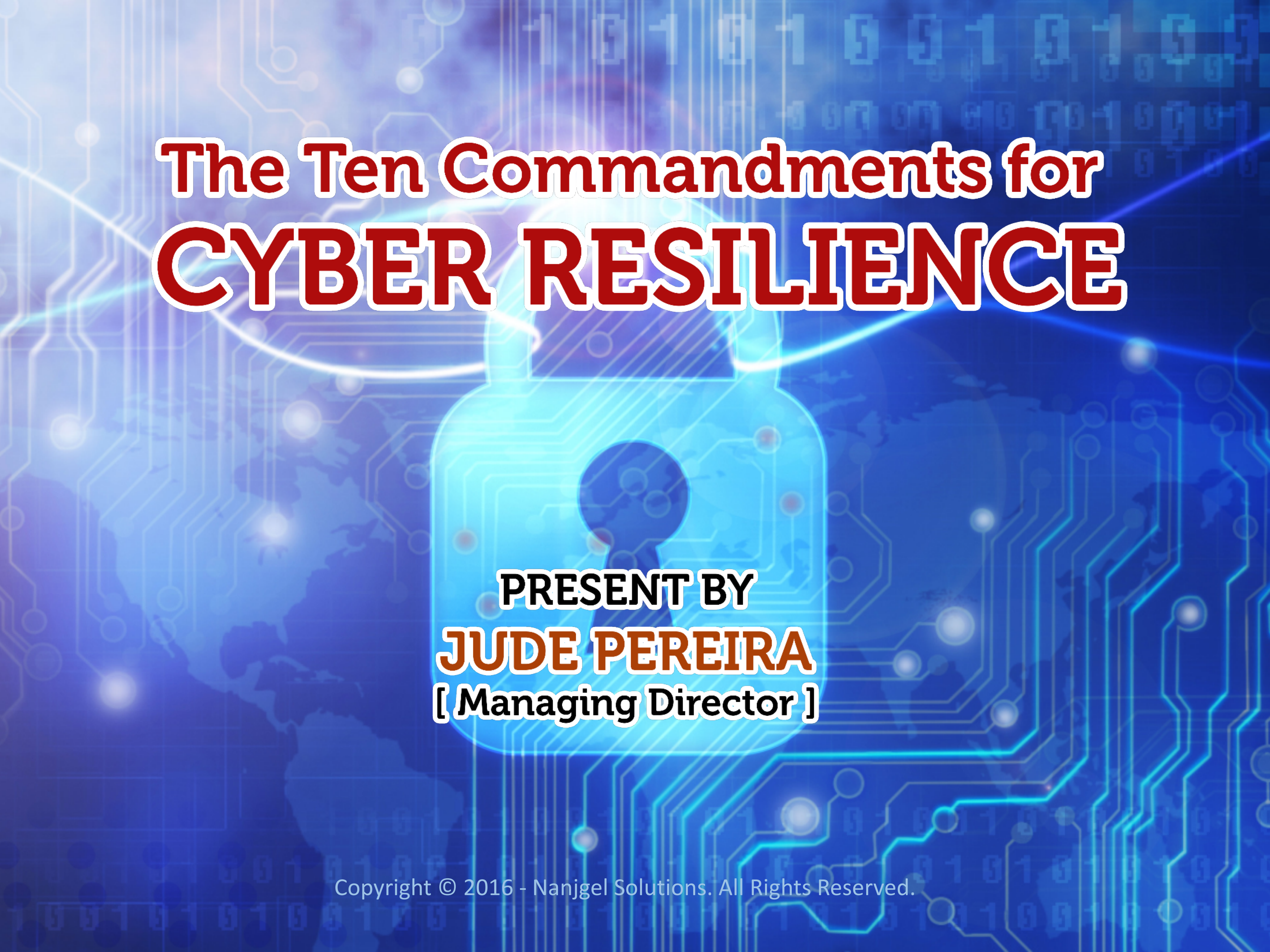


The Ten Commandments for CYBER RESILIENCE

PRESENT BY

JUDE PEREIRA

[Managing Director]

Do I really need to automate provisioning? Only few people join/leave in a month!!

What solution areas should I target first?
Which application?

Which product would work best for me?

Not sure if I have right policies and process to automate via an IAM system

All vendors say they can do. Who is best for me?

AGENDA ……

- Role of a CISO
- Introducing CYBER RESILIENCE
- CYBER RESILIENCE Frameworks
- The TEN Commandments for CYBER RESILIENCE

Role of CISO & Mindset ????

IBM’s 2016 Chief Information Security Officer Study revealed the changing role of the CISO

