

Future-Proofing Your Business: Cybersecurity Strategies for 2025 & Beyond

WEBINAR



AGENDA

- **Welcome and Introductions**
- **About Iviry**
- **The Importance of Cybersecurity Awareness Month**
- **Why Proactive Security is Crucial**
- **Key Insights from the Latest Cybercrime Trends**
- **Actionable Strategies to Defend Against Cyber Threats Going Into 2025**
- **15-Minute Q&A**



LOGISTICS

- This is an interactive 1-hour Webinar Session.
- We will be presenting polls throughout the webinar – feel free to engage!
- A moderator is present on the session monitoring the Q&A chat box.
- This is a recorded session that will be emailed to all attendee's post-webinar and will also be posted to our website.
- The presentation will be emailed to all attendee's and those who couldn't make it.

SPEAKER INTRODUCTION



Adam Kangiser
Compliance Analyst
Iviry, LLC

About:

Adam is a Certified CMMC Registered Practitioner (RP), Network+, with a Master's Degree in Computer Science. With a strong foundation in network security, he brings a wealth of knowledge and expertise to the field of cybersecurity compliance and risk management.

Passionate about helping organizations achieve and maintain CMMC standards, he is dedicated to guiding businesses through the complexities of cybersecurity best practices. Adam understands that each business is unique, and while the standards remain the same, the approach to achieving cybersecurity compliance must fit the specific needs of individual companies.

SPEAKER INTRODUCTION



Randy Delarm
Chief Growth Officer
Iviry, LLC

About:

Randy Delarm is the Chief Growth Officer at Iviry, where he is passionate about helping organizations navigate complex cybersecurity requirements and implement robust security postures that align with DoD standards, such as the Cybersecurity Maturity Model Certification (CMMC).

His 37-year civil service career underscores his deep expertise in defense IT. With an in-depth understanding of the challenges faced by defense contractors, he plays a pivotal role in Iviry's mission to safeguard sensitive information and ensure compliance with federal regulations.

ABOUT IVIRY



- **Defense Industrial Base Focus.**
 - We know the industry and what you're dealing with
- **Global and austere environments.**
 - On Ship.
 - Hardship Areas
 - Combat Zones.
- **International presence.**
- **Path to execute Classified work.**
- **Cultural Fit: We are Veterans.**
- **Cyber-Accreditation Body.**
 - Registered Provider Organization.
 - Training and Certs (RP/Provisional Assessor).

OUR VALUE

1. Data Assurance.

Maintain the Confidentiality, Integrity, and Availability of your data.

2. Security.

Protect your organization and data from exposure to unauthorized access due to an attack, data breach or insider threat.

3. Technology Performance.

Keep your Business Systems & Information Technology functioning efficiently.

5. Compliance.

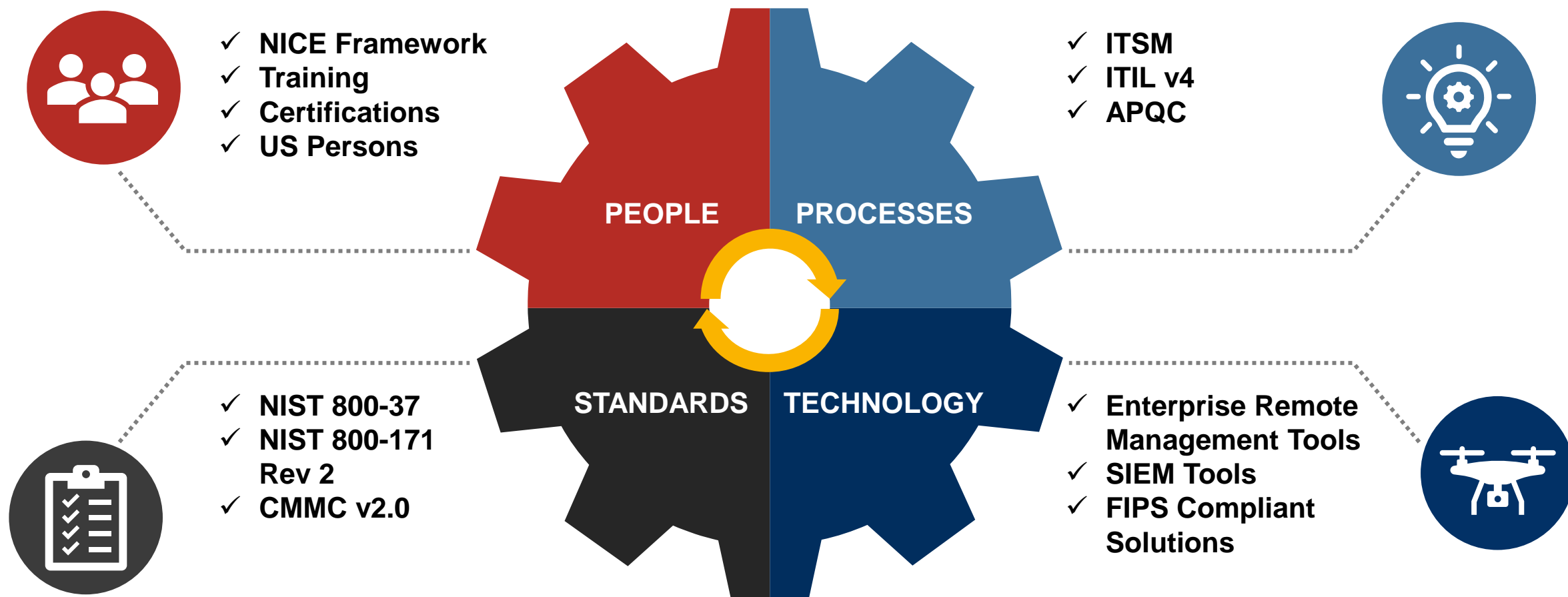
Keep your company compliant with NIST 800-171 standards.

4. Major Incident Response.

Resolve unplanned incidents (natural, cyber) and restore your technology quickly.

