SAIEE Conference 2019: "Secure Connectivity"

Cyber Secure Future: Pitfalls in Conventional Engineering Approach

Lloyd Chego

PhD(Elec)(candidate): UP; MSc(Elec): Wits, BEng(Elec): UP, Higher Cert. Cyber Security (Cum Laude): UJ

Contents

- Introduction
- Evolution of Cyber threats
- Cyber security Goals & Value Chain
- Common Bariers
- People
- Processes
- Technology
- Conclusion

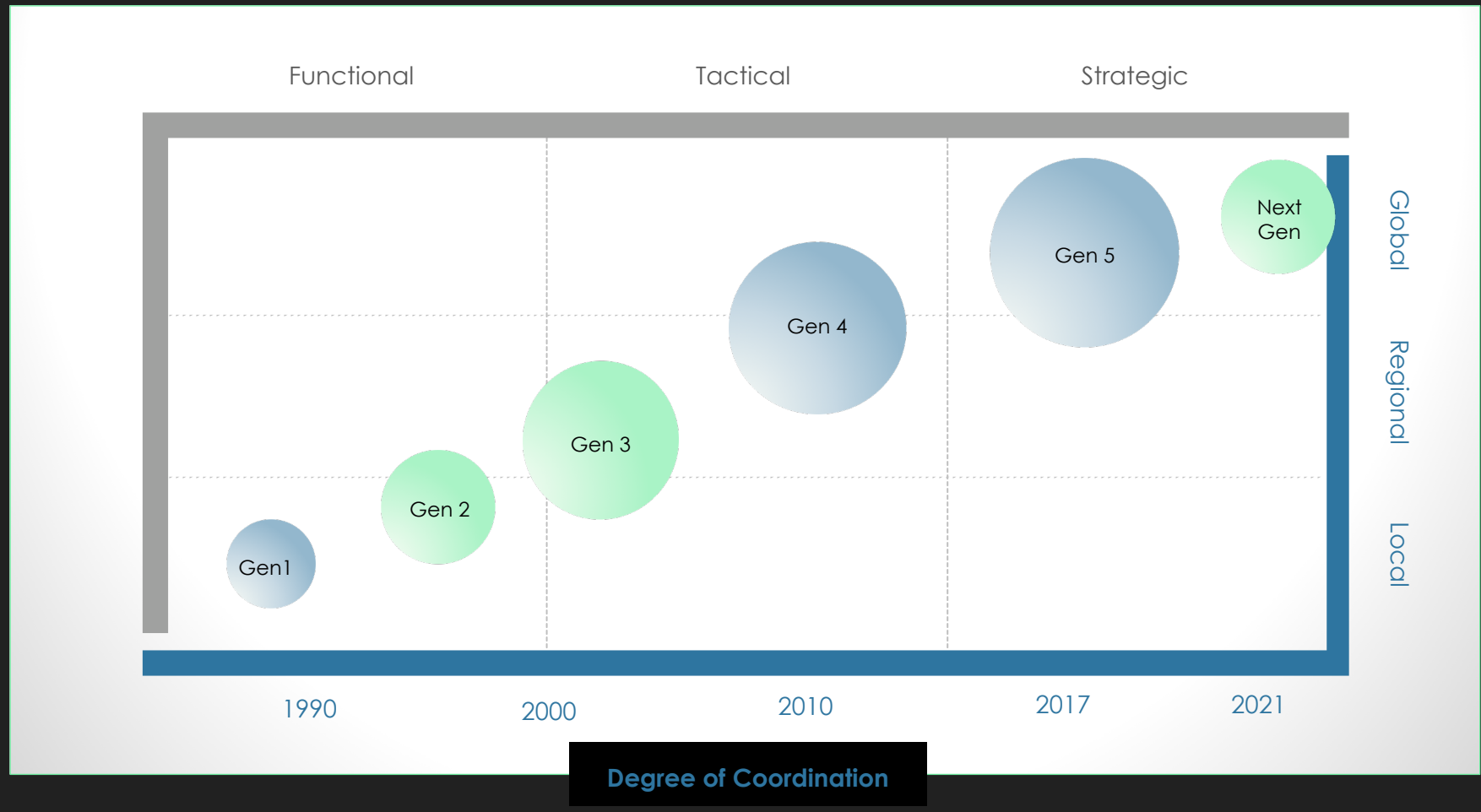
Introduction

- Critical Infrastructure Focus: SA Focused
- What is conventional Engineering approach?
- What pitfalls results in this?
  - Inability to adequately respond to a Cyber Incident.
- Will focus on Processes, People and Technology

