CONNECTWISE®

SECUR-SERV

Finding Alignment with Compliance

Speaker Introductions

Jason Bowra

Scantron Technology Solutions

Sr. VP of Managed Services

Dave Koopmans

Scantron Technology Solutions

Solutions Engineer Manager

Jim Peterson

ConnectWise

Principal Solution Advisor

What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks and programs from digital attacks.

That’s true but businesses really need a comprehensive solution that protects businesses information, reputation, and continuity!

Cybersecurity

A compressive protection solution includes more than blocking attacks, it includes:

- *Cyber Tools*
- *Processes*
- *Teams*
- *BCDR Solutions*
- *Assessments*

Cybersecurity Terms

Attack

An attempt to bypass security measures implemented by an organization

Incident

Bypassing one or more of the security measures implemented by an organization

Breach

Manipulating, extracting, or making data unavailable

Bad Actors

Solo Bad Actor

Nation States

Organized Crime

Your data is valuable to Bad Actors, because it’s valuable to you!

Gaining Access

Bad actors work to find access into corporate systems through social engineering and testing, and environment vulnerabilities!

- *Credentials (49%)*

  Solution: Multi-Factor Authentication (MFA)

- *Phishing (17%)*

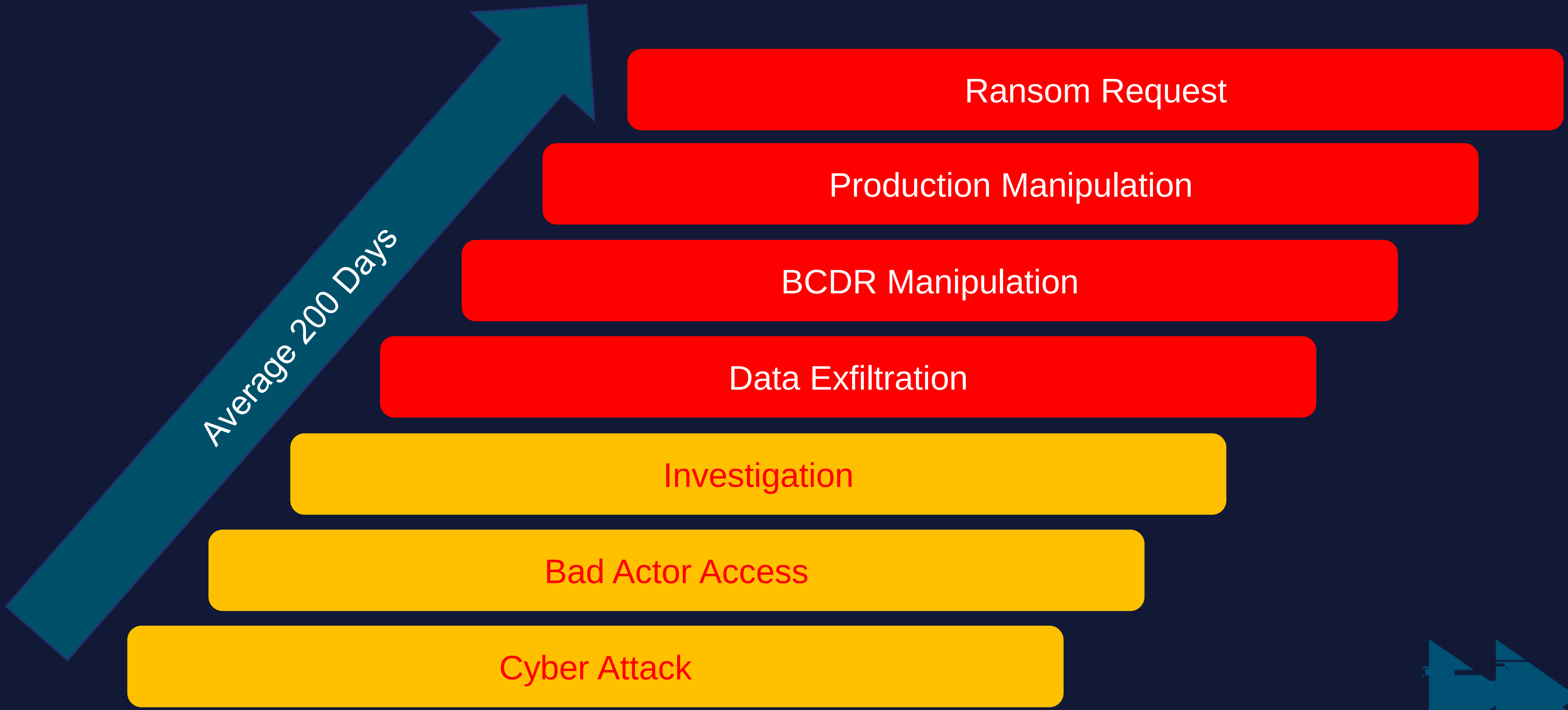
  Solution: Security Awareness Training / Email Filter

- *Exploits (9%)*

  Solution: System Patching

*Verizon 2023 DIBR Report

Gaining Access is just the start



Average 200 Days

Ransom Request

Production Manipulation

BCDR Manipulation

Data Exfiltration

Investigation

Bad Actor Access

Cyber Attack

What are the driving factors?