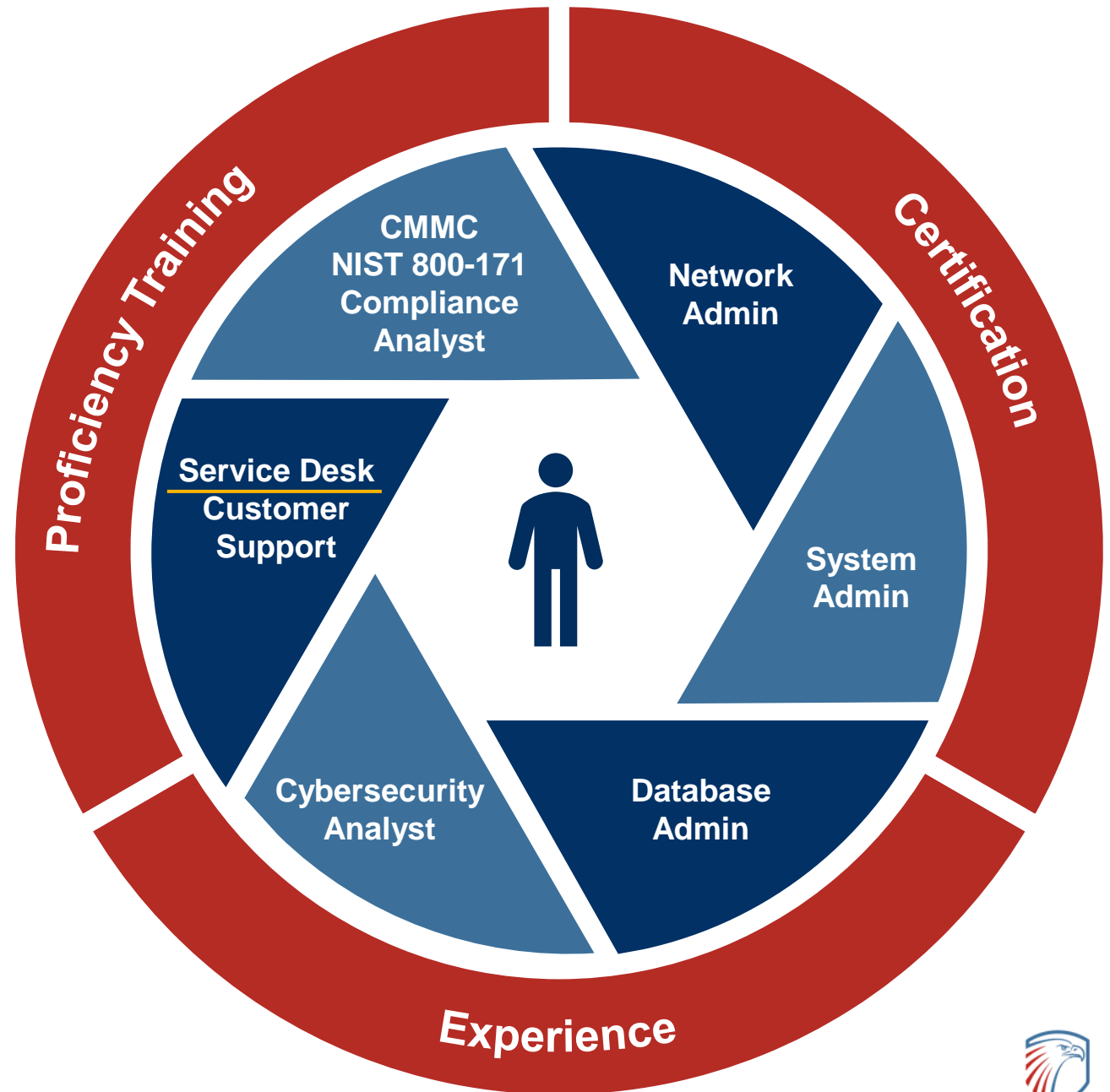


SOLID FOUNDATION



Iviry's Edge:

**Skilled Teams
Strategic Success**



THREATS



Risk Assessment: Consequence vs Likelihood



Cybersecurity Awareness: Defending Against Evolving Threats

Objectives of the Webinar

Importance of Cybersecurity Awareness Month

Cybersecurity Awareness Month highlights the crucial need for **proactive** security measures as cyber threats continue to evolve and pose significant risks to businesses and individuals.

Key Insights from FBI IC3 Report

The latest FBI IC3 Report provides valuable insights into the latest cybercrime trends, including ransomware attacks, business email compromises, and financial fraud, enabling organizations to better prepare and defend against these threats.

Building a Top-Down Cybersecurity Culture

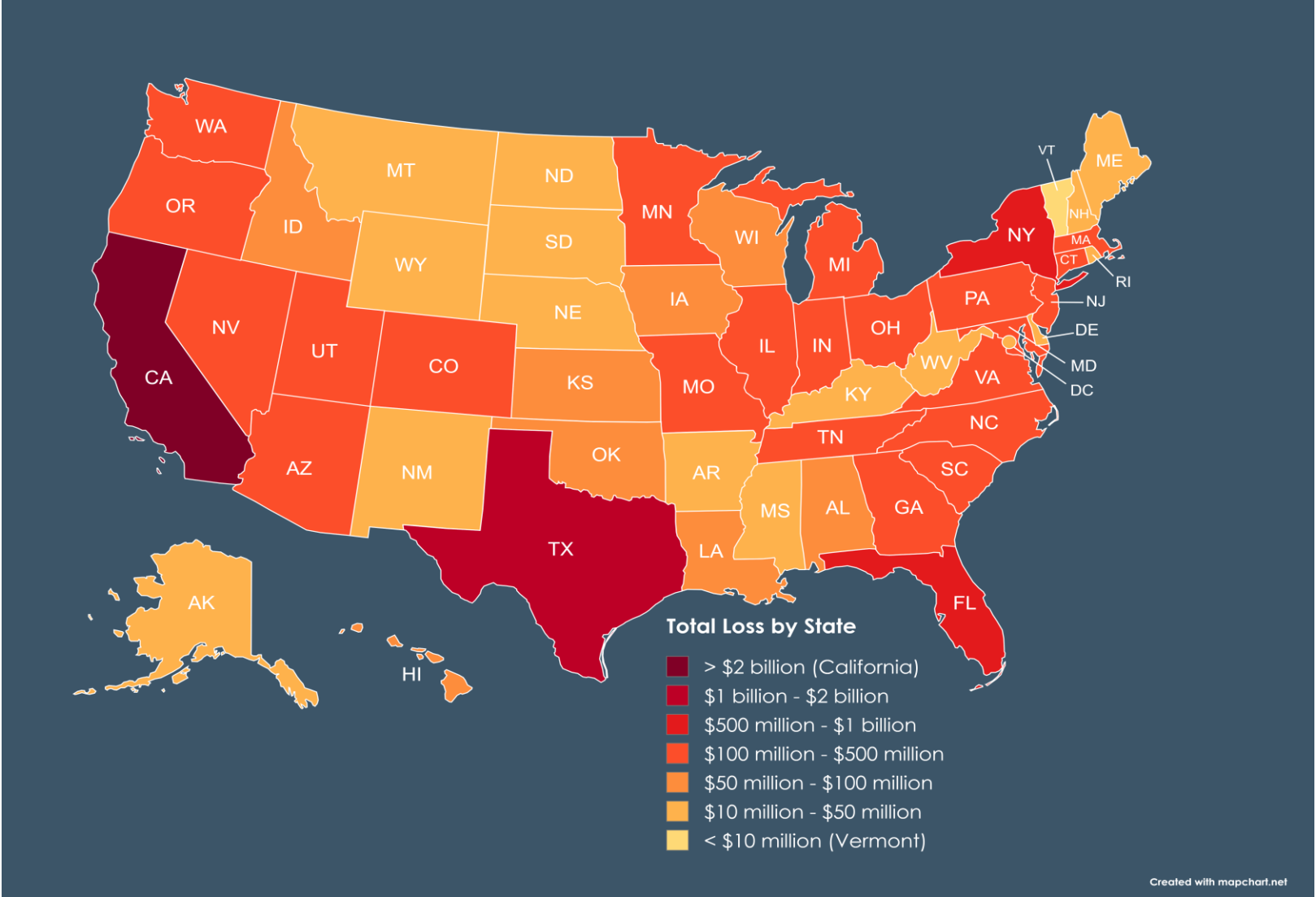
Leadership's role in driving cybersecurity initiatives and ensuring compliance with CMMC standards is crucial to protecting your business.