Source: https://www.huntsmansecurity.com/industries/critical-infrastructure/

Evolution of Cyber Threat

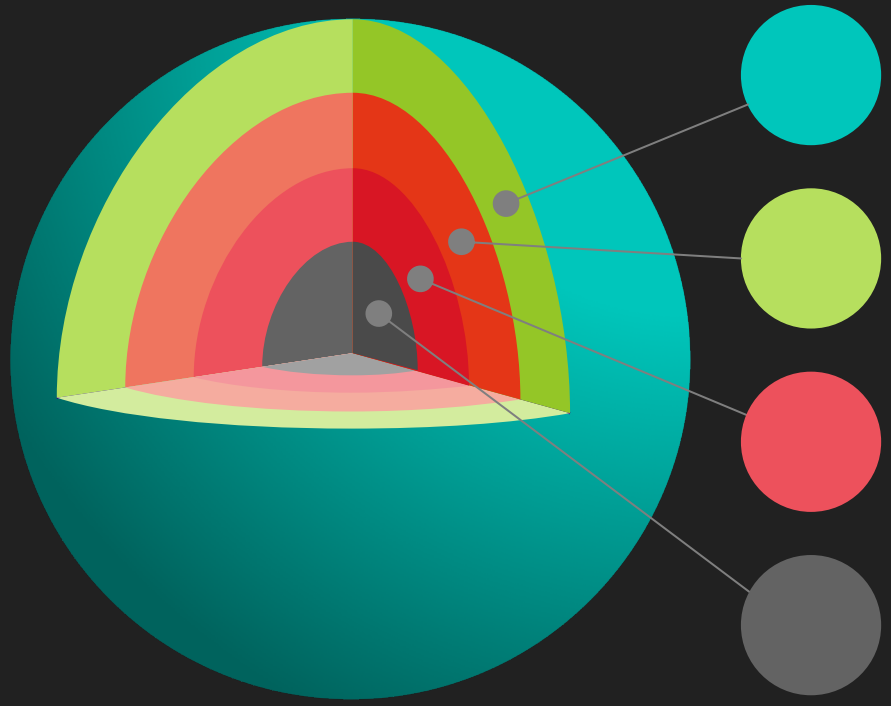
- Gen 1: 80's Viral based attacks. Mostly on Stand-alone PC's/ Systems Drove Anti-virus business
- Gen 2: 90's Network (Internet) based attacks, Firewall business
- Gen 3: 2000's Applications vulnerability exploit based attacks, Focus on Intrusion detection.
- Gen 4: Polymorphic Payloads (various forms) type attacks. Drove deep session inspection tools, sandbox, anti-bots
- Gen 5: Mega Attacks (Cyber warfare, Nation State based attacks, Critical infrastructure attacks, Traditional defences redundancy
- Next Gen: e.g. Quantum Computing, AI, based attacks



Source: https://www.checkpoint.com/downloads/product-related/brochure/gen_v_brochure-.pdf

Cyber Security Goals

Cyber Security is the securing of assets by identifying, defending, responding and recovering from cyber attacks



Confidentiality

Ensure Appropriate authorized use/ disclosure of information or data

Integrity

Prevention of Modification & alteration of data o r information

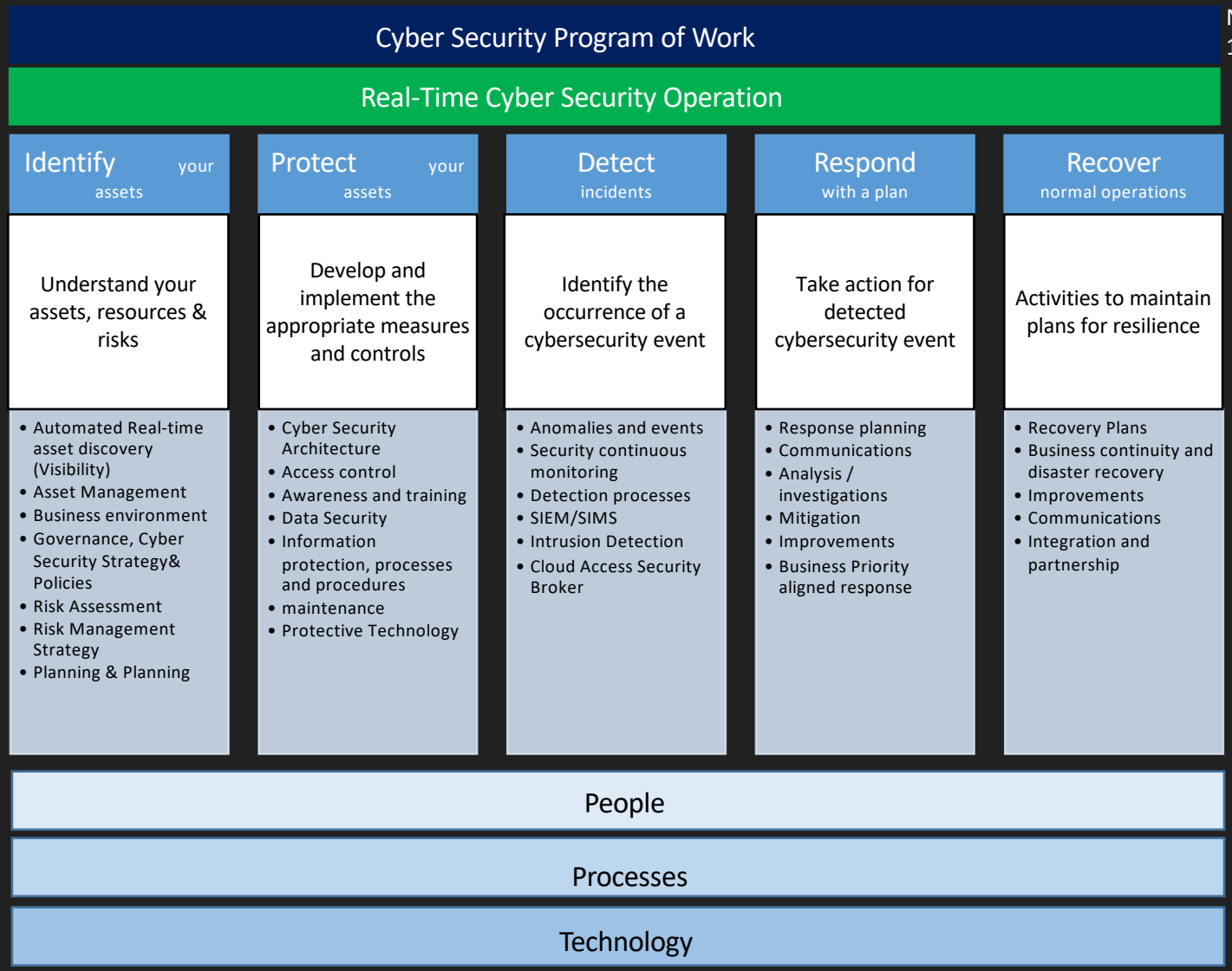
Availability

Systems availability for Appropriate operational use

Resilience

Ability to withstand and be able to operate even after an incident with minimal interruption