Influencers

- Confident / prepared
- Strategic focus

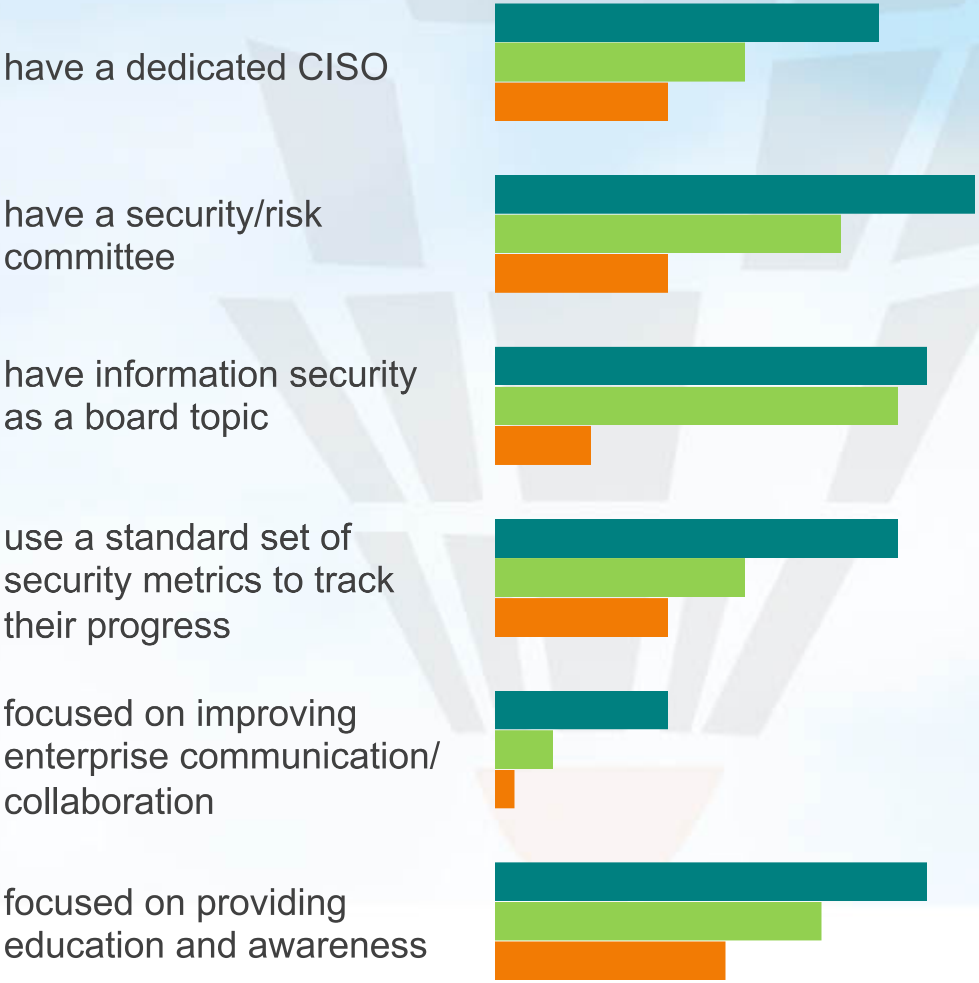
Protectors

- Less confident
- Somewhat strategic
- Lack necessary structural elements

Responders

- Least confident
- Focus on protection and compliance

How they differ



have a dedicated CISO

have a security/risk committee

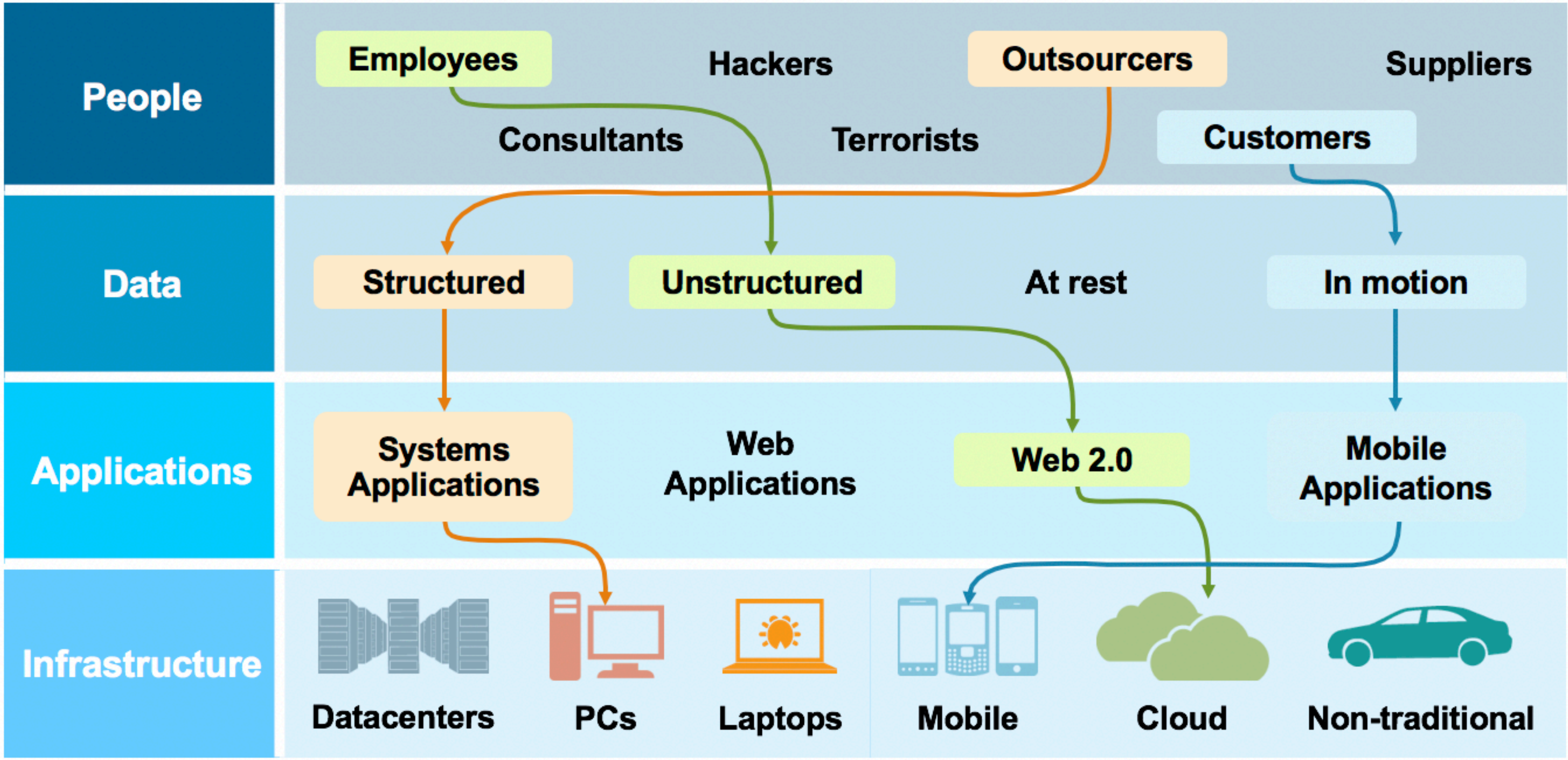
have information security as a board topic