Actionable Strategies for 2025

Implementing robust cybersecurity strategies, such as multi-factor authentication, employee security training, and regular software updates, can help businesses effectively defend against cyber threats in the years to come.

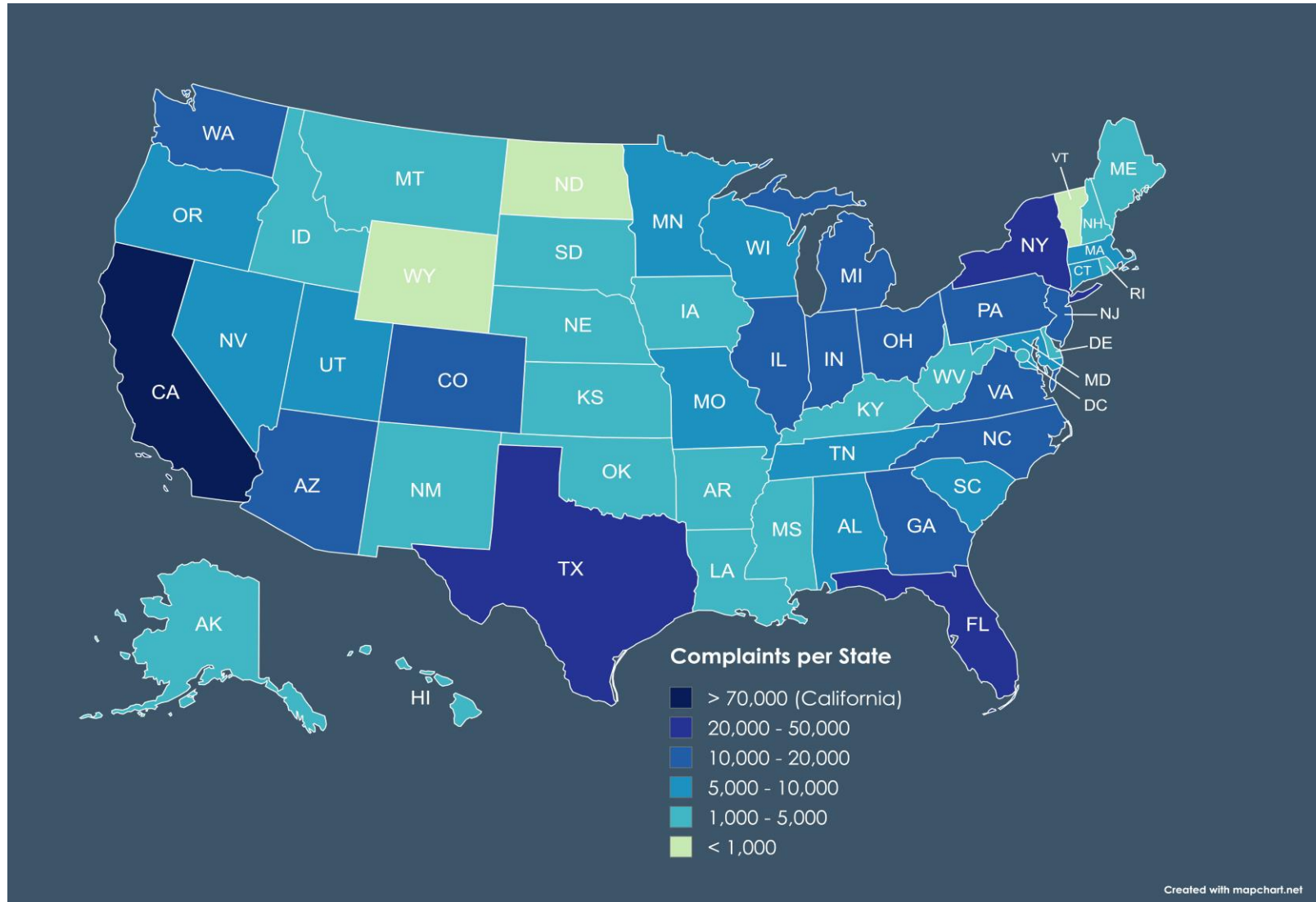
The Financial Impact of Cybercrime

By the Numbers of 2023



Cybercrime Complaints Impacting Financial Loss

By the Numbers of 2023



Evolving Cyber Threat Landscape

● 2016

Business email compromise (BEC) scams result in over \$3 billion in losses for U.S. companies

● 2017

Widespread ransomware attacks, such as WannaCry and NotPetya, cause significant disruptions globally

● 2018

Exponential growth in cryptocurrency-enabled crimes, including crypto jacking and cryptomining malware

● 2019

Emergence of new threat vectors such as Internet of Things (IoT) device vulnerabilities and supply chain attacks

● 2020

Rise in online shopping scams and tech support fraud as more people rely on digital services during the pandemic

● 2021

Increase in phishing attacks, with criminals leveraging COVID-19 pandemic to prey on fears and uncertainty

● 2022

Cybercriminals exploit remote work vulnerabilities and target critical infrastructure sectors

● 2023

The FBI received a 10% increase in cybercrime complaints, representing a 22% increase in cybercrime losses.

**Source: FBI IC3 Reports*



POLL QUESTION

What do you consider to be the biggest vulnerability in your organization?