Cyber Security Value Chain

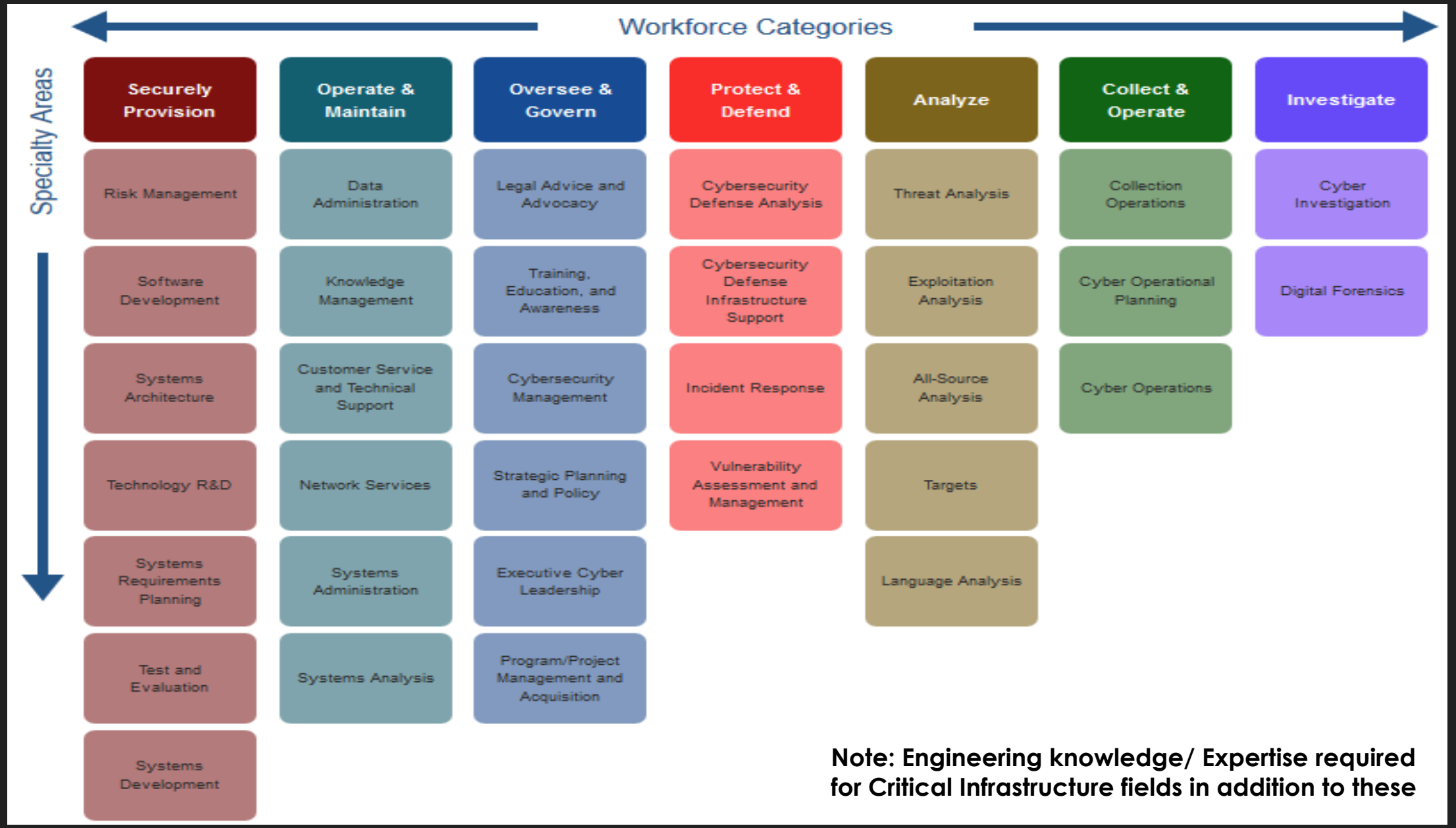


Note:

1. Every part of the Value Chain must be implement for a comprehensive Cyber posture

Key Functional Areas Derived

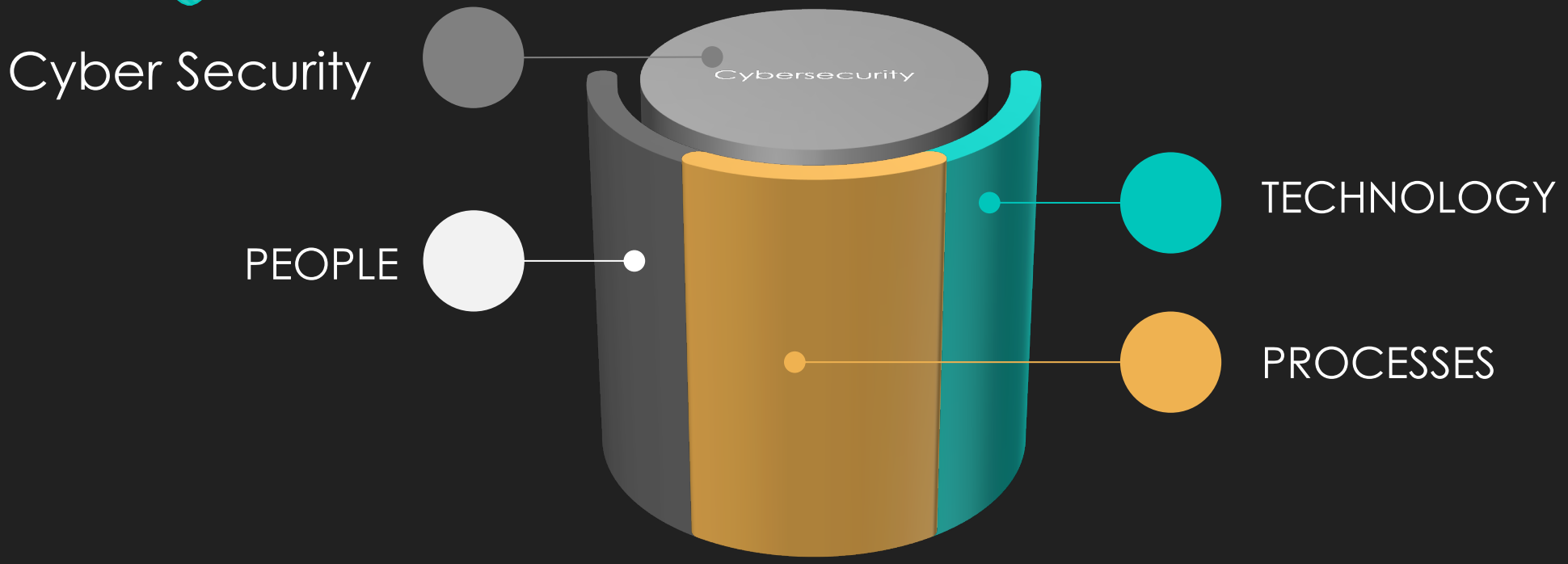
Critical Areas



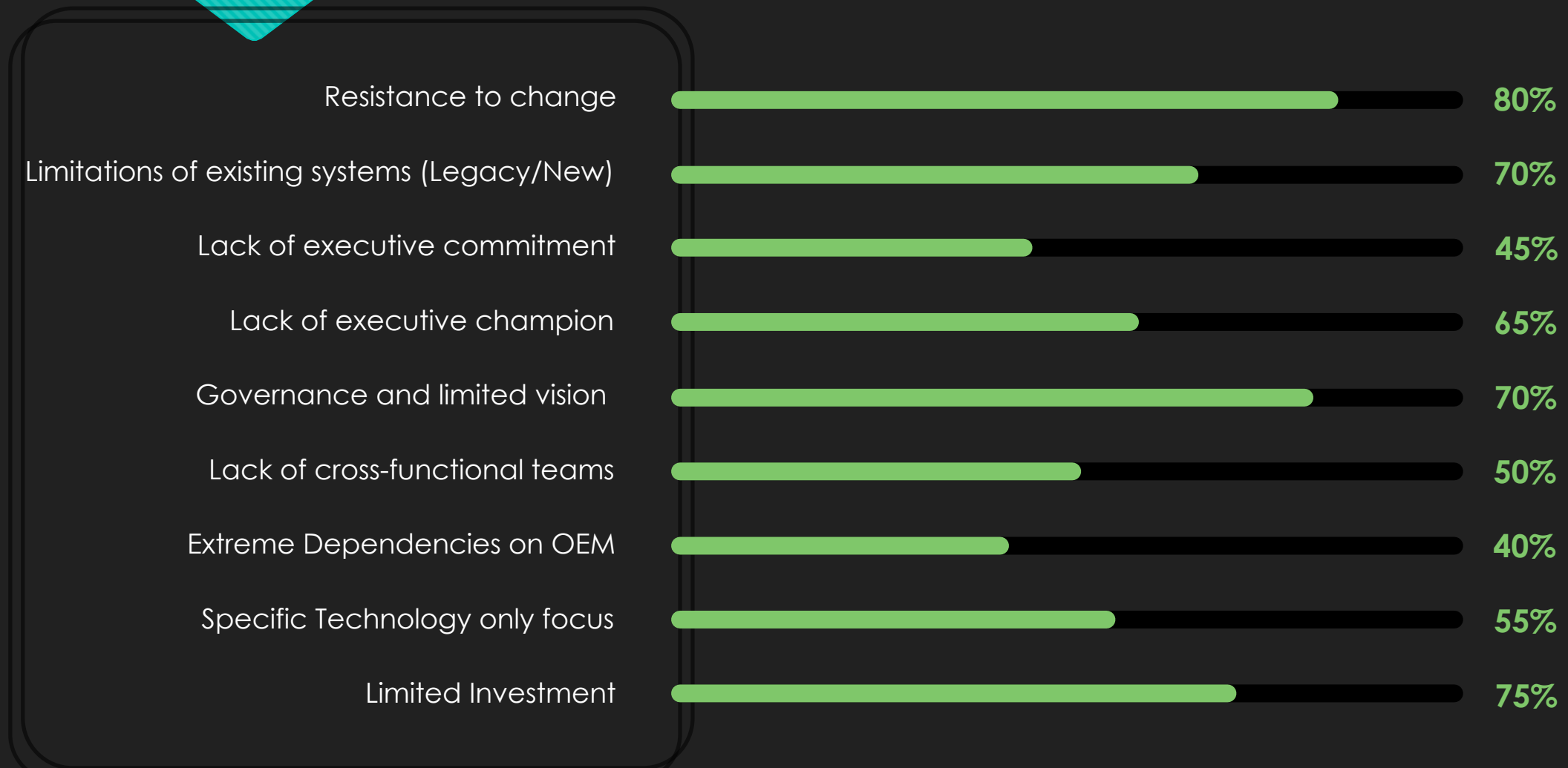
Note: Engineering knowledge/ Expertise required for Critical Infrastructure fields in addition to these

