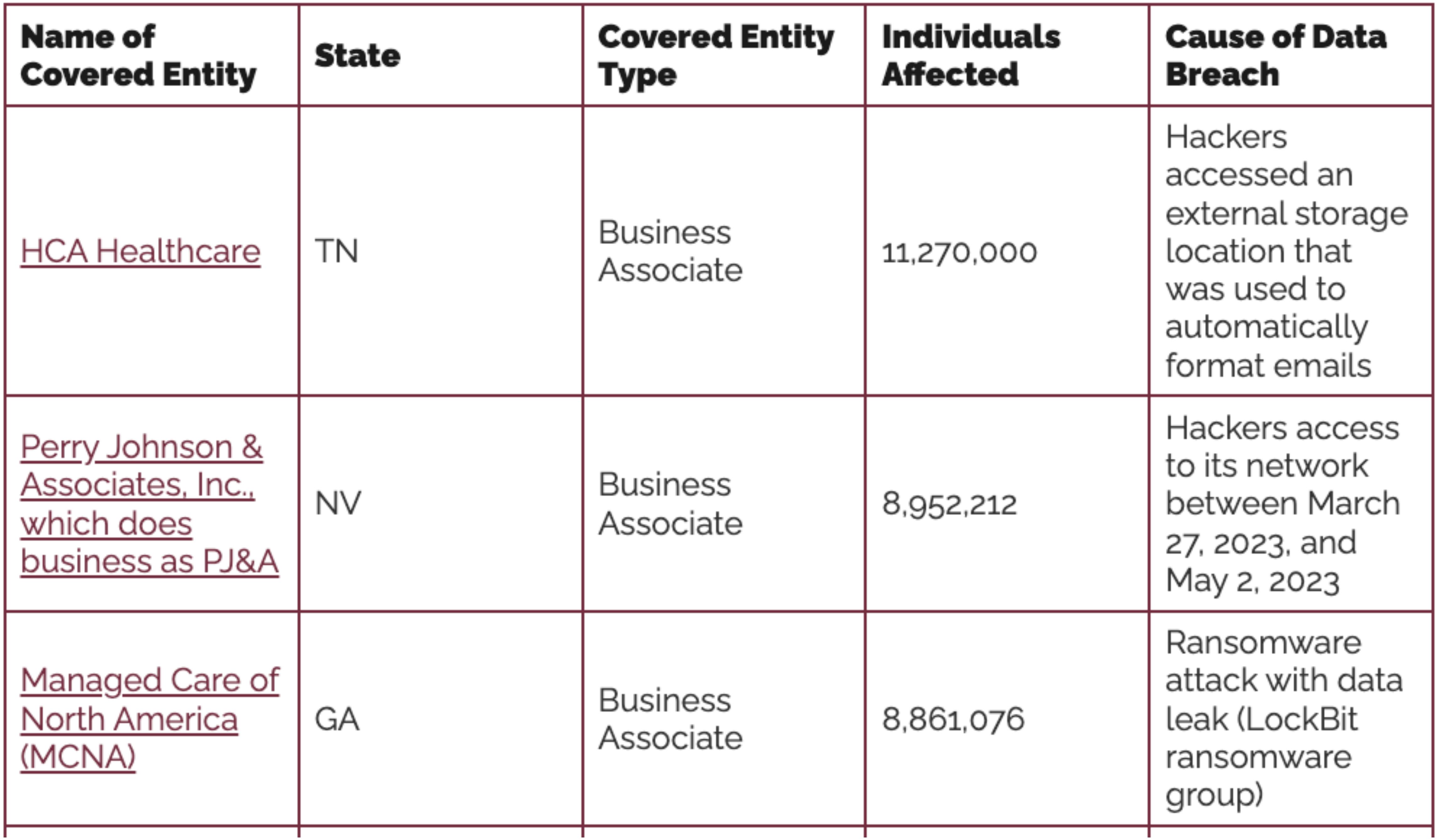
- I am recording this talk and will post the video at
  - **samsclass.info**
- Please put questions in the Zoom chat during the presentation.
- There's a Q&A section at the end which will not be recorded.