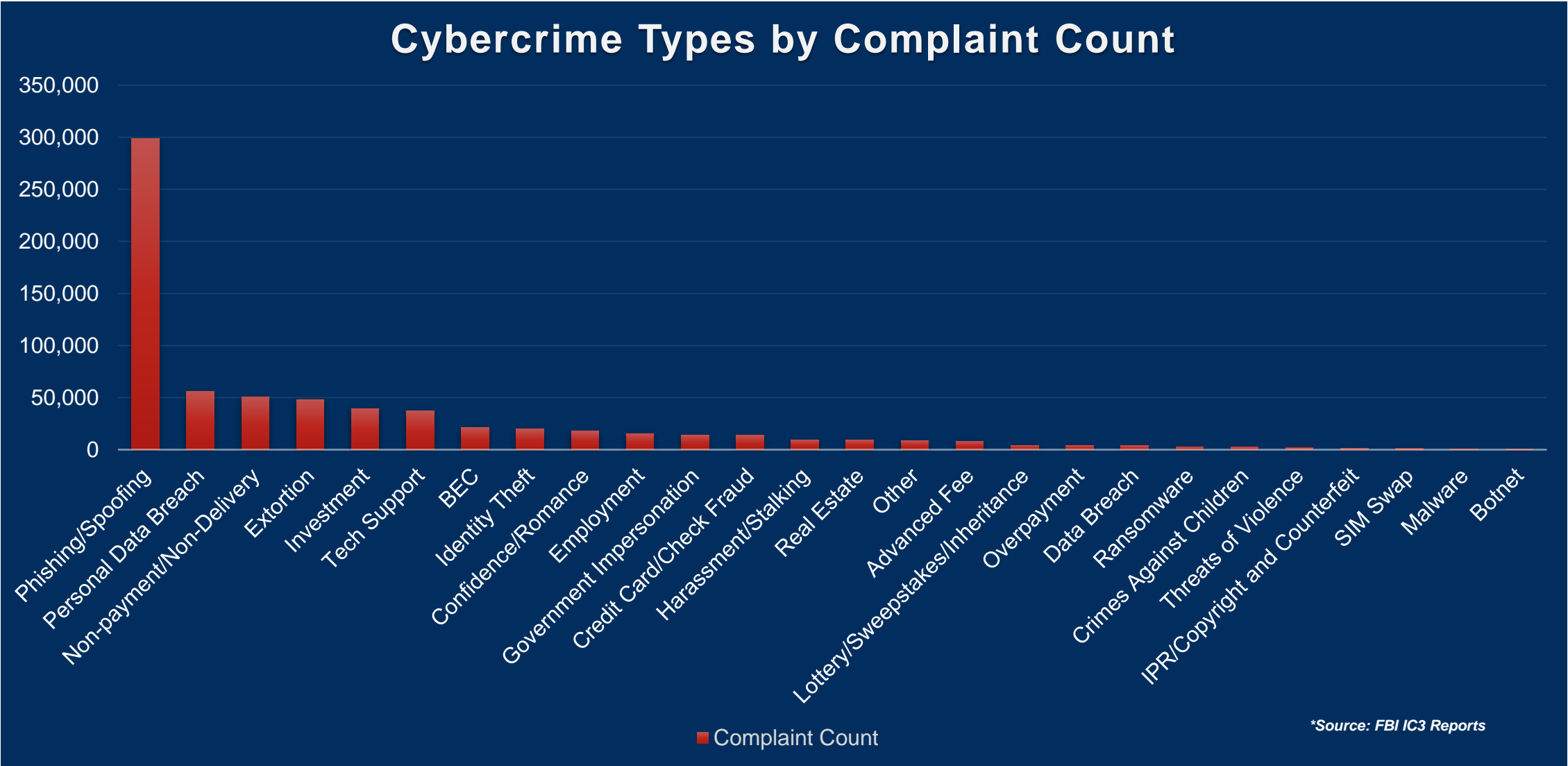
POLL QUESTION

How confident are you in your organization's ability to defend against phishing and social engineering attacks?