use a standard set of security metrics to track their progress

focused on improving enterprise communication/ collaboration

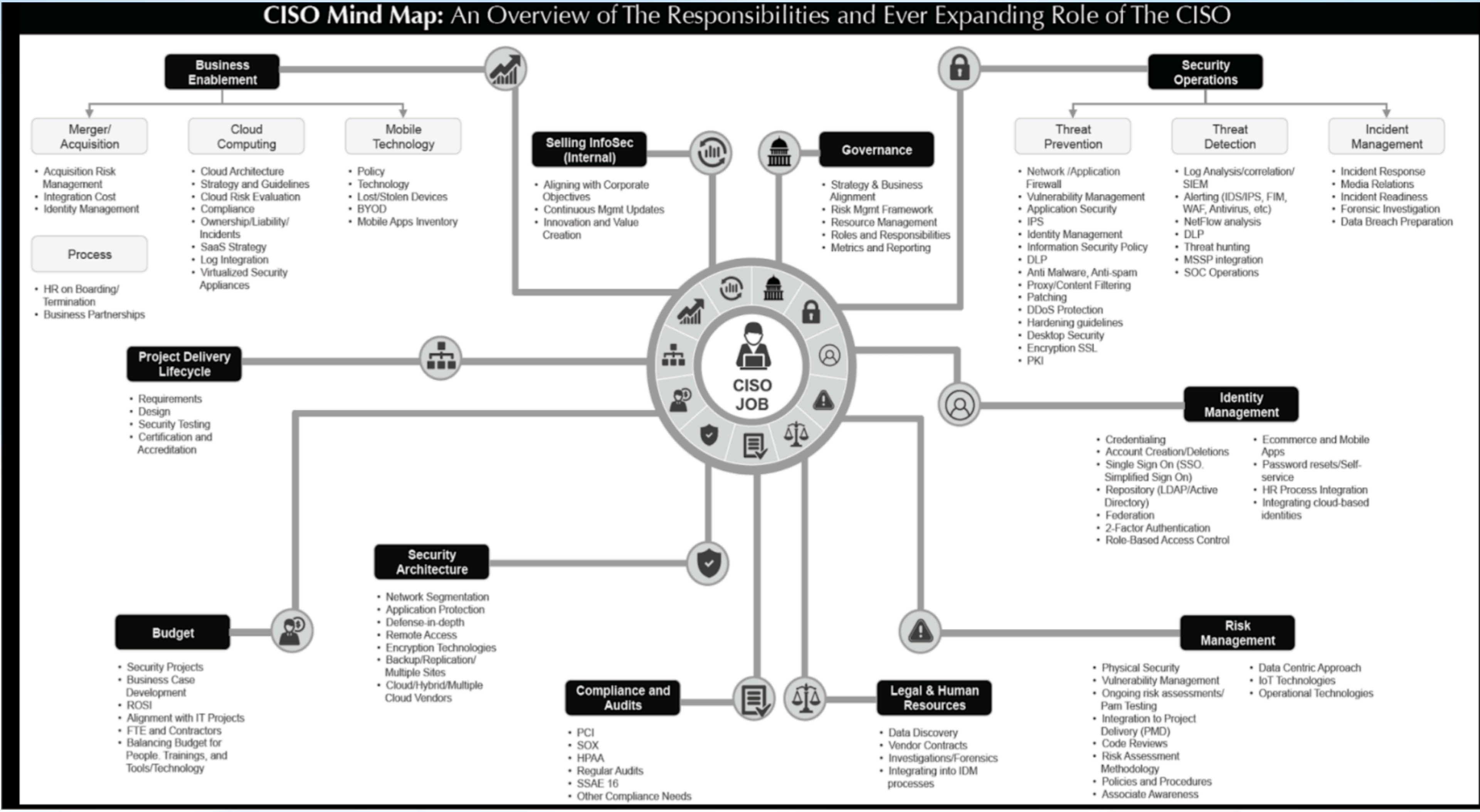
focused on providing education and awareness

Security challenges are a complex, four-dimensional puzzle …



… that requires a new approach

CISO Mind Map: An Overview of The Responsibilities and Ever Expanding Role of The CISO



CISO JOB

Business Enablement

Merger/ Acquisition
- Acquisition Risk Management
- Integration Cost
- Identity Management

Process
- HR on Boarding/ Termination
- Business Partnerships

Cloud Computing
- Cloud Architecture
- Strategy and Guidelines
- Cloud Risk Evaluation
- Compliance
- Ownership/Liability/ Incidents
- SaaS Strategy
- Log Integration
- Virtualized Security Appliances

Mobile Technology
- Policy
- Technology
- Lost/Stolen Devices
- BYOD
- Mobile Apps Inventory

Selling InfoSec (Internal)
- Aligning with Corporate Objectives
- Continuous Mgmt Updates
- Innovation and Value Creation

Governance
- Strategy & Business Alignment
- Risk Mgmt Framework
- Resource Management
- Roles and Responsibilities
- Metrics and Reporting

Security Operations

Threat Prevention
- Network /Application Firewall
- Vulnerability Management
- Application Security
- IPS
- Identity Management
- Information Security Policy
- DLP
- Anti Malware, Anti-spam
- Proxy/Content Filtering
- Patching
- DDoS Protection
- Hardening guidelines
- Desktop Security
- Encryption SSL
- PKI

Threat Detection
- Log Analysis/correlation/ SIEM
- Alerting (IDS/IPS, FIM, WAF, Antivirus, etc)
- NetFlow analysis
- DLP
- Threat hunting
- MSSP integration
- SOC Operations

Incident Management
- Incident Response
- Media Relations
- Incident Readiness
- Forensic Investigation
- Data Breach Preparation

Project Delivery Lifecycle
- Requirements
- Design
- Security Testing
- Certification and Accreditation