Case Studies of Recent Incidents

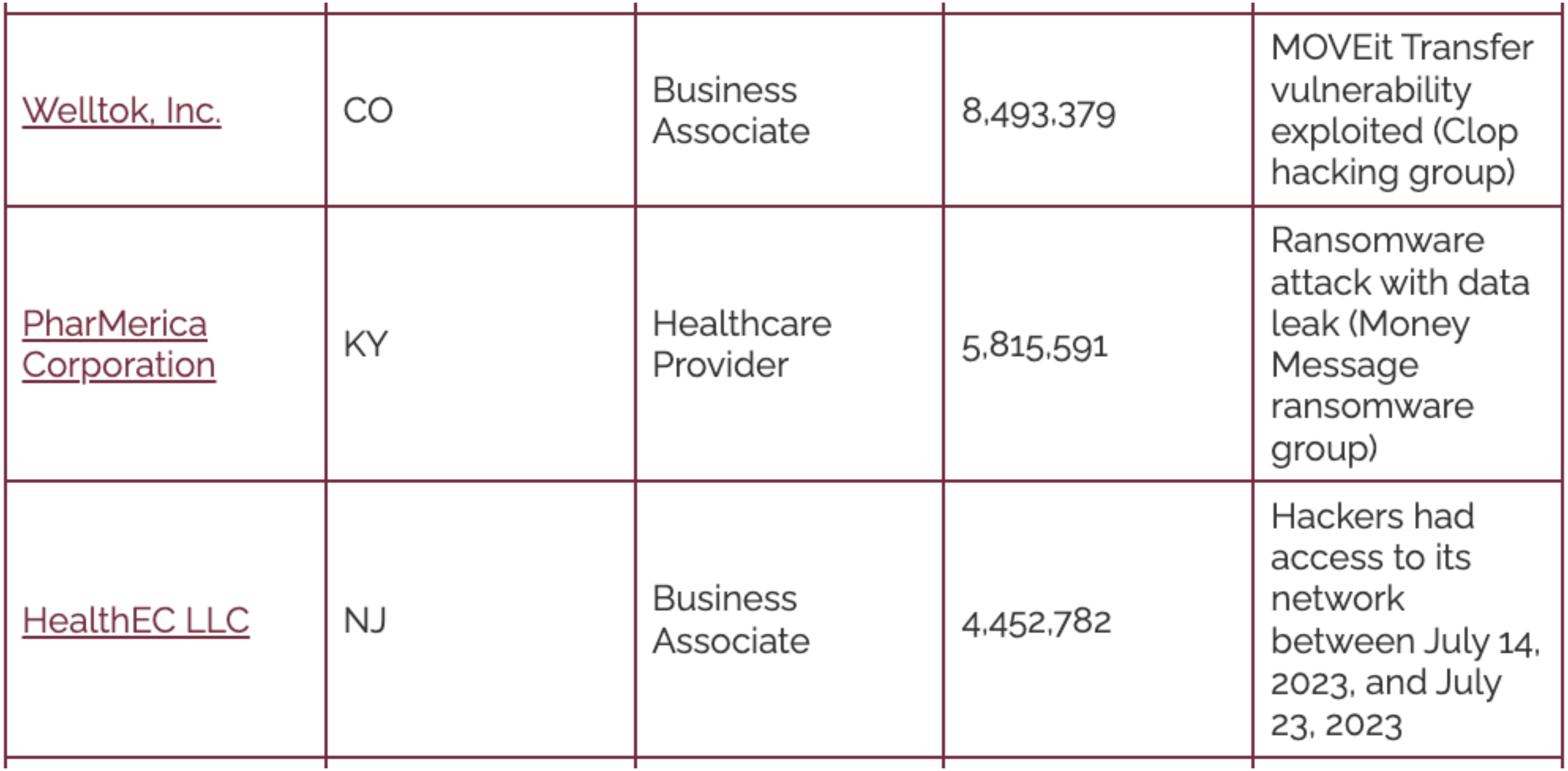


HEALTHCARE DATA BREACHES OF 500+ RECORDS
(2009 - 2023)

© 2024 The HIPAA Journal



Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Cause of Data Breach
HCA Healthcare	TN	Business Associate	11,270,000	Hackers accessed an external storage location that was used to automatically format emails
Perry Johnson & Associates, Inc., which does business as PJ&A	NV	Business Associate	8,952,212	Hackers access to its network between March 27, 2023, and May 2, 2023
Managed Care of North America (MCNA)	GA	Business Associate	8,861,076	Ransomware attack with data leak (LockBit ransomware group)

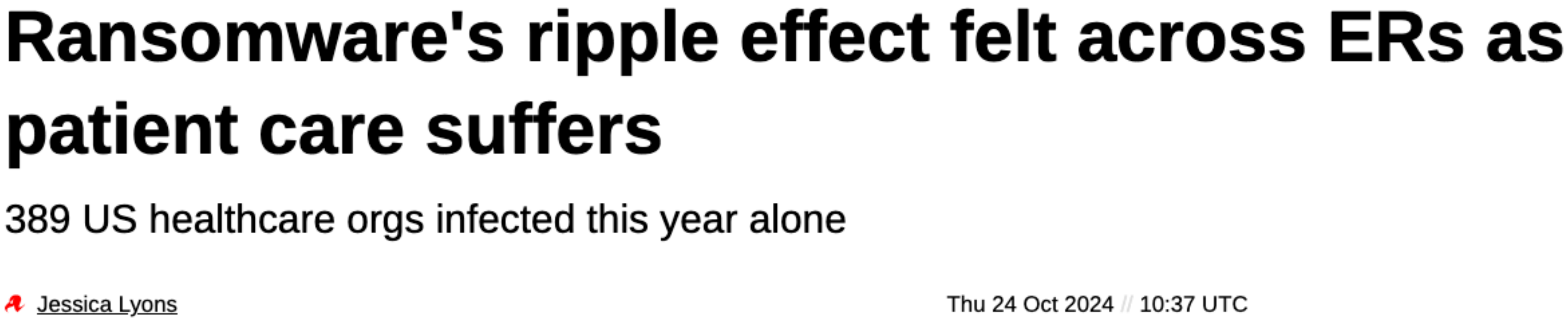


Welltok, Inc.	CO	Business Associate	8,493,379	MOVEit Transfer vulnerability exploited (Clop hacking group)
PharMerica Corporation	KY	Healthcare Provider	5,815,591	Ransomware attack with data leak (Money Message ransomware group)
HealthEC LLC	NJ	Business Associate	4,452,782	Hackers had access to its network between July 14, 2023, and July 23, 2023

Change Healthcare Cyberattack Affected 100 Million Individuals

Posted By Steve Alder on Oct 24, 2024

- The initial point of entry for the BlackCat ransomware affiliate was a server that did not have multifactor authentication enabled
- The cost of the Change Healthcare ransomware attack has risen to $2.457 billion
- Two months after the Change Healthcare ransomware attack, providers were still having difficulty verifying patients' insurance information.



Ransomware's ripple effect felt across ERs as patient care suffers

389 US healthcare orgs infected this year alone

Jessica Lyons

Thu 24 Oct 2024 // 10:37 UTC

- Average admitted payment now up to $4.4 million
- Stroke code activation at hospitals close to one suffering from a ransomware infection jumped from 59 to 103
- Cardiac arrests at a nearby hospital dealing with an infected hospital's overflow of patients increased 81 percent, from 21 cases to 38.
- Survival rates for out-of-hospital cardiac arrests with favorable neurological outcomes plummeted, from 40 percent pre-ransomware infection to 4.5 percent during the incident.

Cybersecurity Maturity

- You can't jump from zero to a mature defense system
- You must make gradual improvements
- To minimize business disruption