Phishing/Spoofing

By the Numbers

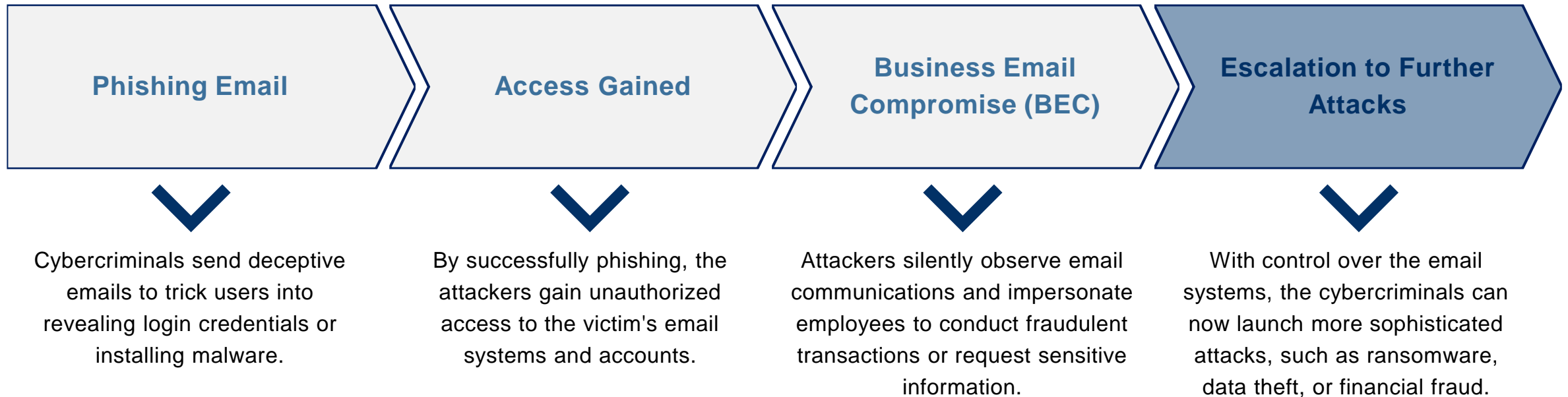


Phishing and Social Engineering

Preventing the Biggest Threat

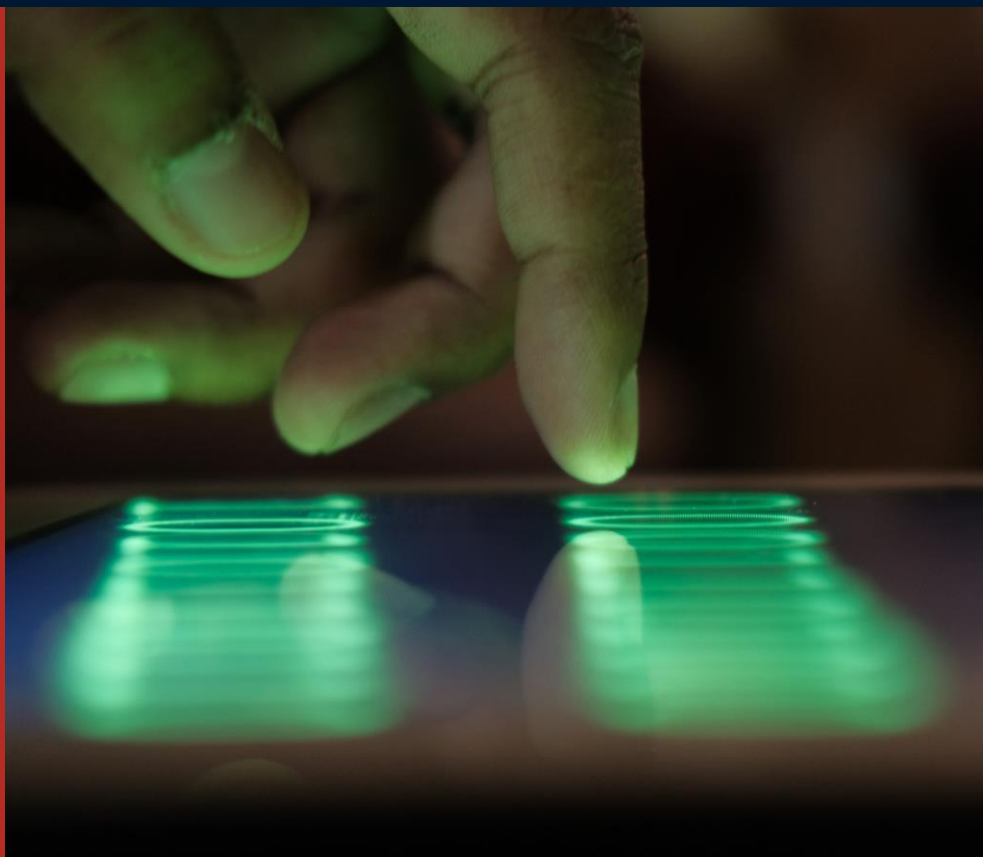
66% Rise in Phishing Attacks

This staggering number highlights how easily human error can be exploited, even in the most secure systems! Phishing is often the first step in a cyberattack, allowing attackers to gain access by stealing login credentials through deceptive tactics like social engineering.



Example of a Phishing Email

What to Look For



From: MSteam-Outlook Message Center <no-reply@office365protectionservices.co.uk>

Sent: 19 September 2018 11:44

To: Bob Smith <Bob.Smith@Company.com>

Subject: Account Verification

 **Fake domain**

This mail is from a trusted sender.



 **Threat**

We're having trouble verifying your Office365 account: Bob.Smith@Company.com on our server, most features will be turned off.

To help prevent account malfunctions, please log into your account portal to verify your account.

 **Spelling mistakes**

[SIGN IN TO MICROSOFT ACCOUNT PORTAL](#)

Note : Outlook will automatically fix your account after this process on the microsoft server and all account features will be turned back on

Thanks for using office365 , we hope to continue serving you.

Microsoft Corporation
One-Microsoft Way Redmond
WA, 98052

 **Grammatical errors**

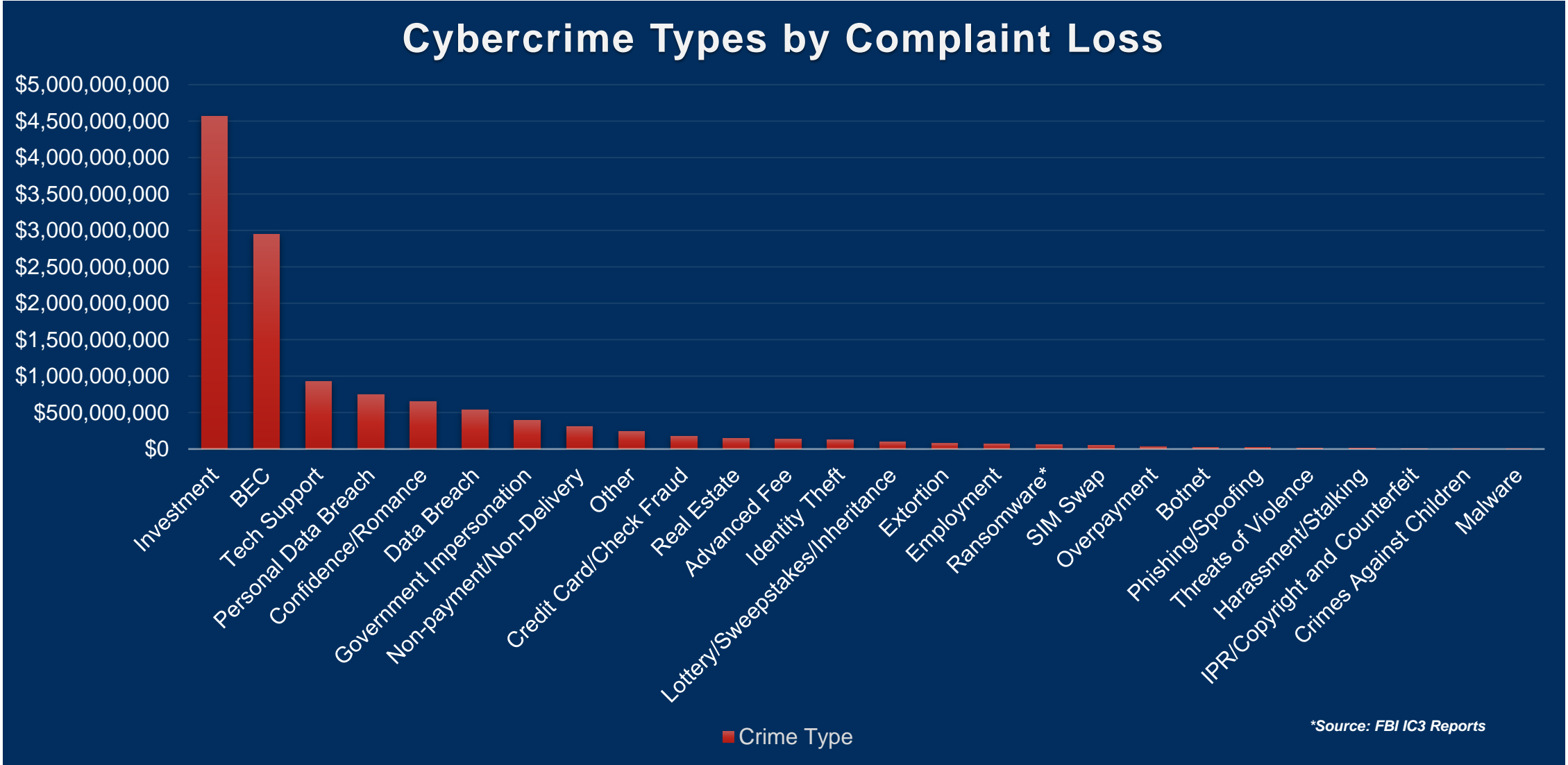
All Right Reserved | Acceptable Use Policy | Privacy Notice

 **Fake email signature**



Business Email Compromise

The 2nd Most Costly Cyber Threat



Business Email Compromise (BEC)

A Gateway to Ransomware

1 Compromise of Account

2 Monetization Methods

3 Data Exfiltration



Ransomware Threats



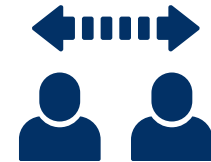
Ransomware Attacks on the Rise

Ransomware incidents have been increasing, with over **2,825** complaints in 2023.