Source: https://www.sans.org/courses/niceframework/

Focus on People, Processes, Technology



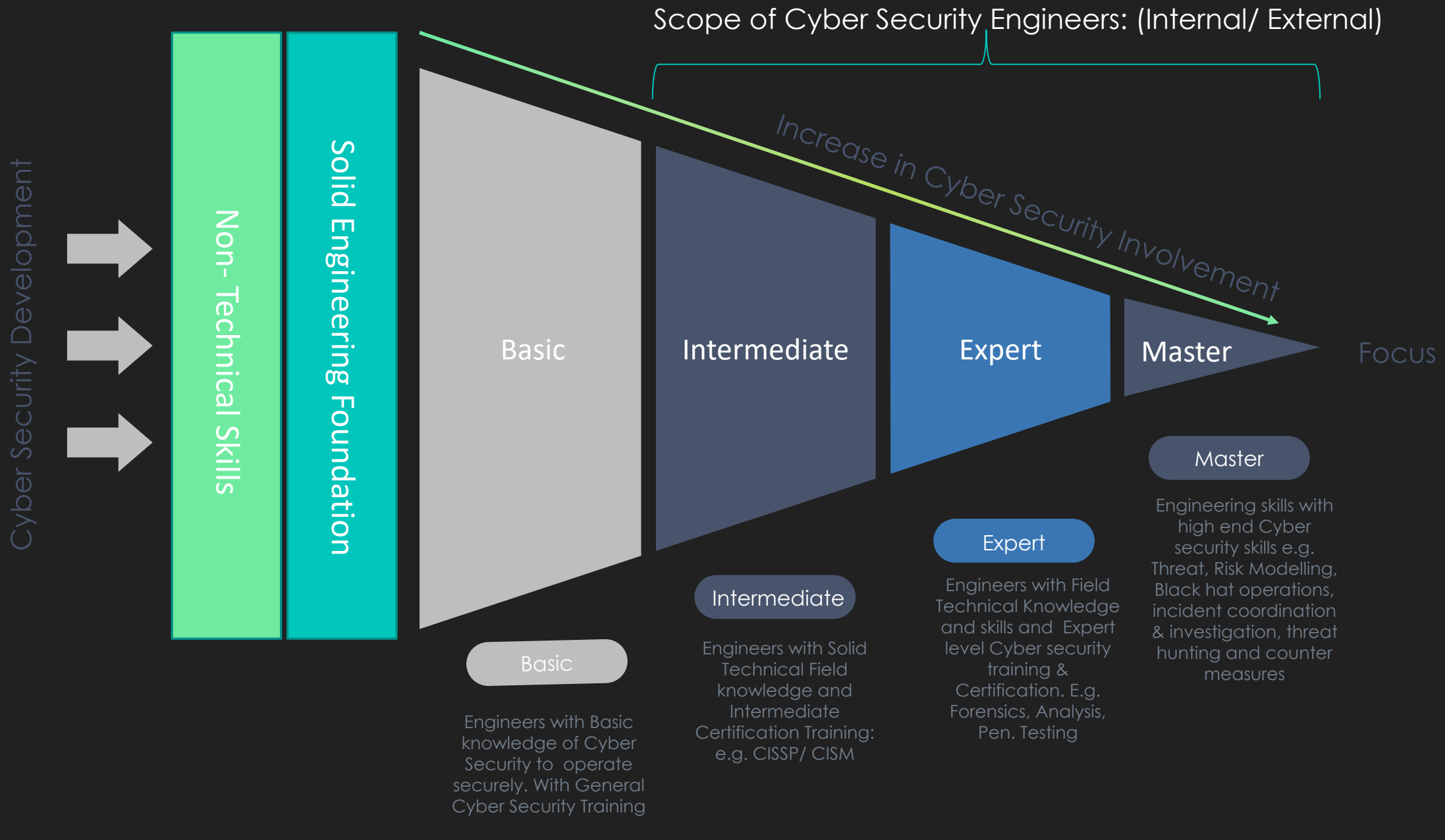
Barriers Resulting in Conventional ways

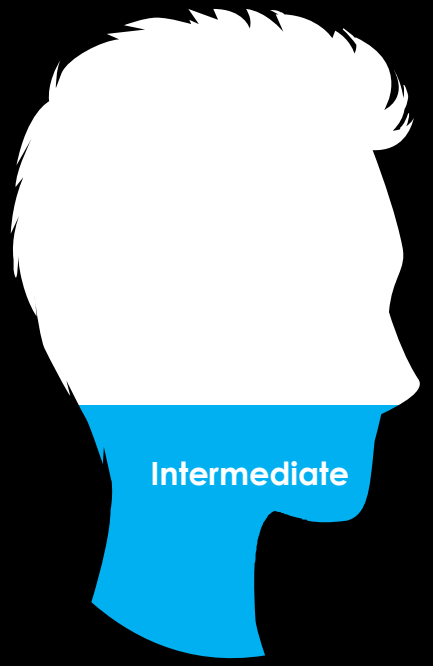


People

- Conventional Engineering Approach to Cyber Security Skills
  - Dual responsibility resulting in limited Cyber Security Focus
  - Limited Expertise creation goals and approach
  - No differentiation of various levels of Skills across value chain
  - Limited structures supporting Cyber Security in critical infrastructure

People… (Goal)


Scope of Cyber Security Engineers: (Internal/ External)
Increase in Cyber Security Involvement
Cyber Security Development
Non- Technical Skills
Solid Engineering Foundation
Basic
Intermediate
Expert
Master
Focus
Basic
Engineers with Basic knowledge of Cyber Security to operate securely. With General Cyber Security Training
Intermediate
Engineers with Solid Technical Field knowledge and Intermediate Certification Training: e.g. CISSP/ CISM
Expert
Engineers with Field Technical Knowledge and skills and Expert level Cyber security training & Certification. E.g. Forensics, Analysis, Pen. Testing
Master
Engineering skills with high end Cyber security skills e.g. Threat, Risk Modelling, Black hat operations, incident coordination & investigation, threat hunting and counter measures