Identity Management
- Credentialing
- Account Creation/Deletions
- Single Sign On (SSO. Simplified Sign On)
- Repository (LDAP/Active Directory)
- Federation
- 2-Factor Authentication
- Role-Based Access Control
- Ecommerce and Mobile Apps
- Password resets/Self-service
- HR Process Integration
- Integrating cloud-based identities

Security Architecture
- Network Segmentation
- Application Protection
- Defense-in-depth
- Remote Access
- Encryption Technologies
- Backup/Replication/ Multiple Sites
- Cloud/Hybrid/Multiple Cloud Vendors

Budget
- Security Projects
- Business Case Development
- ROSI
- Alignment with IT Projects
- FTE and Contractors
- Balancing Budget for People, Trainings, and Tools/Technology

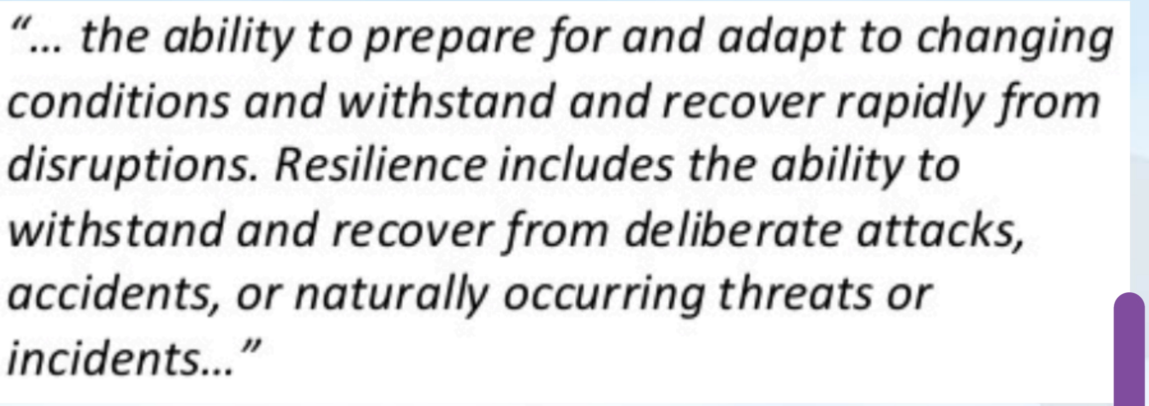
Compliance and Audits
- PCI
- SOX
- HPAA
- Regular Audits
- SSAE 16
- Other Compliance Needs

Legal & Human Resources
- Data Discovery
- Vendor Contracts
- Investigations/Forensics
- Integrating into IDM processes

Risk Management
- Physical Security
- Vulnerability Management
- Ongoing risk assessments/ Pam Testing
- Integration to Project Delivery (PMD)
- Code Reviews
- Risk Assessment Methodology
- Policies and Procedures
- Associate Awareness
- Data Centric Approach
- IoT Technologies
- Operational Technologies

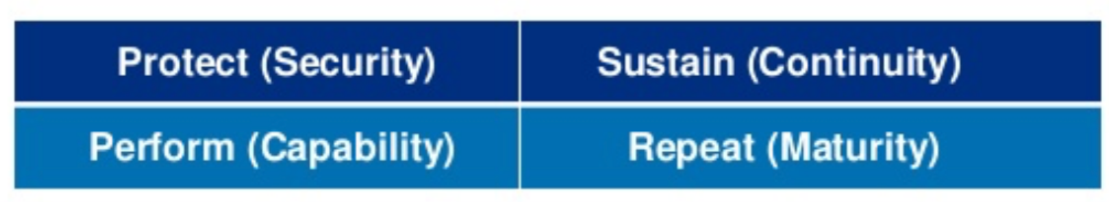
Introducing CYBER RESILIENCE

INTRODUCING CYBER RESILIENCE



"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"

- ***Cyber resilience involves a change in mindset whereby you look to identify how secure the business needs to be in order to survive.***



Protect (Security)	Sustain (Continuity)
Perform (Capability)	Repeat (Maturity)

BARRIERS TO CYBER RESILIENCE?

- Lack of awareness (board level down)
- Silo thinking ("it's an IT problem")
- Narrow focus on regulatory compliance, not risk
- Confusion about what "good" looks like
- Cyber resilience demands a "whole system" view (technology and people)
    - Cyber resilience has to be part of your organisational culture...