Critical Infrastructure Sectors Targeted

Attackers are specifically targeting critical infrastructure sectors, which can have severe consequences for public safety and national security.



Attackers Use Multiple Variants

Ransomware attackers are employing a variety of malware variants to pressure businesses into paying ransom demands.

Ransomware remains a persistent and evolving threat, with attackers becoming more sophisticated in their tactics. Businesses and organizations must remain vigilant and implement robust cybersecurity measures to protect against these attacks.

POLL QUESTION


Does your organization have a disaster recovery plan and incident response plan that has been tested in the last year?



Best Practices for Ransomware Defense

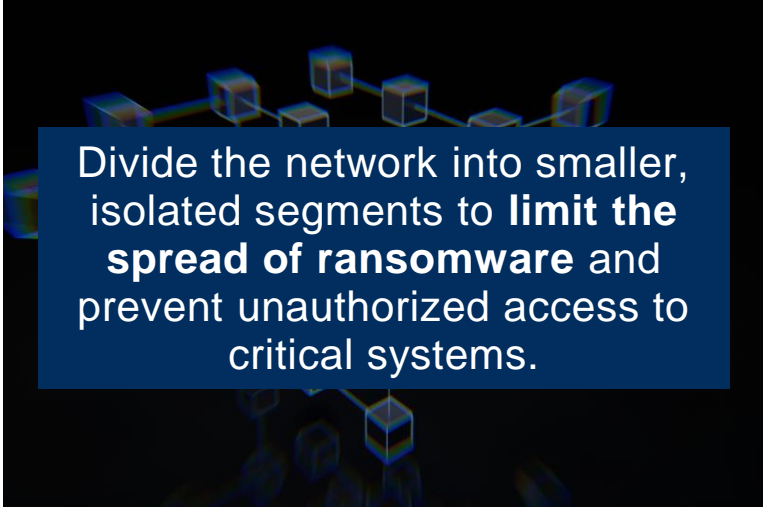
Risk Reduction and Continuity

Regular Software Updates




Ensure all software and systems are kept **up-to-date** with the latest security patches and bug fixes to address known vulnerabilities.

Network Segmentation



Divide the network into smaller, isolated segments to **limit the spread of ransomware** and prevent unauthorized access to critical systems.

Data Backup Strategies



Implement a **robust backup plan** that includes regular, secure, and off-site backups of all important data to minimize the impact of a ransomware attack.

Incident Response Plan

How to React Effectively

Importance of Incident Response

Having a well-defined incident response plan is crucial to minimizing the damage caused by cyberattacks.

What is Incident Response?

Your organization's immediate action plan when a cyberattack or other security breach occurs. Whether it's a phishing attack, ransomware, insider threat, or physical breach, quick detection and containment are critical.

Incident Response Process

The incident response process involves isolating affected systems early and communicating effectively, allowing businesses to limit the damage and take the first step toward recovery.

When to Use Incident Response

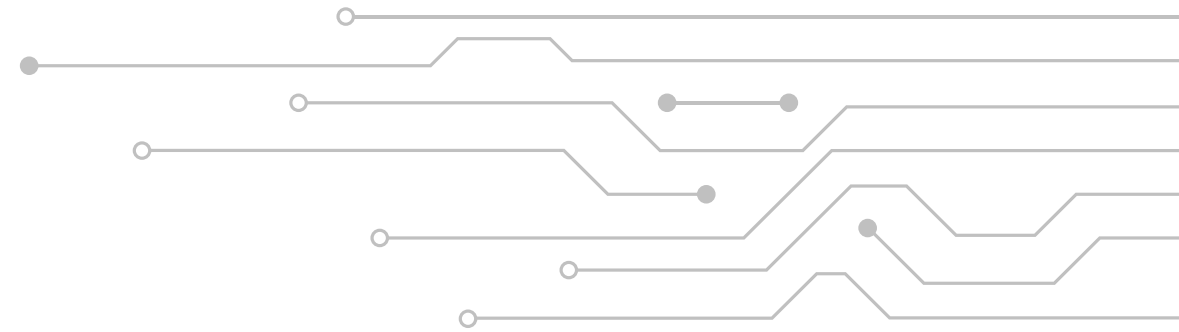
Incident response is used in response to various security incidents, including cyberattacks (like phishing, ransomware), insider threats, and physical security breaches.

Steps of Incident Response

- 1) Identify and Detect:** Recognize unusual activity
- 2) Contain and Eradicate:** Isolate affected systems to prevent further damage
- 3) Respond and Notify:** Communicate internally and externally to handle the situation effectively.

Business Continuity

Ensuring Operational Stability



Continuity Planning

Developing a comprehensive business continuity plan to identify critical functions and establish alternative processes to maintain operations during disruptions.



Communication Protocols

Establishing clear communication plans to keep employees, customers, and stakeholders informed during disruptions, ensuring a smooth transition and minimizing operational impact.



Vendor Relationships

Evaluating and managing third-party vendor relationships to ensure the reliability and resilience of the supply chain, reducing the risk of disruptions.