Cyber Security

Engineering

Non-Technical

Cyber Security

Engineering

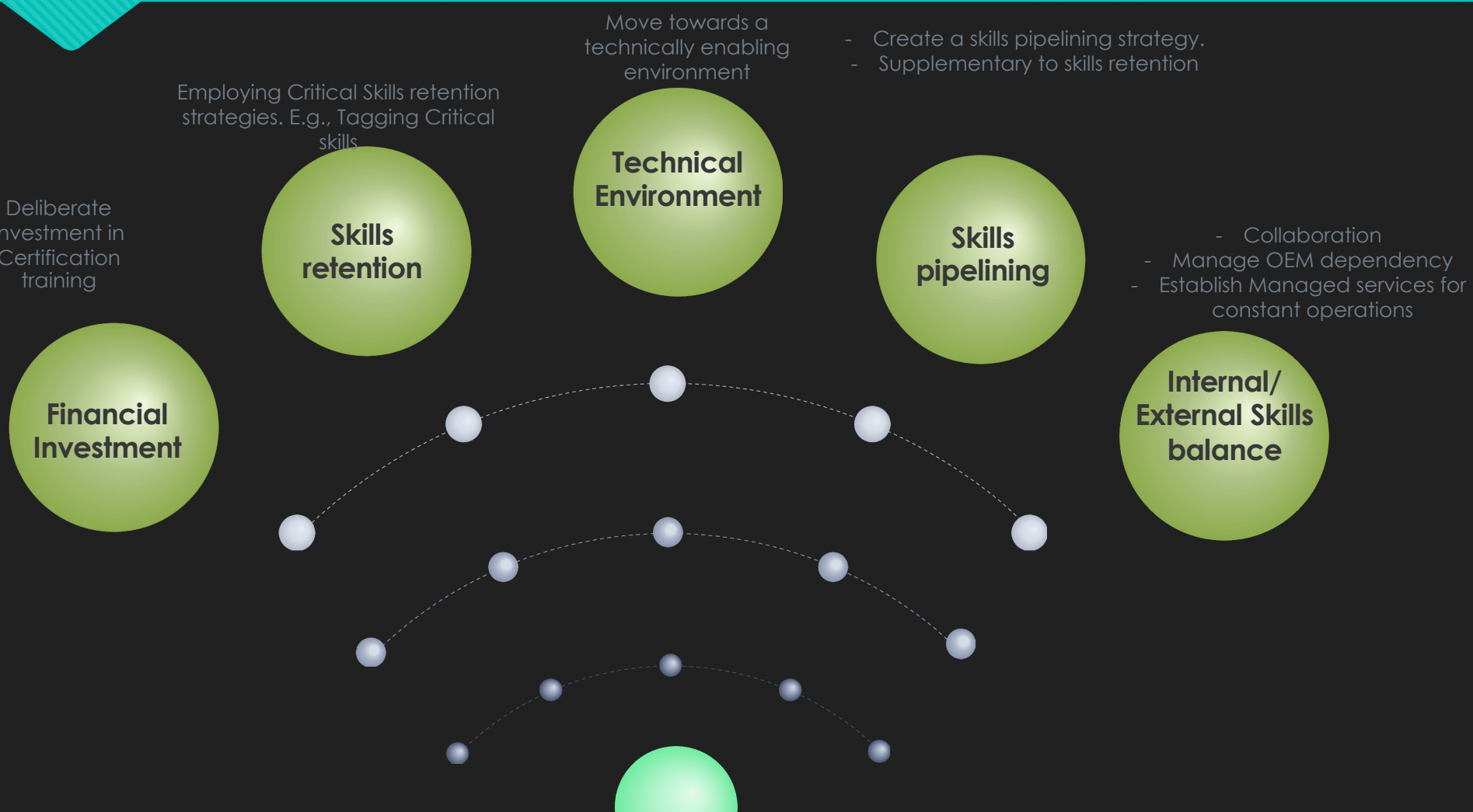
Non- Technical

Cyber Security

Engineering

Non-Technical

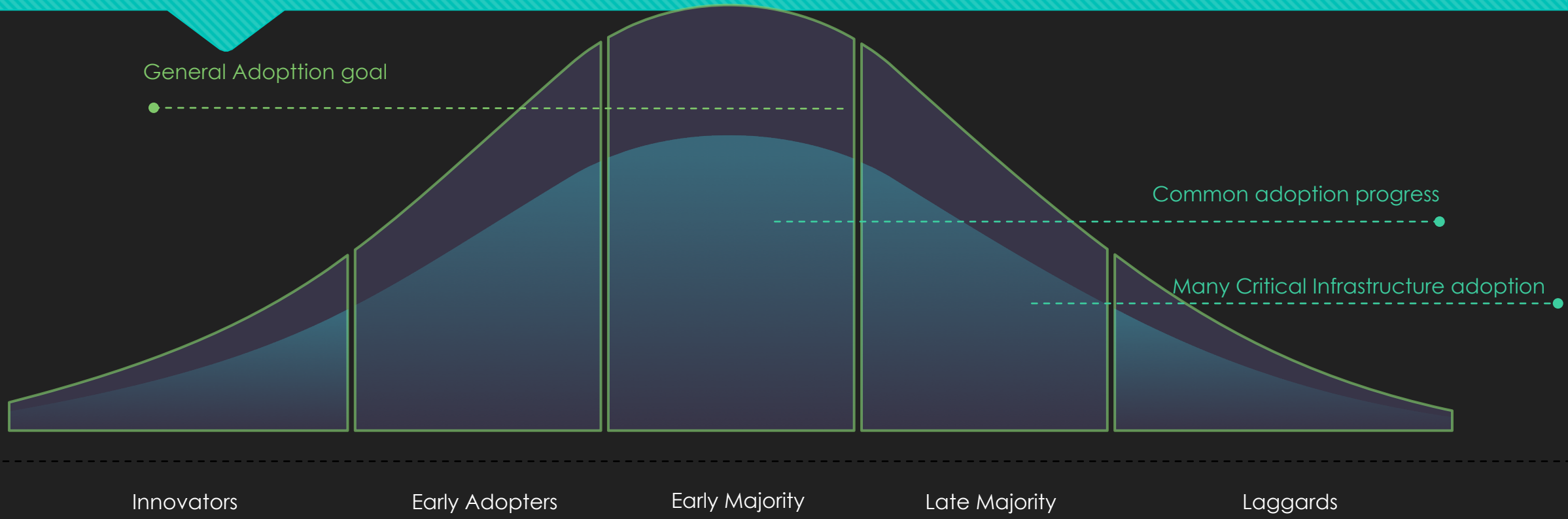
People… (Goal Drivers)