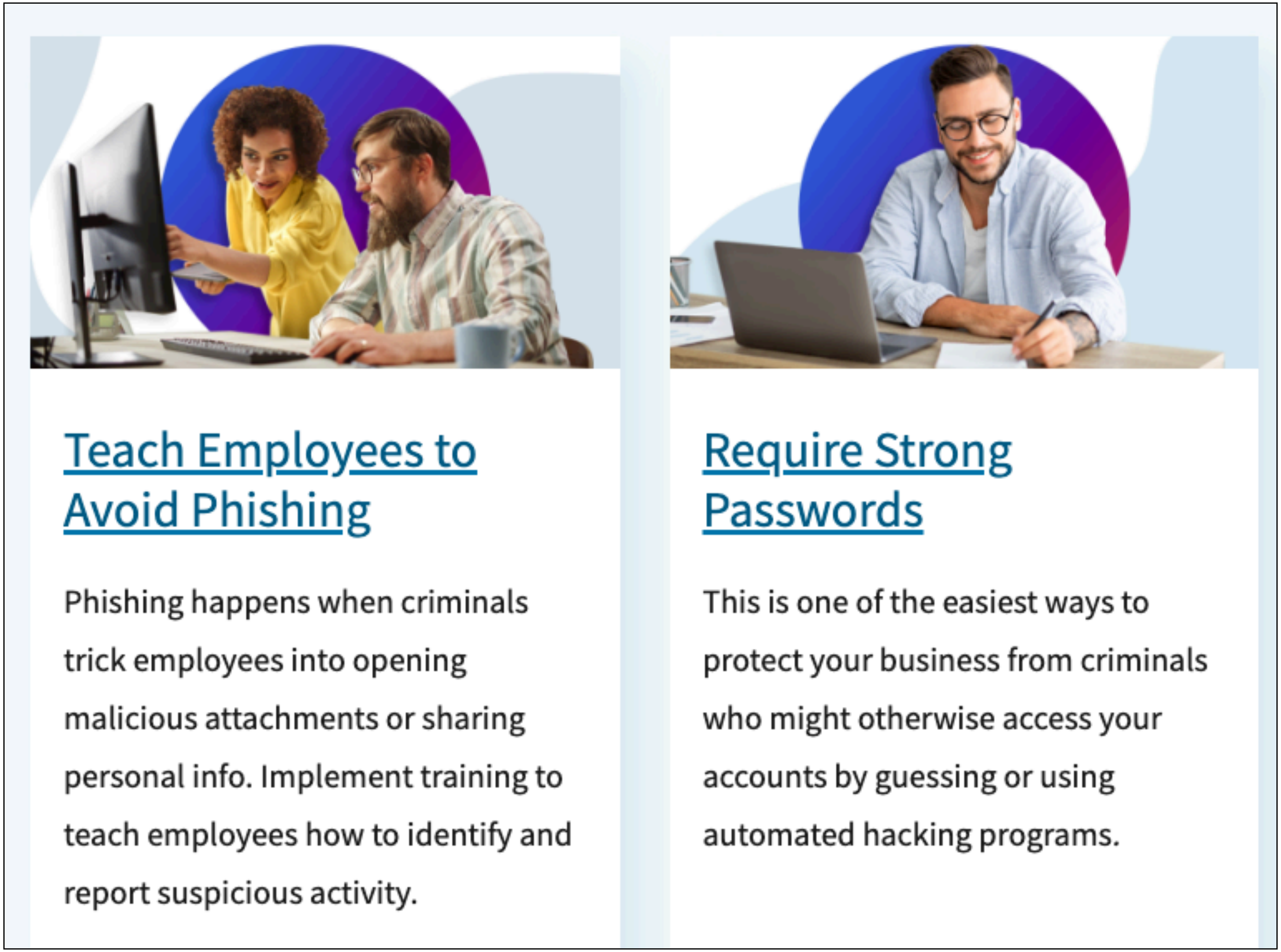
First Steps

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

https://www.cisa.gov/
secure-our-world/secure-your-business

Four Easy Ways to Protect Your Business



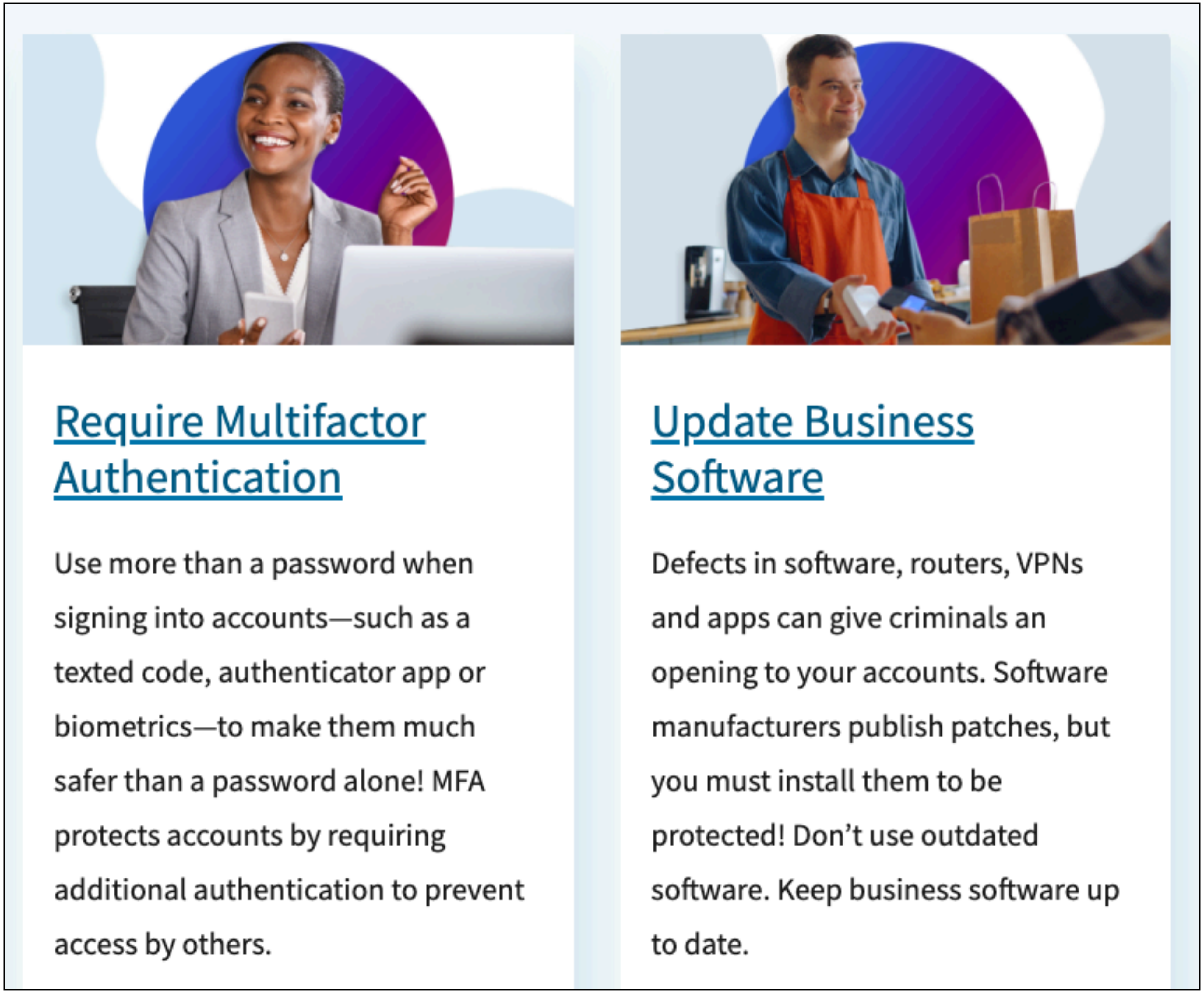
Teach Employees to Avoid Phishing

Phishing happens when criminals trick employees into opening malicious attachments or sharing personal info. Implement training to teach employees how to identify and report suspicious activity.