Operational Resilience

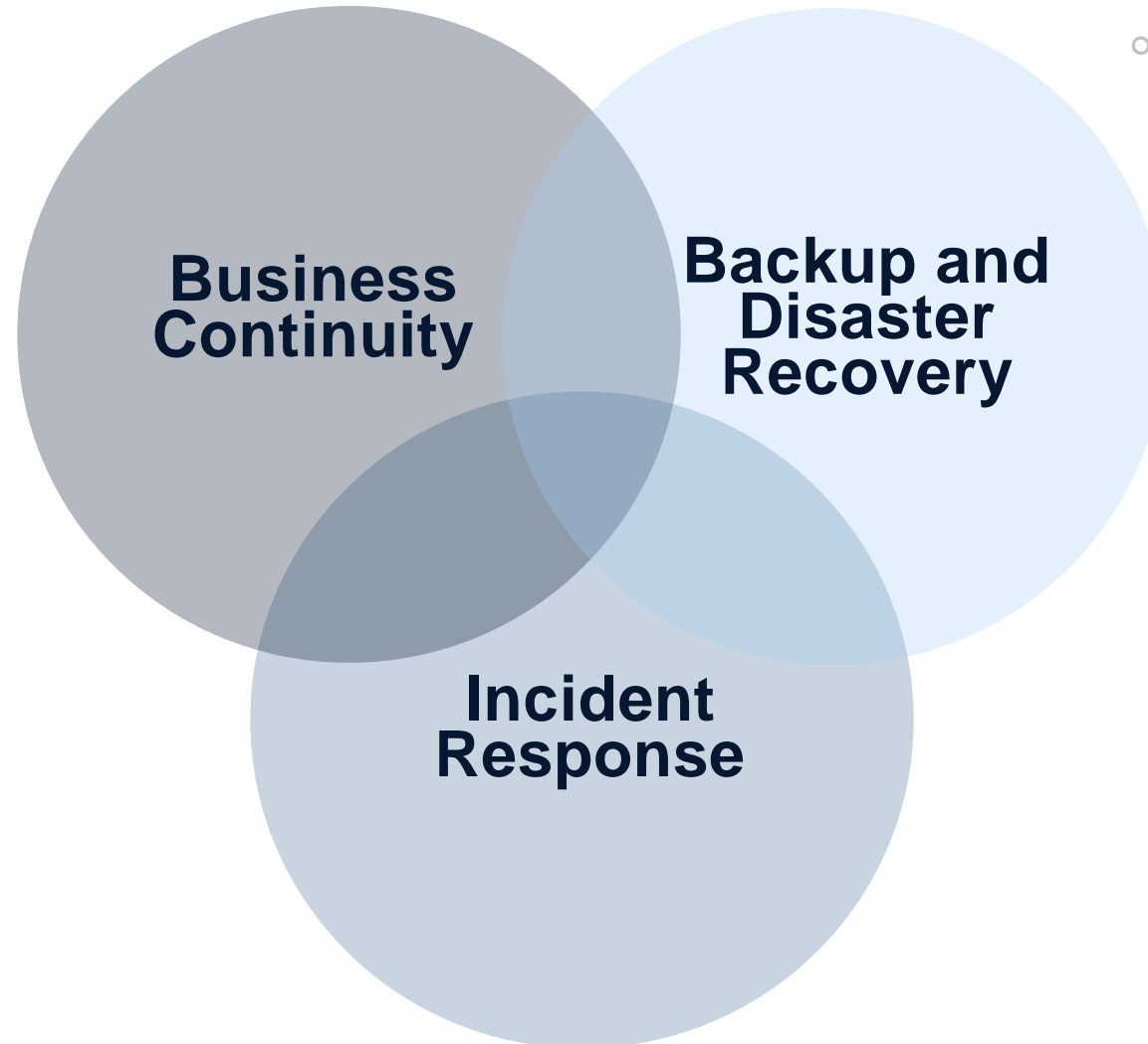
Fostering a culture of operational resilience within the organization, empowering teams to adapt and respond effectively to various crisis scenarios.



Disaster Recovery

Implementing robust disaster recovery strategies to restore essential systems and data in the event of natural disasters, cyberattacks, or other unexpected events.

Integrating Incident Response, Business Continuity, & BDR



POLL QUESTION

Does your leadership team actively promote cybersecurity training and awareness programs?



Creating a Culture of Compliance

Approximately **95%**
of cyber breaches
are caused by
human error.

✓ Set the Tone From The Top

Leadership commitment is essential - Senior Executives must establish and actively promote a cybersecurity-focused culture.

✓ Engage Employees from the Start

Empower middle-management leaders by actively engaging them to carry this message to their staff, emphasizing the importance of compliance.

✓ Provide Regular & Substantive Training

Develop a training program to regularly educate employees across the enterprise.

✓ Continually Assess & Improve

Evaluate how well your training is working through deployment of phishing campaigns. Measure results of the campaign and plan a path forward in an after-action review with leadership.

POLL QUESTION

Is your company implementing any type of cybersecurity framework?

Ex: NIST, ISO, Other



NIST SP 800-171 Control Types

This isn't "just an IT thing"

AC	AT	AU	CM	IA	IR	MT	MP	PS	PE	RA	CA	SC	SI
3.1.1	3.2.1	3.3.1	3.4.1	3.5.1	3.6.1	3.7.1	3.8.1	3.9.1	3.10.1	3.11.1	3.12.1	3.13.1	3.14.1
3.1.2	3.2.2	3.3.2	3.4.2	3.5.2	3.6.2	3.7.2	3.8.2	3.9.2	3.10.2	3.11.2	3.12.2	3.13.2	3.14.2
3.1.3	3.2.3	3.3.3	3.4.3	3.5.3	3.6.3	3.7.3	3.8.3		3.10.3	3.11.3	3.12.3	3.13.3	3.14.3
3.1.4		3.3.4	3.4.4	3.5.4		3.7.4	3.8.4		3.10.4		3.12.4	3.13.4	3.14.4
3.1.5		3.3.5	3.4.5	3.5.5		3.7.5	3.8.5		3.10.5			3.13.5	3.14.5
3.1.6		3.3.6	3.4.6	3.5.6		3.7.6	3.8.6		3.10.6			3.13.6	3.14.6
3.1.7		3.3.7	3.4.7	3.5.7			3.8.7					3.13.7	3.14.7
3.1.8		3.3.8	3.4.8	3.5.8			3.8.8					3.13.8	
3.1.9		3.3.9	3.4.9	3.5.9			3.8.9					3.13.9	
3.1.10				3.5.10								3.13.10	
3.1.11				3.5.11								3.13.11	
3.1.12												3.13.12	
3.1.13												3.13.13	
3.1.14												3.13.14	
3.1.15												3.13.15	
3.1.16												3.13.16	
3.1.17													
3.1.18													
3.1.19													
3.1.20													
3.1.21													
3.1.22													

Administrative (e.g., policies, standards & procedures)

Technical Configurations (e.g., security settings)

Software Solution

Hardware Solution

Software or Hardware Solution

Assigned Tasks To Cybersecurity Personnel

Assigned Tasks To IT Personnel

Assigned Tasks To Application/Asset/Process Owner

Configuration or Software Solution

Configuration or Software or Hardware or Outsourced Solution



The Compliance Challenge

DFARS 252.204-70 (70 series)**

NIST

CMMC

7012

- Introduced 2013, implemented 2016, updated 2019. Aligns to 110 NIST 800-171 controls.
- Requires SSP, POA&M and reporting of certain events to DoD.
- **Enforceable through DCMA**

7019

- Implemented Nov 2020.
- Requirement to have a recent NIST 800-171 assessment on record in SPRS
- “Recent” defined as – within last 3 years.