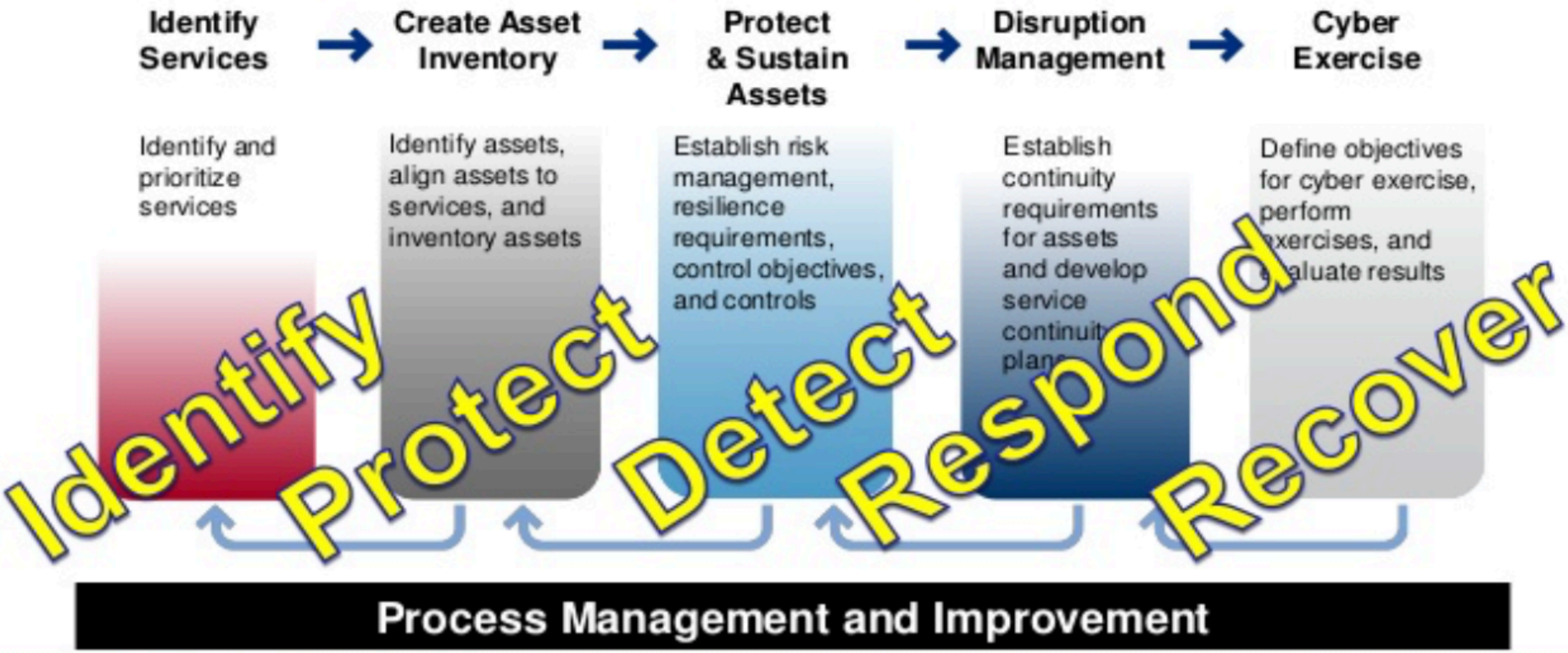
RISKS TO VALUE

- Loss of corporate reputation and customer trust
- Financial loss and reduced productivity
- Regulatory fines
- Reduced competitive advantage through IP theft
- (Damaged personal reputations)

CYBER RESILIENCE FRAMEWORKS

Cyber Resilience Review and the Framework

Relationship between DHS' Cyber Resilience Review and the NIST Cybersecurity Framework ***[CRR to NIST CSF crosswalk available]***



Identify Services → **Create Asset Inventory** → **Protect & Sustain Assets** → **Disruption Management** → **Cyber Exercise**

Identify and prioritize services

Identify assets, align assets to services, and inventory assets

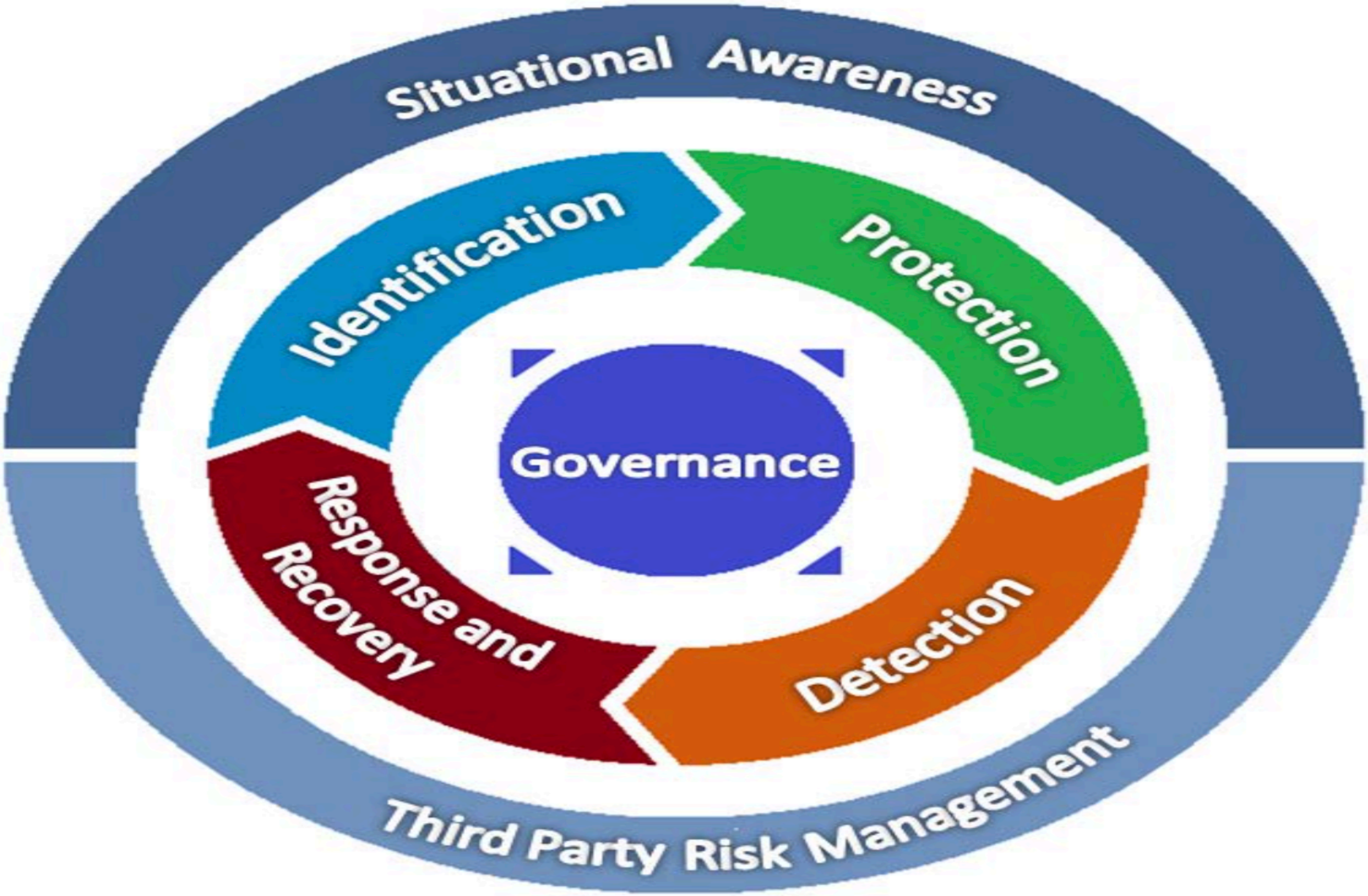
Establish risk management, resilience requirements, control objectives, and controls