Require Strong Passwords

This is one of the easiest ways to protect your business from criminals who might otherwise access your accounts by guessing or using automated hacking programs.

Four Easy Ways to Protect Your Business



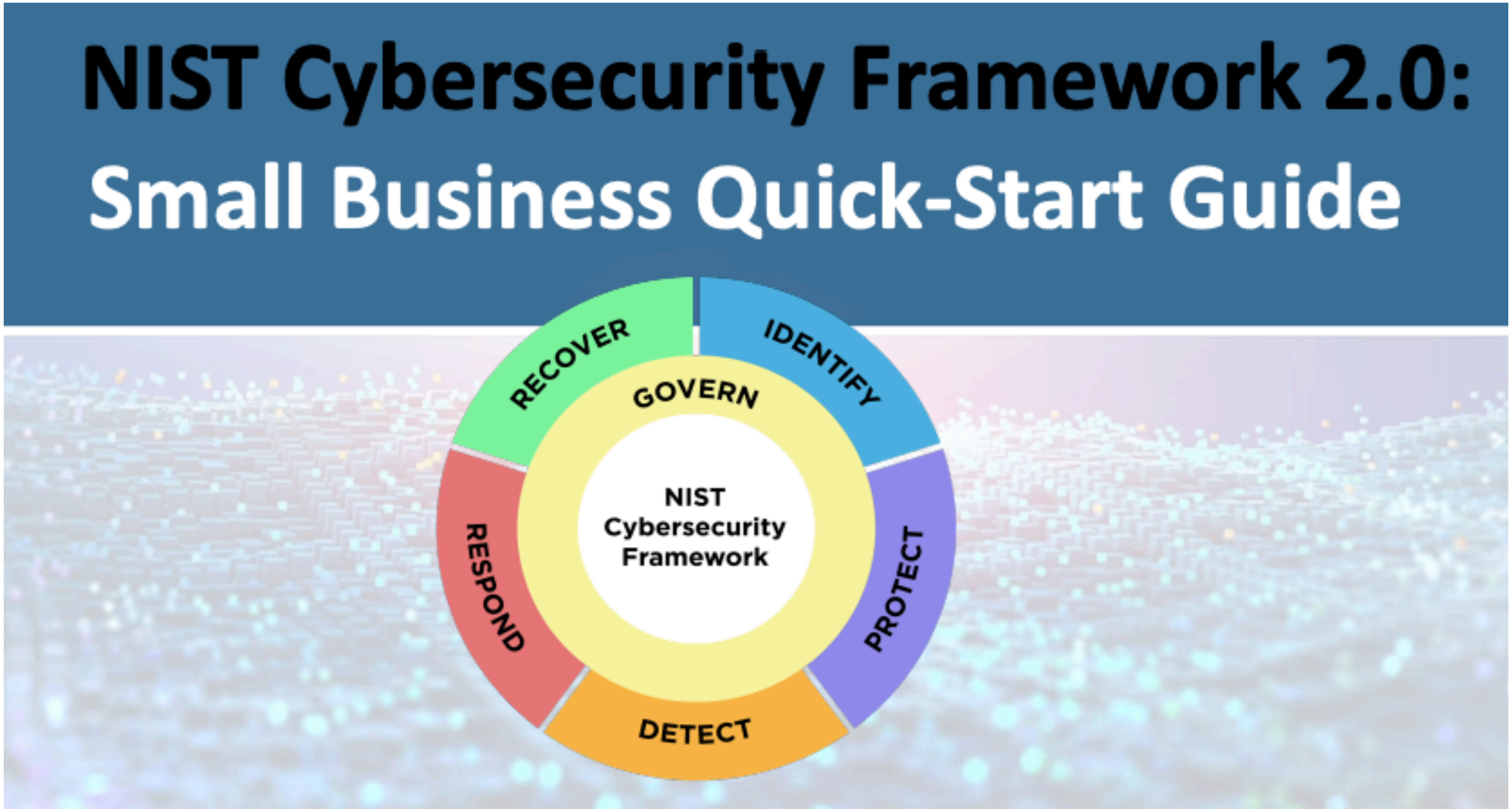
Require Multifactor Authentication

Use more than a password when signing into accounts—such as a texted code, authenticator app or biometrics—to make them much safer than a password alone! MFA protects accounts by requiring additional authentication to prevent access by others.

Update Business Software

Defects in software, routers, VPNs and apps can give criminals an opening to your accounts. Software manufacturers publish patches, but you must install them to be protected! Don't use outdated software. Keep business software up to date.

What is a cybersecurity framework?



NIST Cybersecurity Framework 2.0:

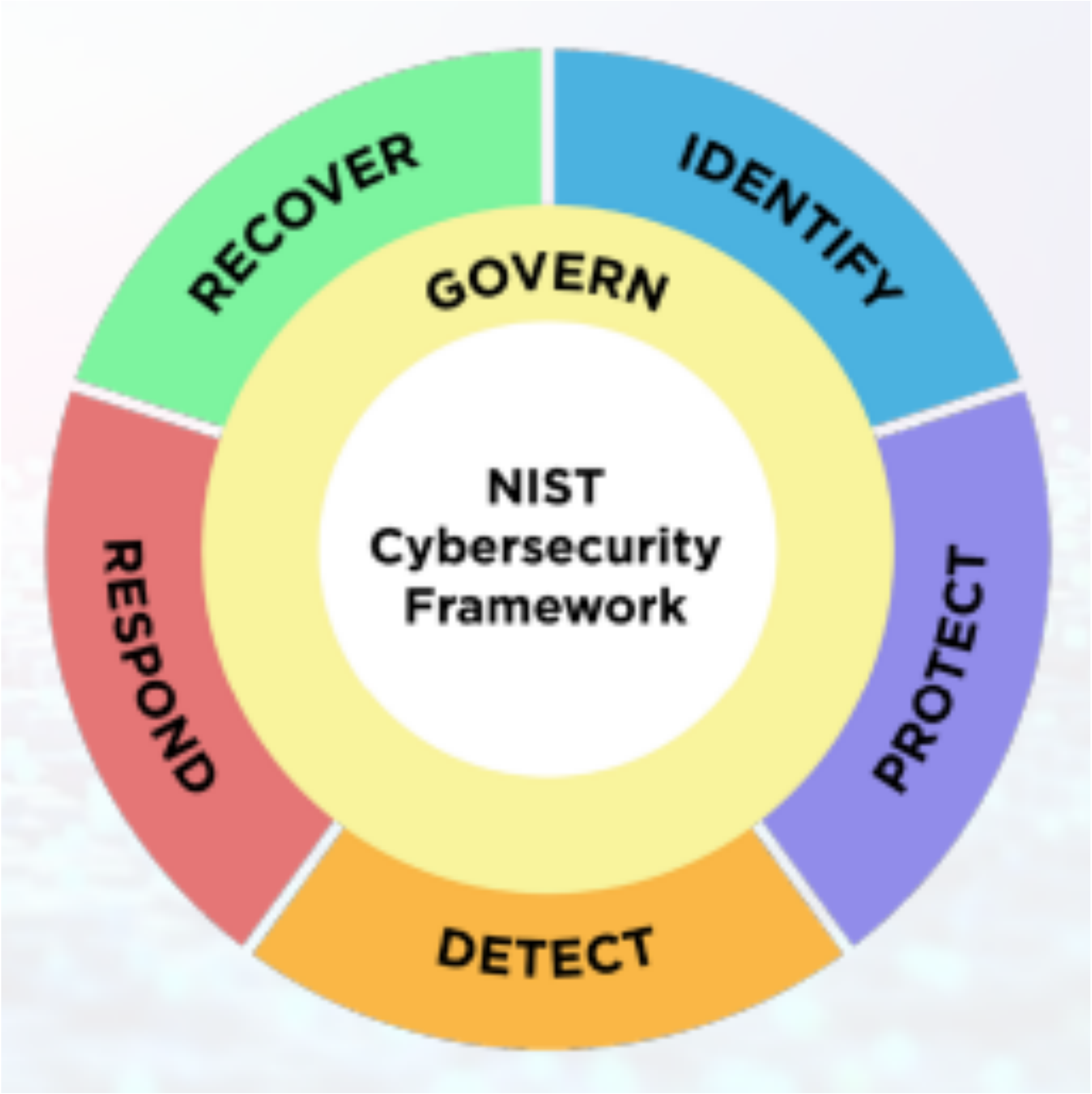
Small Business Quick-Start Guide

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf

Slides and video available at samsclass.info

Purpose

- To guide small-to-medium sized businesses
  - Who have modest or no cybersecurity plans
- To kick-start their cybersecurity risk management strategy



Govern

- Establish and monitor your business's cybersecurity risk management strategy, expectations, and policy
- Understand
    - Cybersecurity risks to your mission
    - Legal regulatory, and contractual requirements
    - Who within your business is responsible
        - For deploying and executing the cybersecurity strategy

Specific Functions

- Identify
  - Determine your current cybersecurity risks
- Protect
  - Implement safeguards to reduce the risks
- Detect
  - Find and analyze attacks and compromises

Specific Functions

- Respond
  - Contain, investigate, and eradicate after incidents
- Recover
  - Restore assets and operations to normal function