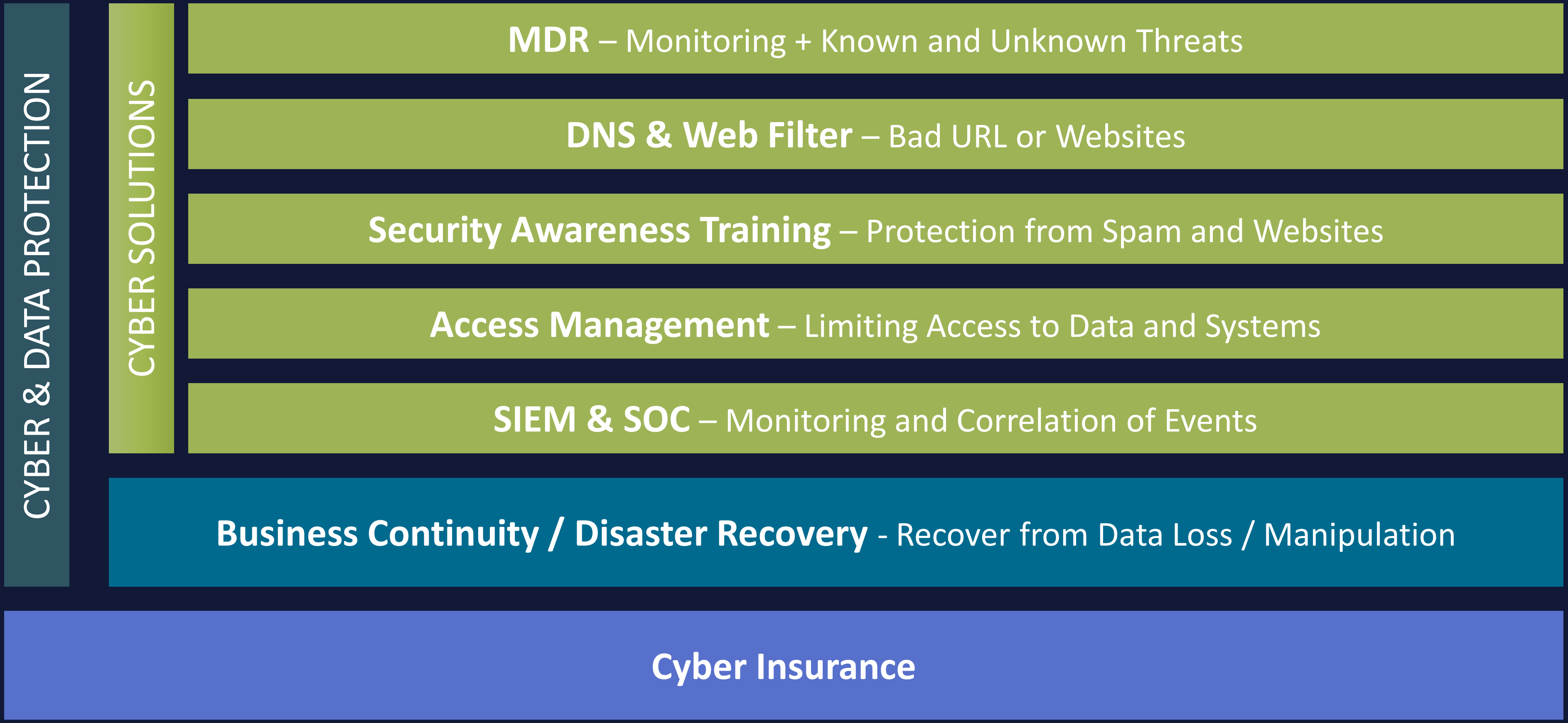
Unfortunately, many SMBs do not believe they are at risk from cyber attacks because they are ‘too small’.   There is no ‘too small’, if you have valuable data then you are a target!