Establish continuity requirements for assets and develop service continuity plans

Define objectives for cyber exercise, perform exercises, and evaluate results

Process Management and Improvement

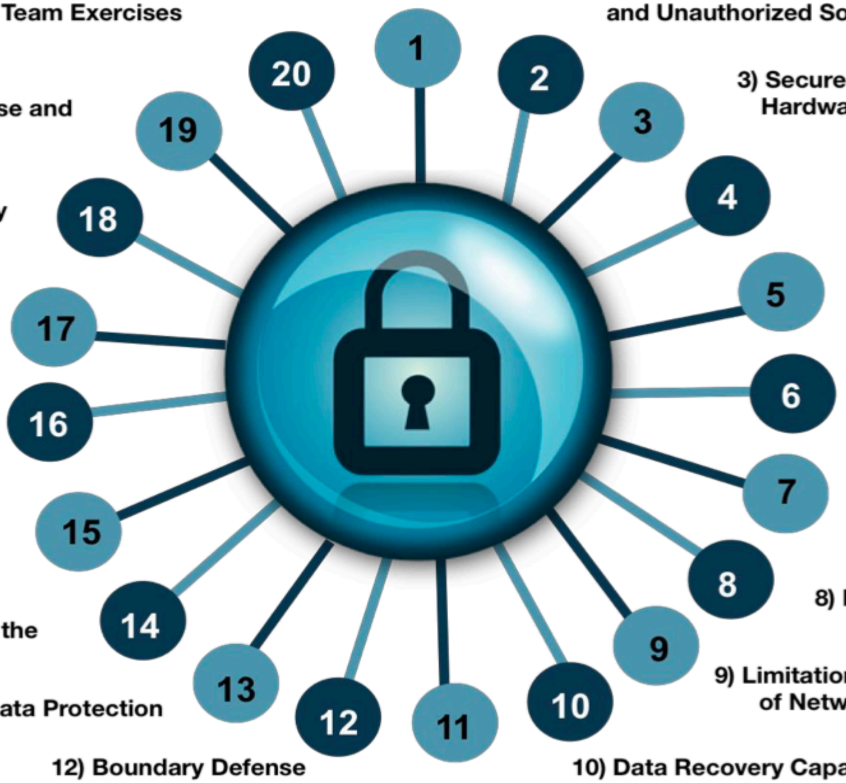
Cyber Resilience Assessment Framework



Cybersecurity Resilience Maturity Framework

	Maturity Descriptor	Employment of Security Controls	Security Tailored to Mission	Participate in Information Sharing (threat/vul.)	Response to Cyber Threats	Resilience to Cyber Attacks
Step 2: Address Sophisticated Attacks	Level 5: Resilient	Augment CSC Based on Mission	Mission Assurance Focused	Real Time Response to Inputs	Anticipate Threats	Operate Through Sophisticated Attack
	Level 4: Dynamic	Augment CSC Based on Mission	Mission Focused	Real Time Response to Inputs	Rapid Reaction To Threats	Able to respond to Sophisticated Attack
Step 1: Implement CSC Baseline	Level 3: Managed	CSC Integrated and Continuously Monitored	Partially Mission Focused	Respond to Information Inputs	Respond to Attacks After the Fact	Protection against Unsophisticated Attack
	Level 2: Performed	Foundational/ Critical Security Controls (CSC) Implemented	Mission Agnostic	Inconsistent Response to Information Inputs	Respond to Attacks After the Fact	Some Protection Against Unsophisticated Attacks
	Level 1: No Resilience	Inconsistent Deployment of Security Controls	None	None	No Response	Susceptible to Unsophisticated Attacks