Levels of Cybersecurity Maturity

C2M2

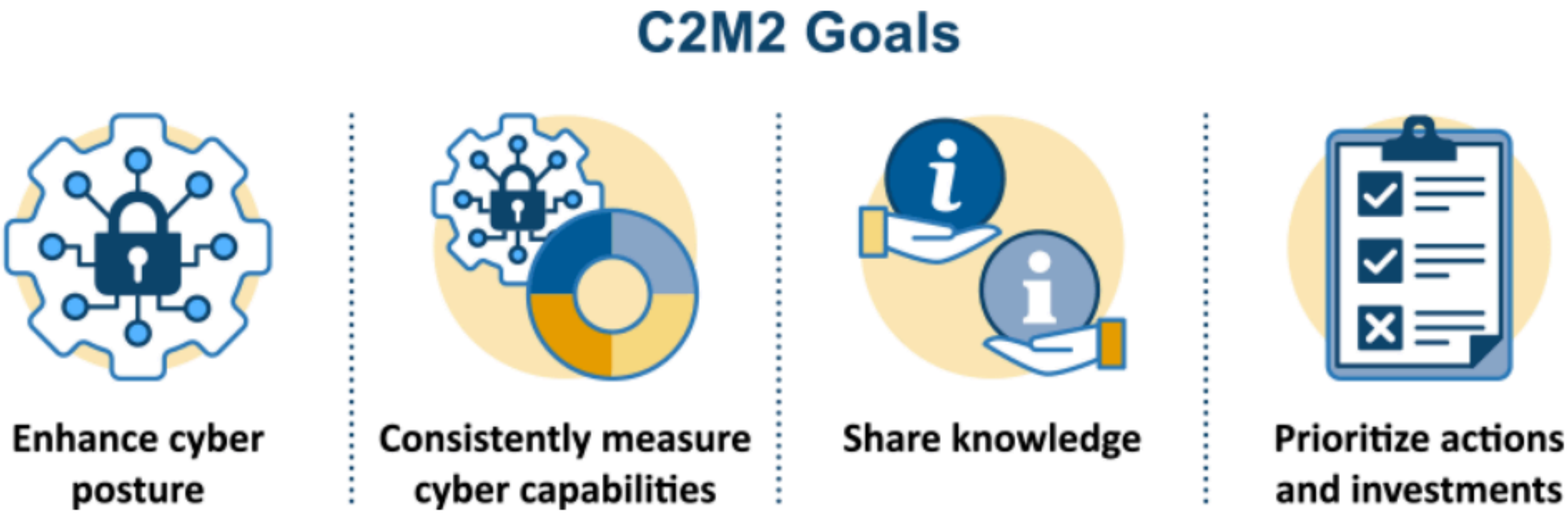
Cybersecurity Capability Maturity Model

Office of
CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

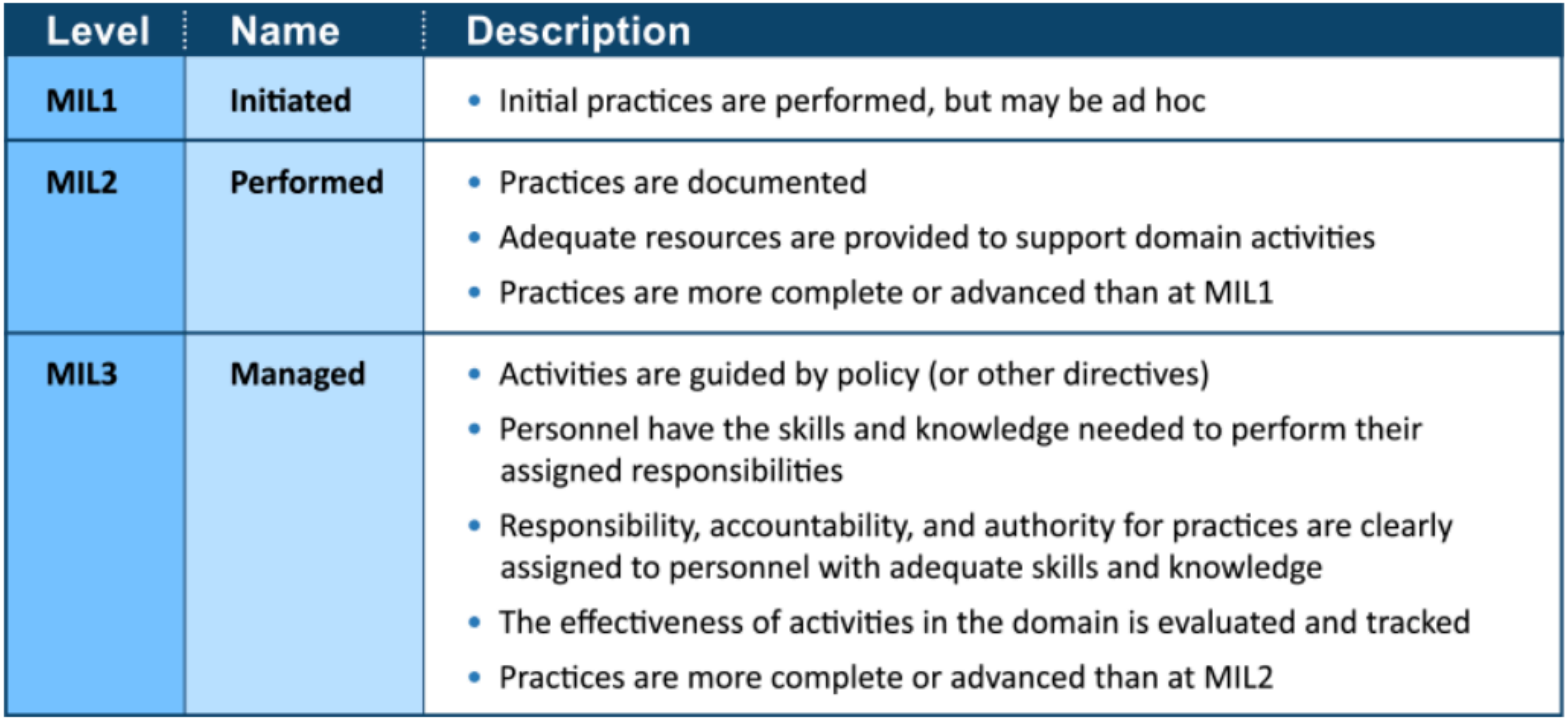
https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

A Maturity Model

- You can't jump from zero to a mature defense system
- You must make gradual improvements

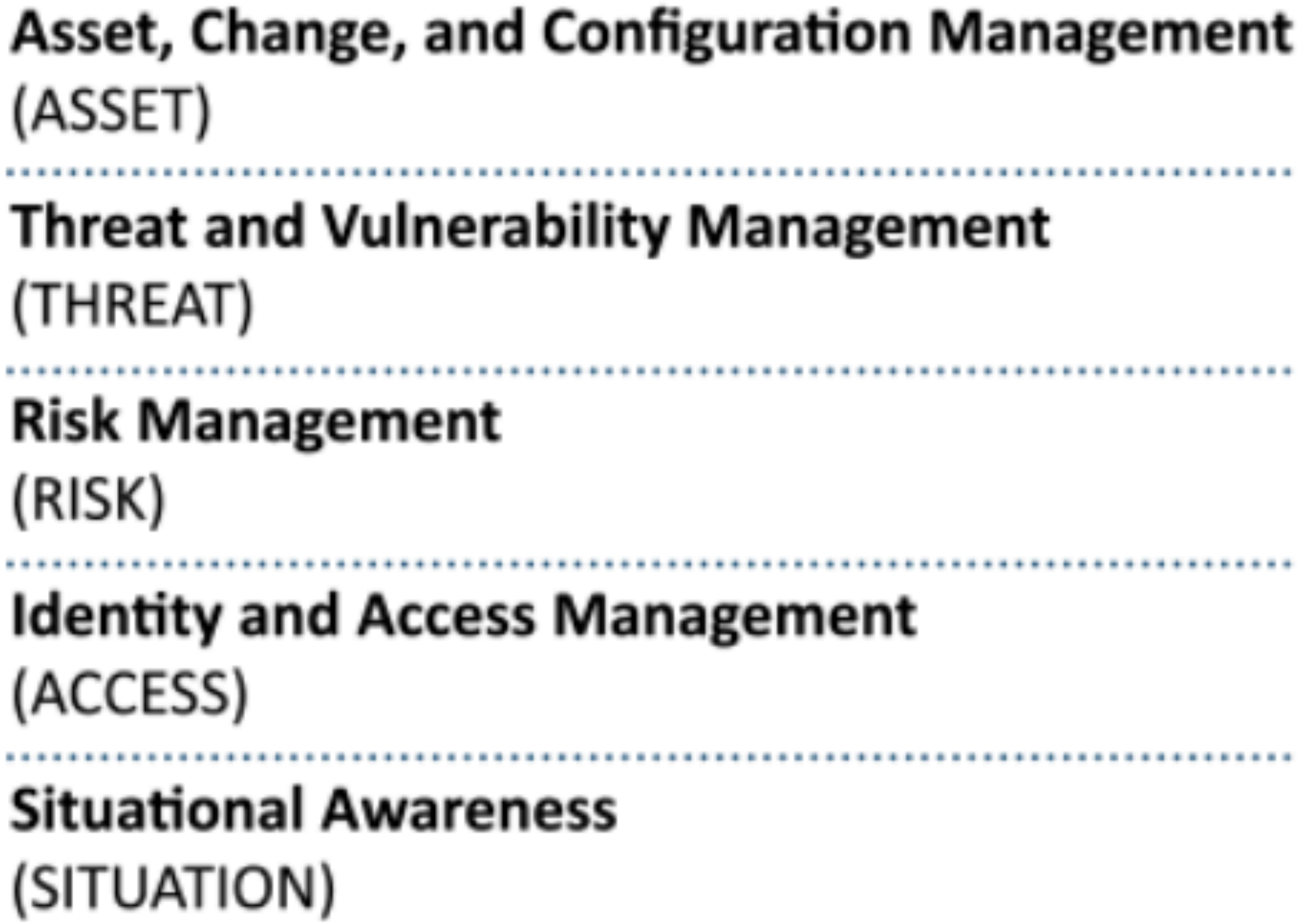

C2M2 Goals
Enhance cyber posture
Consistently measure cyber capabilities
Share knowledge
Prioritize actions and investments