- *Financial (95%)**
- *Espionage (4%)**
- *Ideology (>1%)**
- *Grudge (>1%)**
- *Other (>1%)**

$10.3 Billion in 2022**

* Verizon 2023 DIBR Report
**FBI – Internet Crime Report

Cybersecurity Layering Options



CYBER & DATA PROTECTION

CYBER SOLUTIONS

MDR – Monitoring + Known and Unknown Threats

DNS & Web Filter – Bad URL or Websites

Security Awareness Training – Protection from Spam and Websites

Access Management – Limiting Access to Data and Systems

SIEM & SOC – Monitoring and Correlation of Events

Business Continuity / Disaster Recovery - Recover from Data Loss / Manipulation

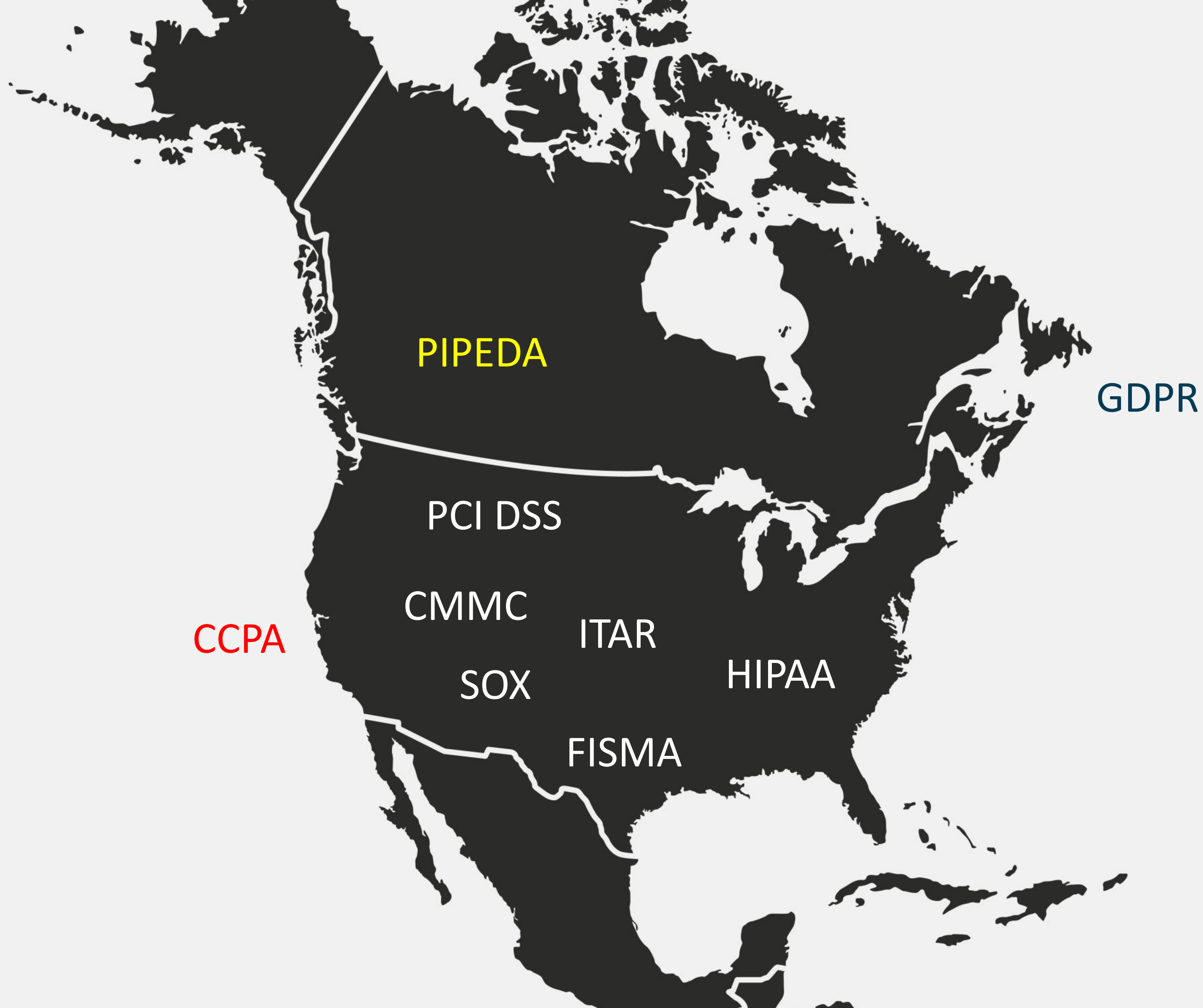
Cyber Insurance

Compliance & Cybersecurity

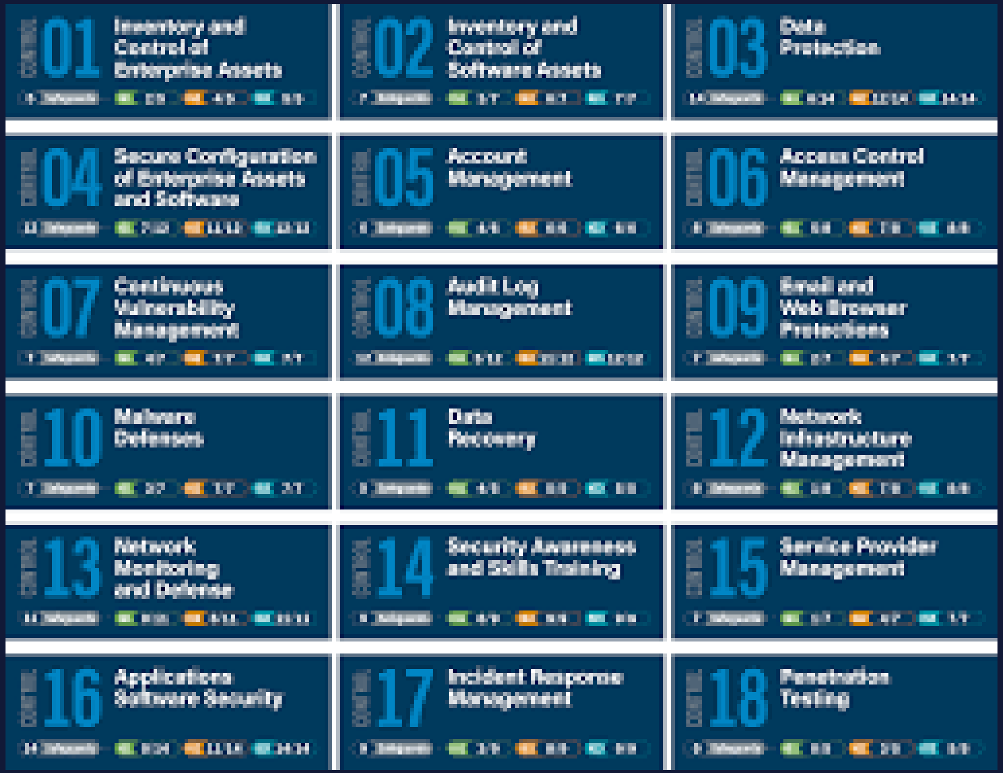