Cyber Resilience Controls



1) Inventory of Authorized and Unauthorized Devices

2) Inventory of Authorized and Unauthorized Software

3) Secure Configurations for Hardware and Software

4) Continuous Vulnerability Assessment and Remediation

5) Controlled Use of Administrative Privileges

6) Maintenance, Monitoring and Analysis of Audit Logs

7) Email and Web Browser Protections

8) Malware Defenses

9) Limitation and Control of Network Ports

10) Data Recovery Capability

11) Secure Configurations for Network Devices

12) Boundary Defense

13) Data Protection

14) Controlled Access Based on the Need to Know

15) Wireless Access Control

16) Account Monitoring and Control

17) Security Skills Assessment and Appropriate Training to Fill Gaps

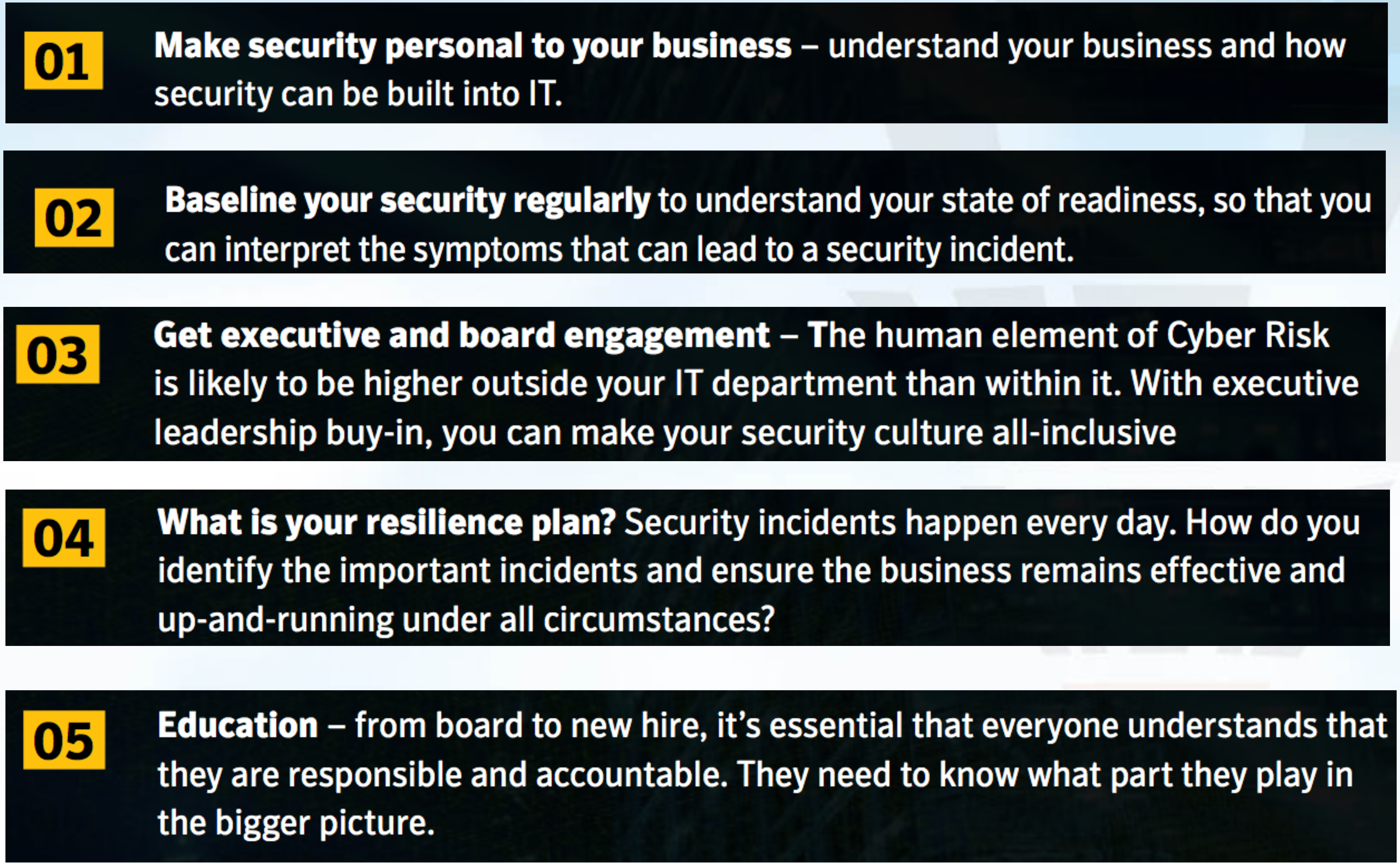
18) Application Software Security

19) Incident Response and Management

20) Penetration Tests and Red Team Exercises

TEN Commandments for CYBER RESILIENCE

Ten Commands For Cyber Resilience



01 **Make security personal to your business** – understand your business and how security can be built into IT.

02 **Baseline your security regularly** to understand your state of readiness, so that you can interpret the symptoms that can lead to a security incident.

03 **Get executive and board engagement** – The human element of Cyber Risk is likely to be higher outside your IT department than within it. With executive leadership buy-in, you can make your security culture all-inclusive

04 **What is your resilience plan?** Security incidents happen every day. How do you identify the important incidents and ensure the business remains effective and up-and-running under all circumstances?

05 **Education** – from board to new hire, it's essential that everyone understands that they are responsible and accountable. They need to know what part they play in the bigger picture.

06 **Do the basics well** – leverage government and industry guidelines. This includes aspects such as patching and good user-level access management.

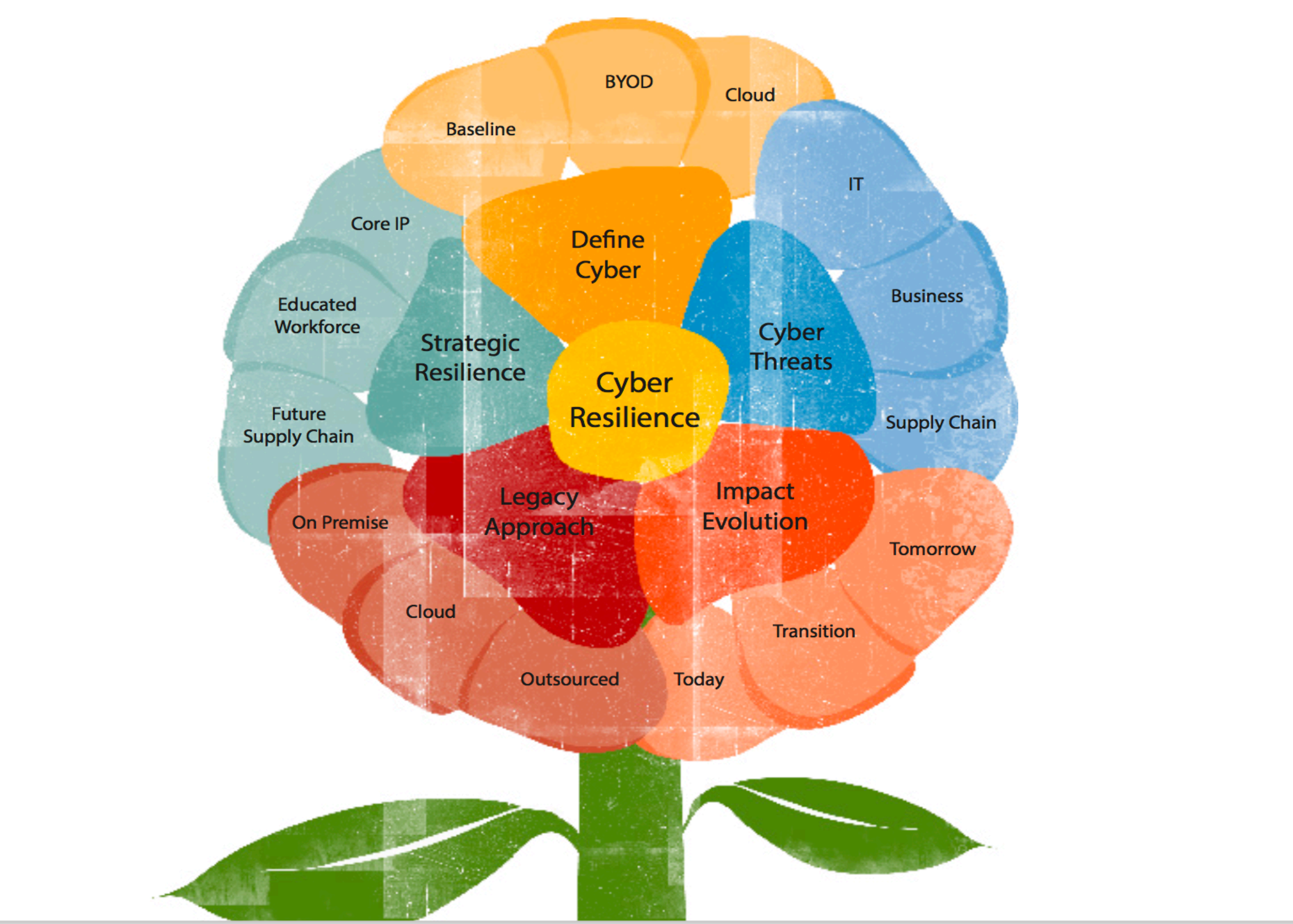
07 **Plan for today and scale for the future** – for example, BYOD is here to stay. Hence, we must stop applying quick fixes to such issues, unless they are aligned to a longer-term strategy.