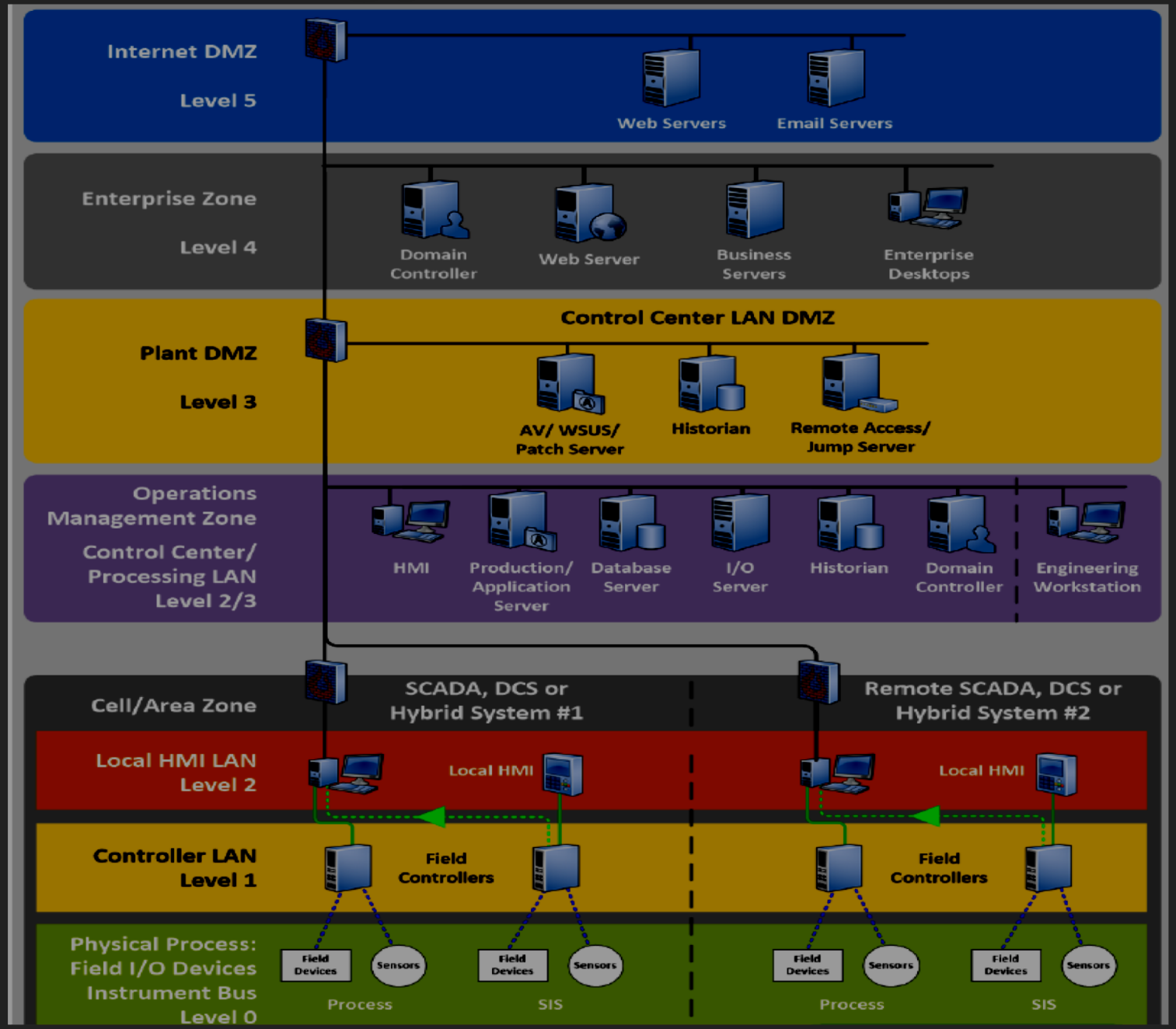
Technology

- Conventional Engineering Approach to Technology
  - Adoption rate "Culture" of technology in critical Infrastructure
  - Legacy systems and Obsolete technology (including retrofitting issues)
  - Limited Design and Architecture = "Product Focused" approach.