Many industries required specific people, process, and technologies that naturally are part of a proper cybersecurity solution

Challenges with Compliance

- Understanding Compliance
- Aligning Environments
- Enforcing Standards


PIPEDA
GDPR
PCI DSS
CMMC
CCPA
ITAR
SOX
HIPAA
FISMA

Starting Alignment: Two Main Helpers



01 Inventory and Control of Enterprise Assets

02 Inventory and Control of Software Assets

03 Data Protection

04 Secure Configuration of Enterprise Assets and Software

05 Account Management

06 Access Control Management

07 Continuous Vulnerability Management

08 Audit Log Management

09 Email and Web Browser Protections

10 Malware Defenses

11 Data Recovery

12 Network Infrastructure Management

13 Network Monitoring and Defense

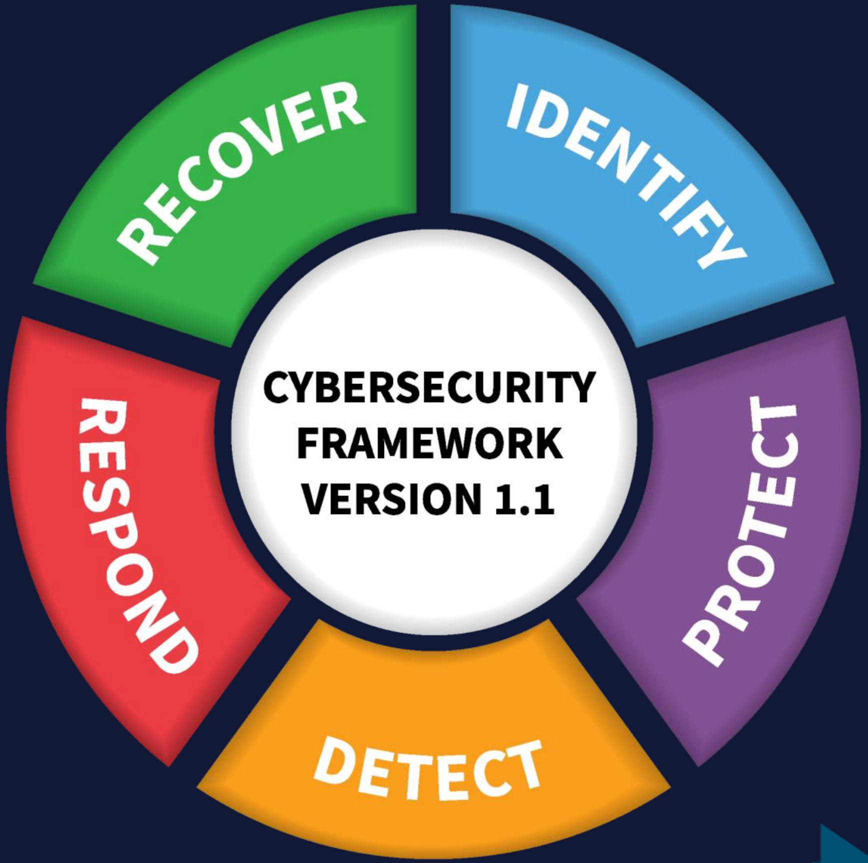
14 Security Awareness and Skills Training