Maturity Indicator Levels



Level	Name	Description
MIL1	**Initiated**	• Initial practices are performed, but may be ad hoc
MIL2	**Performed**	• Practices are documented • Adequate resources are provided to support domain activities • Practices are more complete or advanced than at MIL1
MIL3	**Managed**	• Activities are guided by policy (or other directives) • Personnel have the skills and knowledge needed to perform their assigned responsibilities • Responsibility, accountability, and authority for practices are clearly assigned to personnel with adequate skills and knowledge • The effectiveness of activities in the domain is evaluated and tracked • Practices are more complete or advanced than at MIL2

Domains



Asset, Change, and Configuration Management
(ASSET)

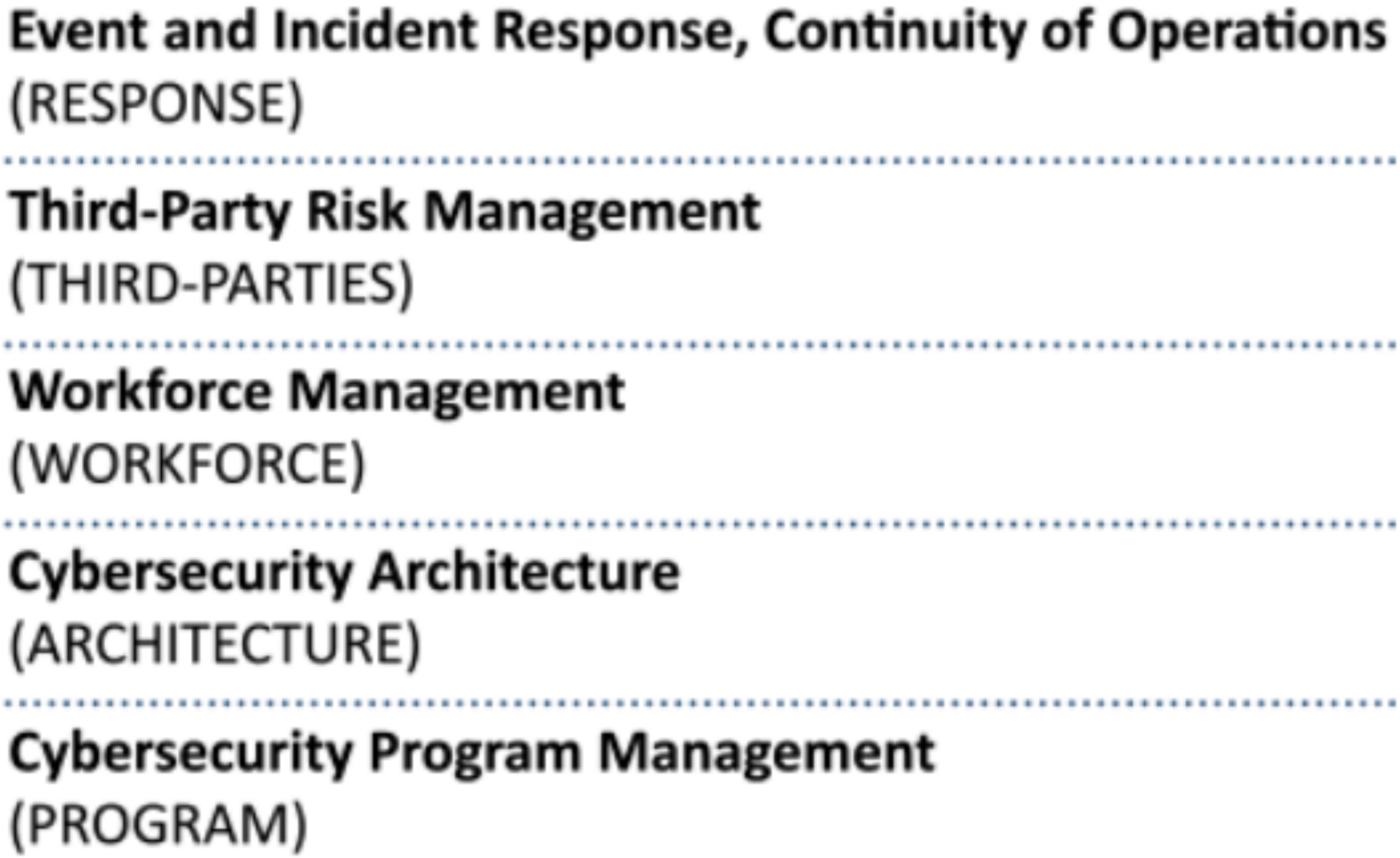
Threat and Vulnerability Management
(THREAT)

Risk Management
(RISK)

Identity and Access Management
(ACCESS)

Situational Awareness
(SITUATION)

Domains



Event and Incident Response, Continuity of Operations
(RESPONSE)

Third-Party Risk Management
(THIRD-PARTIES)

Workforce Management
(WORKFORCE)

Cybersecurity Architecture
(ARCHITECTURE)

Cybersecurity Program Management
(PROGRAM)

ASSET and THREAT

- **Asset, Change, and Configuration Management (ASSET)**
  - Manage the organization’s IT and OT assets, including both hardware and software, and information assets commensurate with the risk to critical infrastructure and organizational objectives.
- **Threat and Vulnerability Management (THREAT)**
  - Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization’s infrastructure (such as critical, IT, and operational) and organizational objectives.

RISK and ASSESS

- **Risk Management (RISK)**
  - Establish, operate, and maintain an enterprise cyber risk management program to identify, analyze, and respond to cyber risk the organization is subject to, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.
- **Identity and Access Management (ACCESS)**
  - Create and manage identities for entities that may be granted logical or physical access to the organization’s assets. Control access to the organization’s assets, commensurate with the risk to critical infrastructure and organizational objectives.