08 **Start small, but think big.** Information protection is a long-term project, but we need to start where we will add the most business value and then continue to expand where there is further, long-term business value. This can include, for example, the supply chain and how we interact with our wider network of vendors and partners. The key here is to think big but have a maturity plan, which must be linked to strategic business value and growth.

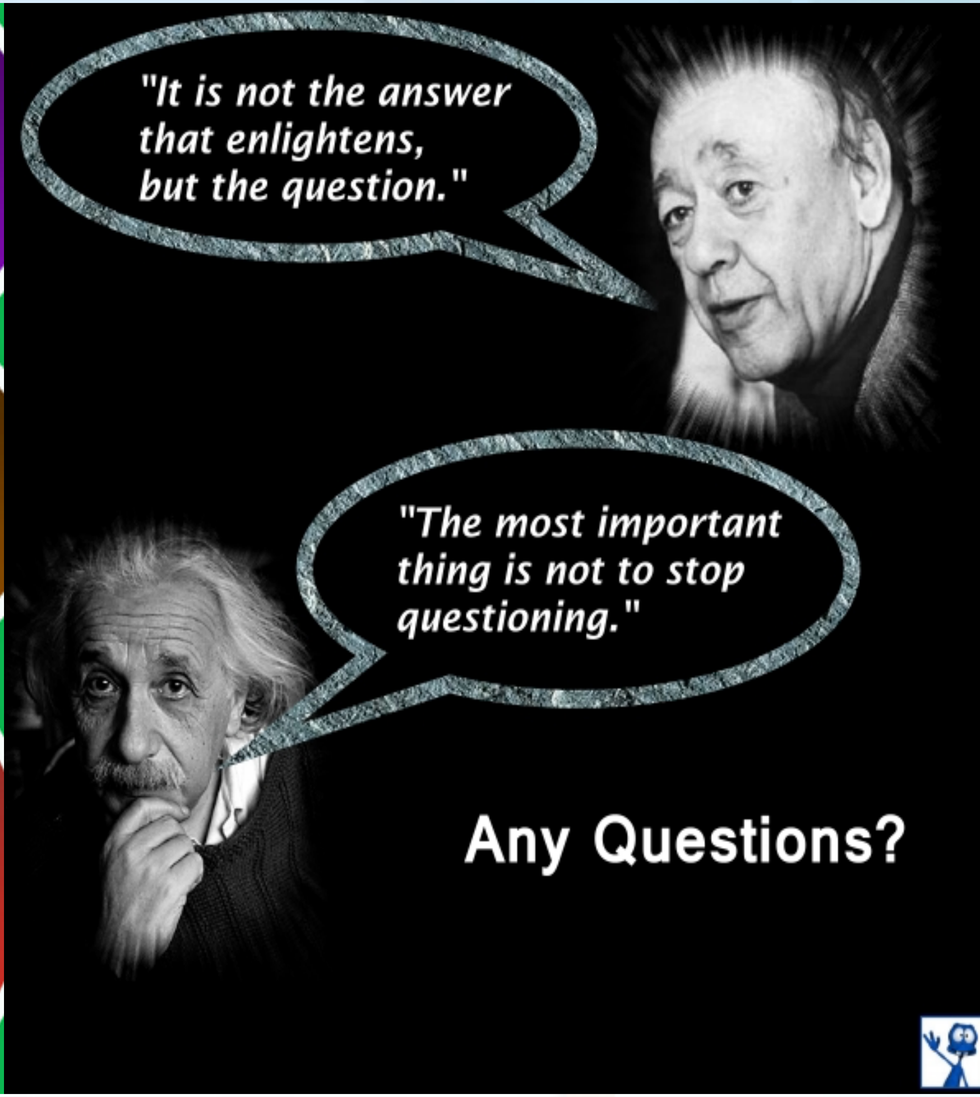
09 **Be accountable** – understand what the regulatory, legislative and peer-to-peer controls are that you need to adhere to. Make sure you have a clearly defined owner for each of these and an executive sponsor.

10 **Don’t wait for it to happen** – test your processes, procedures and people regularly. Make sure you have clearly defined lifecycles that reflect changes in business strategy, technology use and culture. Make sure your strategy is current and effective for the business and the risks.

Summary of Cyber Resilience



WHO?
WHOM?
WHEN?
WHOSE?
QUESTIONS
HOW?
WHAT?
WHY?
WHERE?
WHICH?


"It is not the answer that enlightens, but the question."
"The most important thing is not to stop questioning."
Any Questions?