15 Service Provider Management

16 Applications Software Security

17 Incident Response Management

18 Penetration Testing



CYBERSECURITY FRAMEWORK VERSION 1.1

IDENTIFY

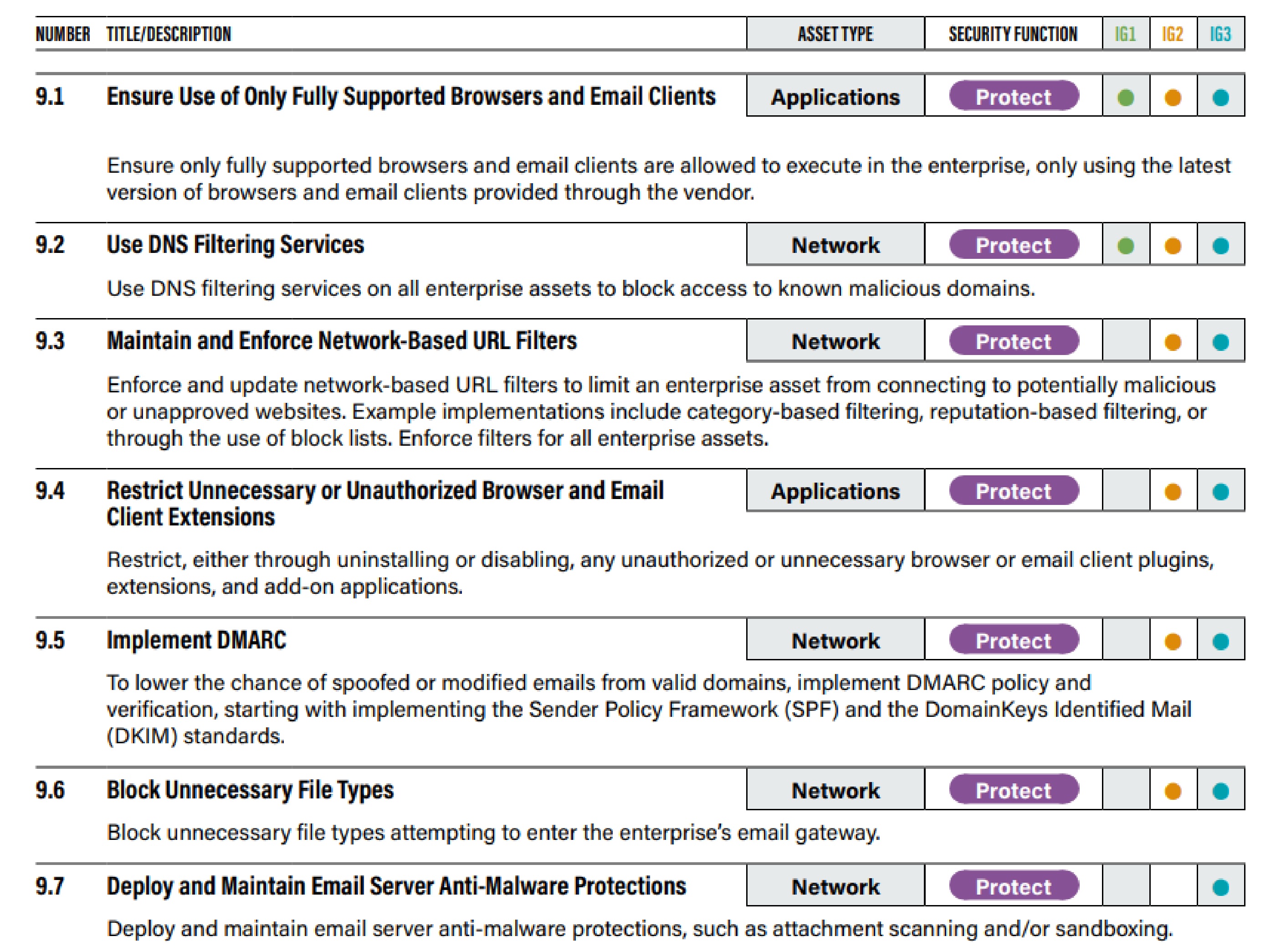
PROTECT

DETECT

RESPOND

RECOVER

Starting Alignment: Safeguards and Controls



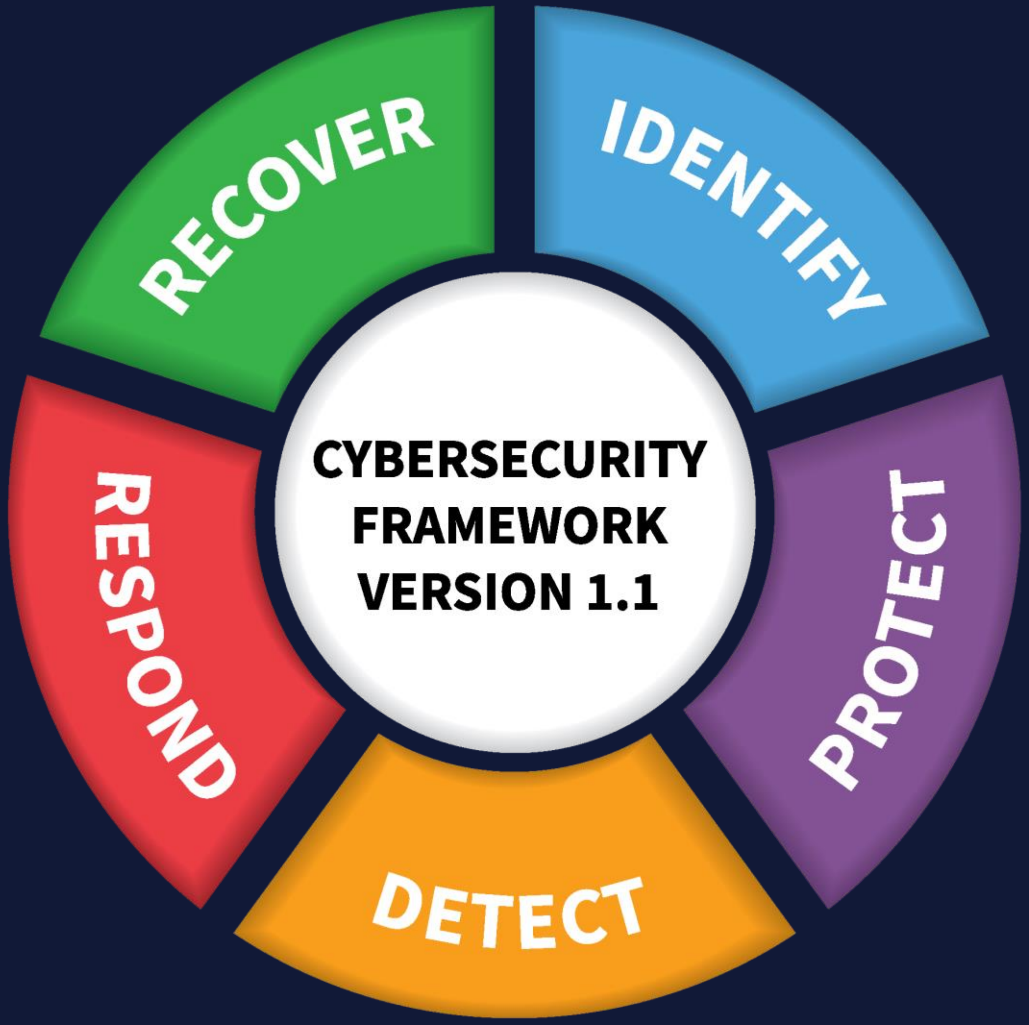
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
9.1	**Ensure Use of Only Fully Supported Browsers and Email Clients** Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	Applications	Protect	●	●	●
9.2	**Use DNS Filtering Services** Use DNS filtering services on all enterprise assets to block access to known malicious domains.	Network	Protect	●	●	●
9.3	**Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.	Network	Protect		●	●
9.4	**Restrict Unnecessary or Unauthorized Browser and Email Client Extensions** Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.	Applications	Protect		●	●
9.5	**Implement DMARC** To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.	Network	Protect		●	●
9.6	**Block Unnecessary File Types** Block unnecessary file types attempting to enter the enterprise's email gateway.	Network	Protect		●	●
9.7	**Deploy and Maintain Email Server Anti-Malware Protections** Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.	Network	Protect			●