SITUATION and RESPONSE

- **Situational Awareness (SITUATION)**
  - Establish and maintain activities and technologies to collect, monitor, analyze, alarm, report, and use operational, security, and threat information, including status and summary information from the other model domains, to establish situational awareness for both the organization's operational state and cybersecurity state.
- **Event and Incident Response, Continuity of Operations (RESPONSE)**
  - Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and incidents and to sustain operations during cybersecurity incidents, commensurate with the risk to critical infrastructure and organizational objectives.

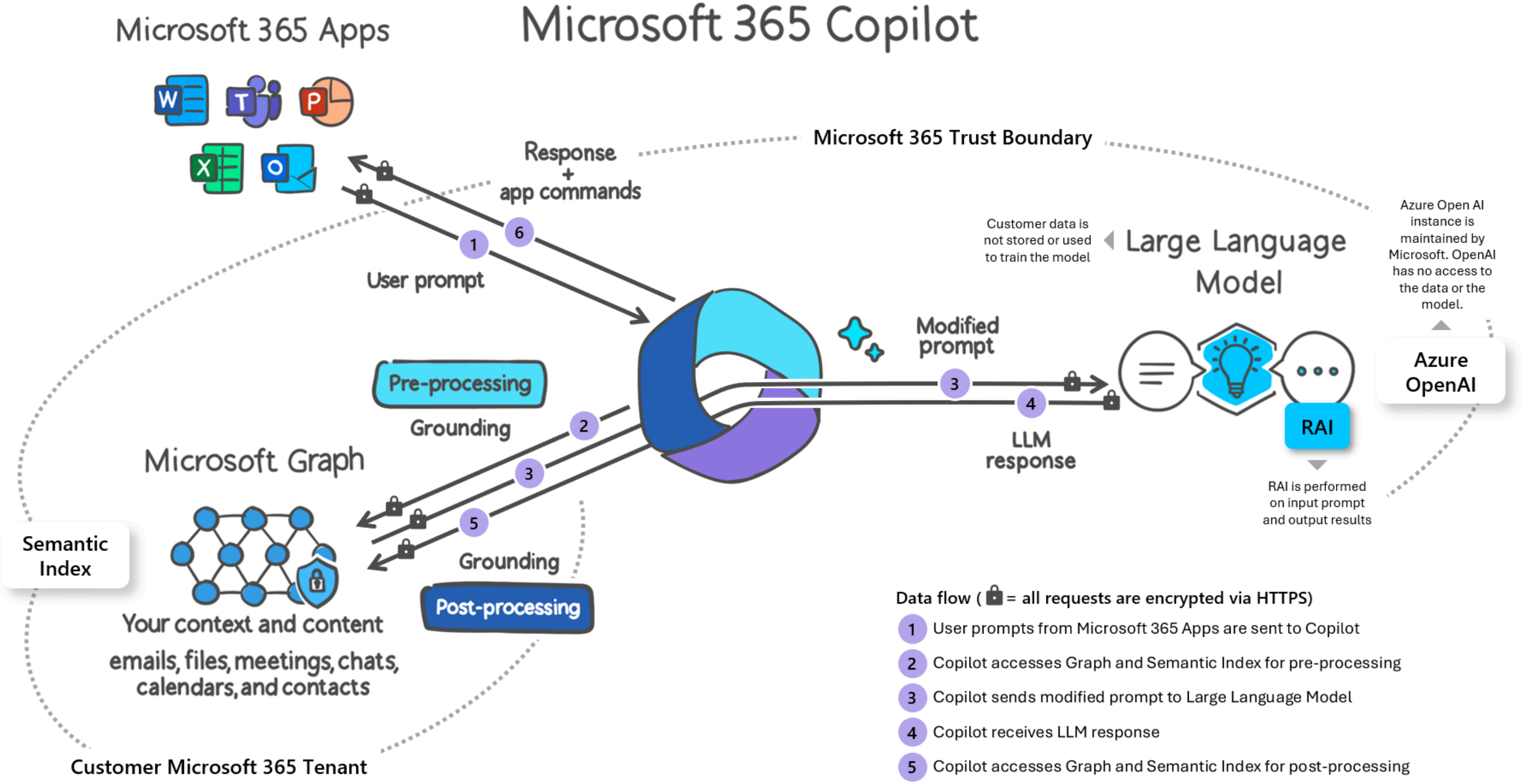
THIRD-PARTIES and WORKFORCE

- **Third-Party Risk Management (THIRD-PARTIES)**
  - Establish and maintain controls to manage the cyber risks arising from suppliers and other third parties, commensurate with the risk to critical infrastructure and organizational objectives.
- **Workforce Management (WORKFORCE)**
  - Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.

ARCHITECTURE and PROGRAM

- **Cybersecurity Architecture (ARCHITECTURE)**
  - Establish and maintain the structure and behavior of the organization’s cybersecurity architecture, including controls, processes, technologies, and other elements, commensurate with the risk to critical infrastructure and organizational objectives.
- **Cybersecurity Program Management (PROGRAM)**
  - Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization’s cybersecurity activities in a manner that aligns cybersecurity objectives with both the organization’s strategic objectives and the risk to critical infrastructure.

Microsoft 365 Copilot



Data flow (🔒 = all requests are encrypted via HTTPS)

1 User prompts from Microsoft 365 Apps are sent to Copilot

2 Copilot accesses Graph and Semantic Index for pre-processing

3 Copilot sends modified prompt to Large Language Model

4 Copilot receives LLM response

5 Copilot accesses Graph and Semantic Index for post-processing

6 Copilot sends the response, and app command back to Microsoft 365 Apps

Q & A

Slides and video available at samsclass.info

Sources

- Gina M. Raimondo and Laurie E. Locascio, NIST Special Publication 1300: NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide (2024)
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf
- CISA: Secure Your Business (2024)
  - https://www.cisa.gov/secure-our-world/secure-your-business
- Cybersecurity Capability Maturity Model (C2M2) from the U.S. Department ot Energy (2022)
  - https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

Sources

- Security Breaches in Healthcare in 2023
  - https://www.hipaajournal.com/security-breaches-in-healthcare/
- Change Healthcare Cyberattack Affected 100 Million Individuals
  - https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/
- Ransomware's ripple effect felt across ERs as patient care suffers
  - https://www.theregister.com/2024/10/24/ransomware_ripple_effect_hospitals/

Sources

- About C2M2
  - https://c2m2.doe.gov/about