7020

- Implemented Nov 2020 - NIST 800-171 DoD Assessment Requirements:
 - Submit report in SPRS; Remediate or adjudicate findings within 14 days; DCMA Access
 - **Flow down requirements – primes must drive supplier compliance**

7021

- Drafted Nov 2020, Multiple Revisions – CMMC Program
- CMMC 3rd Party assessments at least every 3 years, at Award or Option
- **Flow down requirements – primes must drive supplier compliance at every tier**

*

**32 CFR published to Federal Register October 15, 2024.
Will take effect December 15, 2024.**

Noteworthy Updates

CMMC Rulemaking Timeline

32 CFR final rule published to Federal Register

October 15, 2024

- ✓ Sets rules for CMMC program and governs the requirements for assessments
- ✓ Assessments may begin as of October 15, 2024

48 CFR proposed rule public comment period ended

October 15, 2024.

- ✓ This will now be reviewed by DoD and final rule is expected by Q2 2025.
- ✓ 48 CFR incorporates CMMC requirements into DoD contracts.
- ✓ Phased rollout begins once the final rule is published.



The Challenge - Latest Timelines

DoD Companion Video

Phase 1: (Sep – Nov 2024) (Q2 2025)

- Implementation date projected for 3rd or 4th Quarter FY 2024
- CMMC formally included in Solicitations

Phase 2: (Jun 2025) (Q4 2025)

- **+ 6 Months** from Implementation date
- Level 2 Cert **Required at Award**
- 80% of NIST-800171 R2 Controls Complete
- No POA&M for 3 or 5-Point Controls (encryption excepted)
- Fully compliant \leq 180 days

Phase 3: (Jun 2026) (Q4 2026)

- **+ 12 Months** from Phase 2 (+18 months from Implementation date)
- Level 1, 2, 3 Certification **at Award**
- No POA&M

Phase 4: (Jun 2027) (Q4 2027)

- +12 months from Phase 3 (30 months from Implementation)
- Fully implemented – all solicitations at award



***View the CMMC DoD Companion Video [HERE](#)**

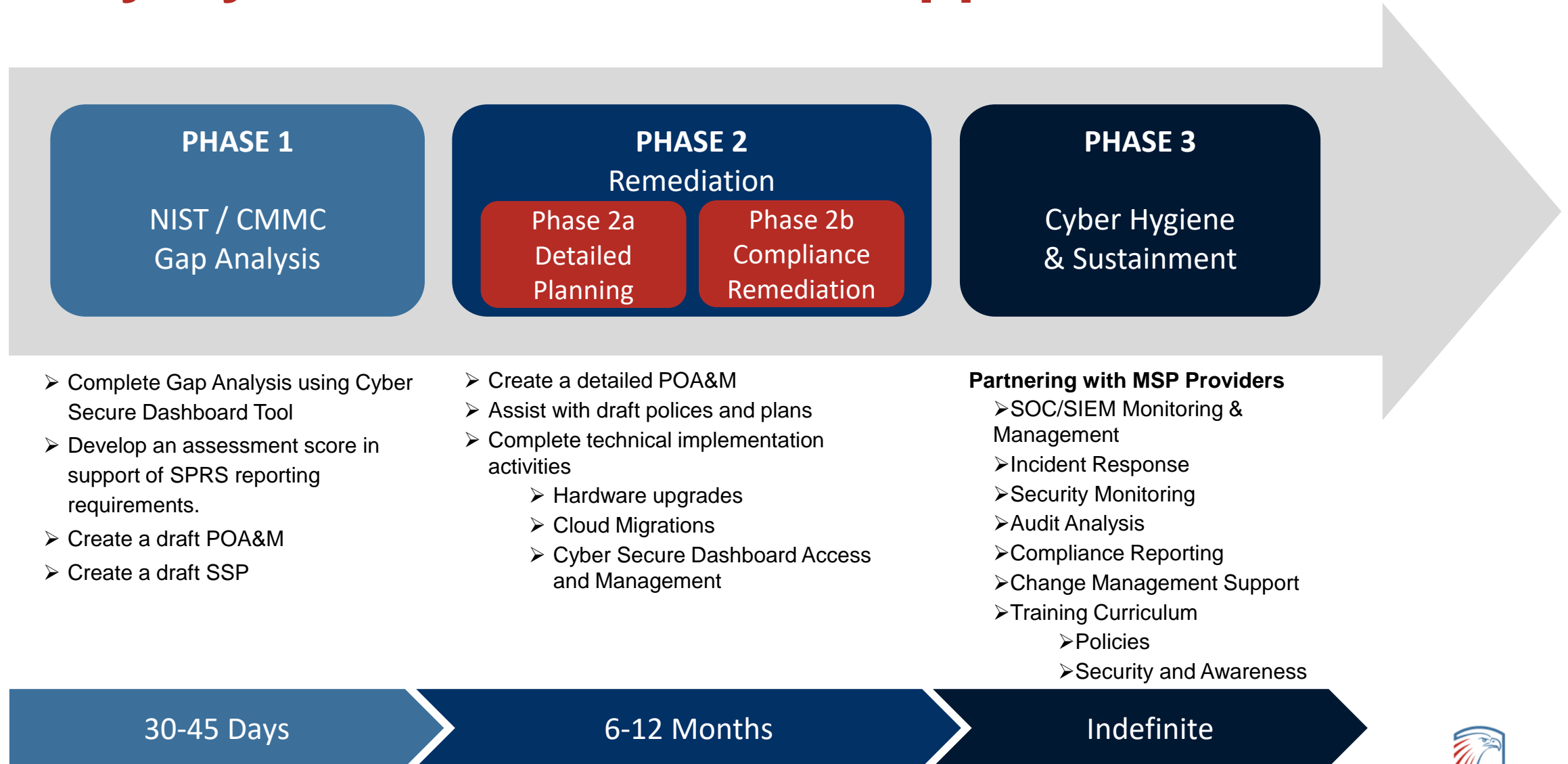
Prime contractors must ensure Subcontractors are compliant at all Tiers, which provides them the ability to dictate more rapid timelines as a discriminator.

Compliance Process

It's a Marathon – Not a Sprint

1. Planning... and planning to plan
2. Roughly a 70/30 split for Documentation/Technical implementation
3. Many factors involved:
 - ✓ Executive Buy-In
 - ✓ Funding
 - ✓ Technological solutions
 - ✓ Documentation
 - ✓ Timeline
 - ✓ Change Management

Iviry CyberMentum Phased Approach



Q & A





THINK IVIRY FOR IT

Iviry, LLC

1901 S Bell St, Suite 325
Arlington, VA 22202

www.iviry.com | 866.960.9658

marketing@iviry.com



APPENDIX



Reference Links and Supporting Material from the Webinar

- [FBI Internet Crime Report](#)
- [Iviry Blog Post on CMMC Final Ruling Published Oct. 15, 2024](#)
- [DoD Companion Video on CMMC Compliance](#)