Aligning with Compliance - NIST

NIST 800-53

National Institute of Standards and Technologies

- 23 Categories
- 108 Controls



Aligning with Compliance - CIS

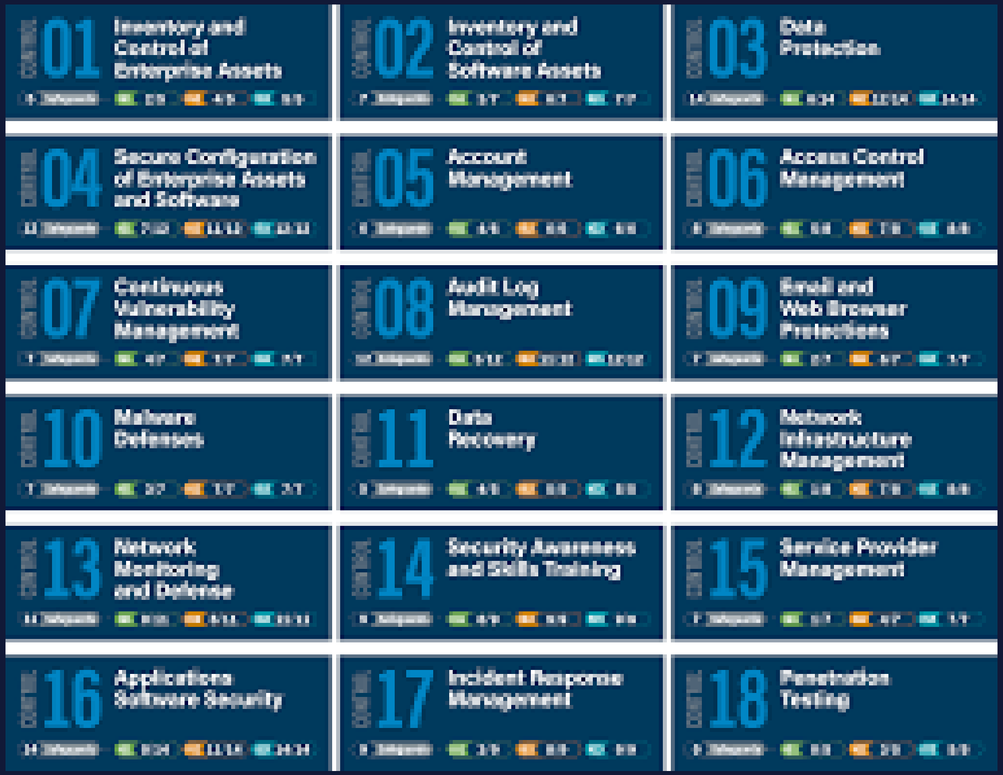
CIS v8

Center for Information Security

- 18 Critical Security Controls

Implementation Group

- IG1 = 56 Safeguards
- IG2 = 130 Safeguards
- IG3 = 153 Safeguards



01 Inventory and Control of Enterprise Assets	02 Inventory and Control of Software Assets	03 Data Protection
04 Secure Configuration of Enterprise Assets and Software	05 Account Management	06 Access Control Management
07 Continuous Vulnerability Management	08 Audit Log Management	09 Email and Web Browser Protections
10 Malware Defenses	11 Data Recovery	12 Network Infrastructure Management
13 Network Monitoring and Defense	14 Security Awareness and Skills Training	15 Service Provider Management
16 Applications Software Security	17 Incident Response Management	18 Penetration Testing

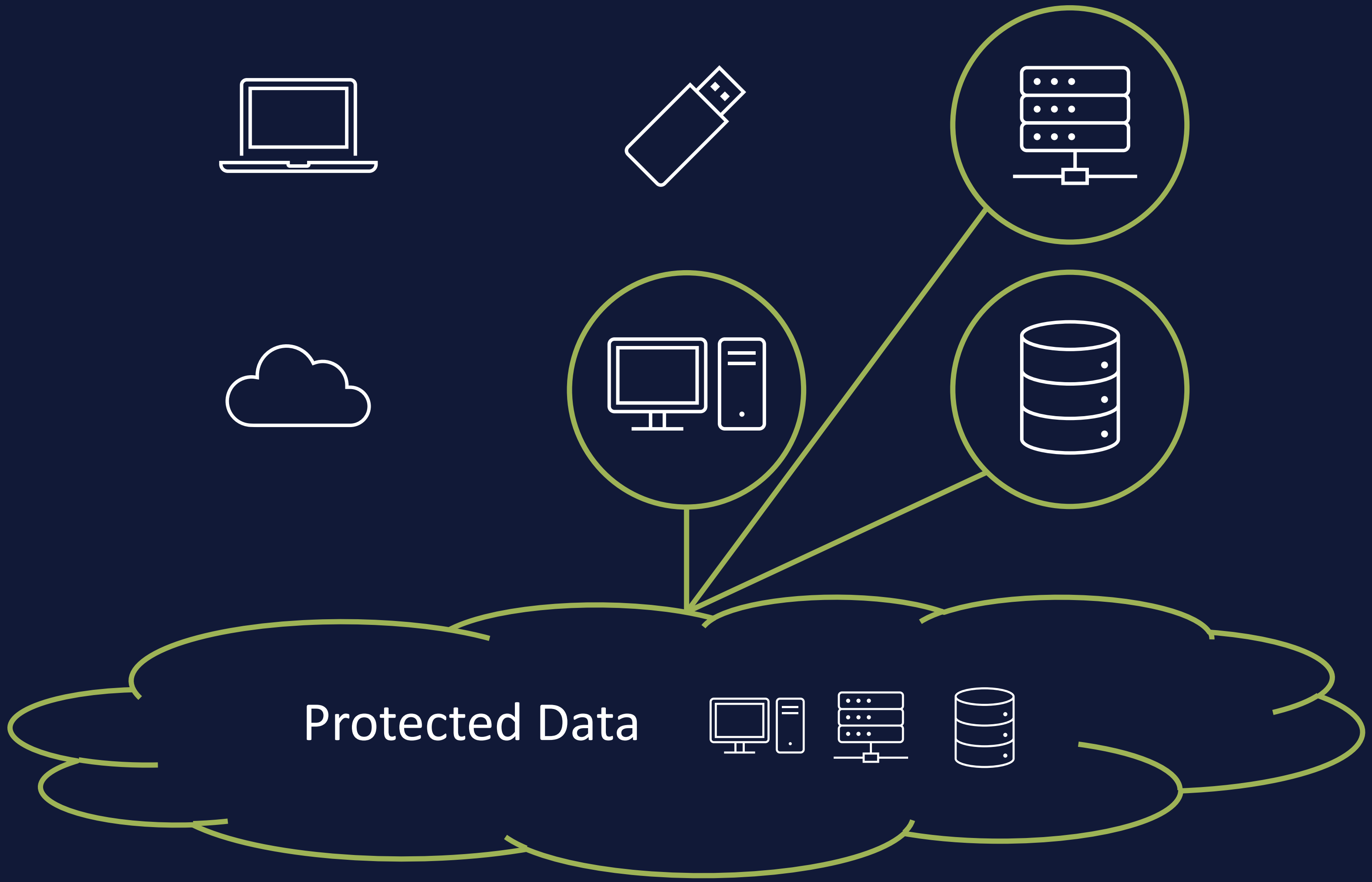
Enforcement Challenges

- *Set and Forget*
- *Continual Improvement*
- *Internal Policy and Process*
- *Review and Testing*

5 Foundational Items for Compliance

- *EDR / MDR: Endpoint or Managed Detect and Response*
- *MFA: Multi Factor Authentication*
- *SAT: Security Awareness Training*
- *IAM/PAM/ZTA: Access Management*
- *BCDR: Business Continuity / Disaster Recovery*

Reminder: Working from Anywhere = Data Everywhere



The Real OG: BCDR

BCDR ensures that you can recover your environment when all else fails!

Backup is not enough

Having a copy of your data does not help figure out who does what and when

Last Line of Defense

Just because you can eventually recover your data does not mean your business will recover

Data is Everywhere

Work from anywhere = data everywhere

Financial Impact

Being shutdown is expensive for short periods of time and business threating for long timelines

Wrapping it up!

Compliance is challenging and is a journey. CIS and NIST are great at helping build a framework that simplifies the challenges of alignment. Enforcement is the real hard part.

Understand

Knowing your compliance needs and working with a valued partner

Align

Either you do it or you don’t, look at the intention of the control.

Enforce

Don’t set and forget, it’s a journey.

Questions?

CONNECTWISE

SECUR-SERV

Thank You!