Technology... Technology Adoption

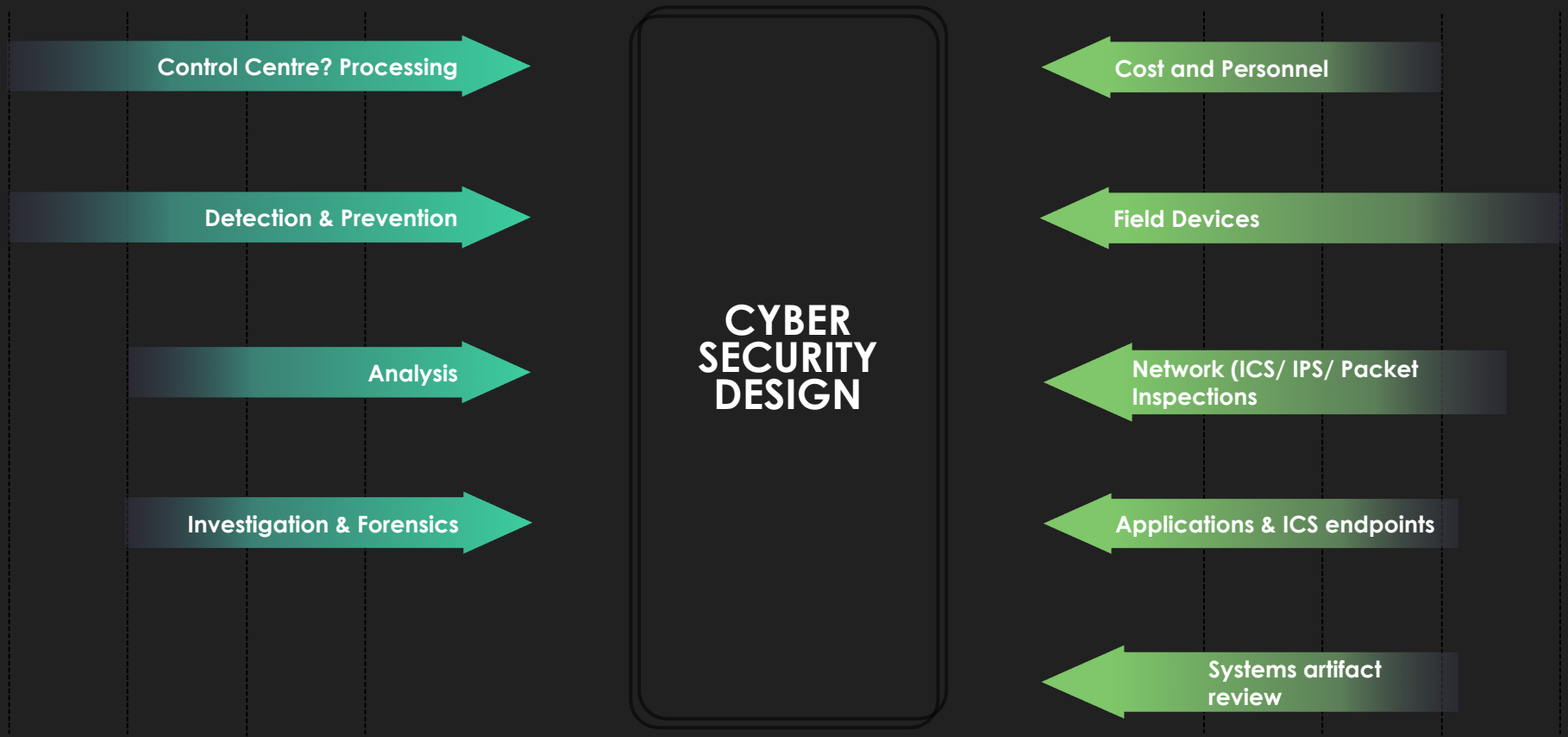


Technology… Design & Architecture Driven Implementation

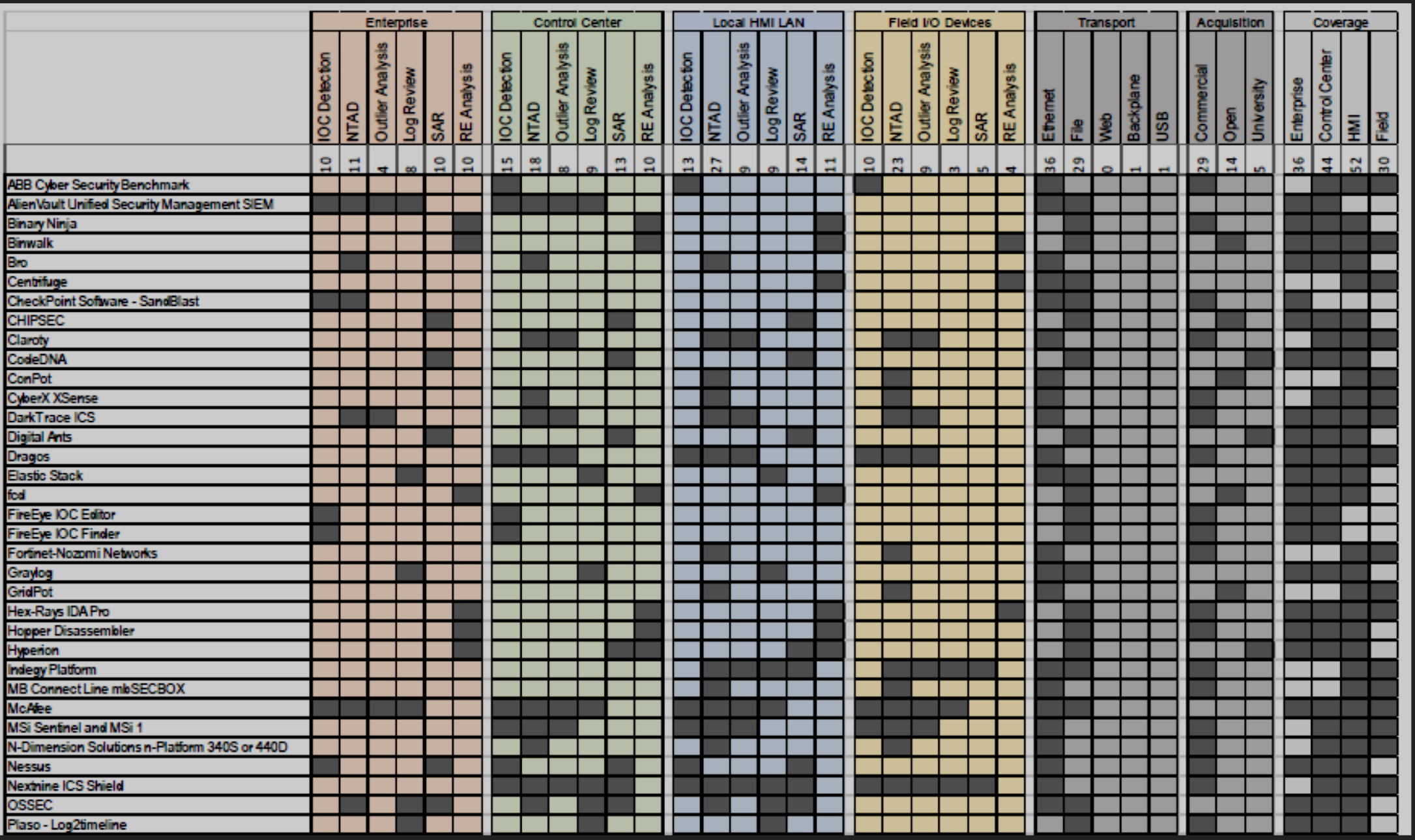


Source: A Survey of Security Tools for ICS Environment

Technology… Design & Architecture Driven Implementation



Technology… Matrix

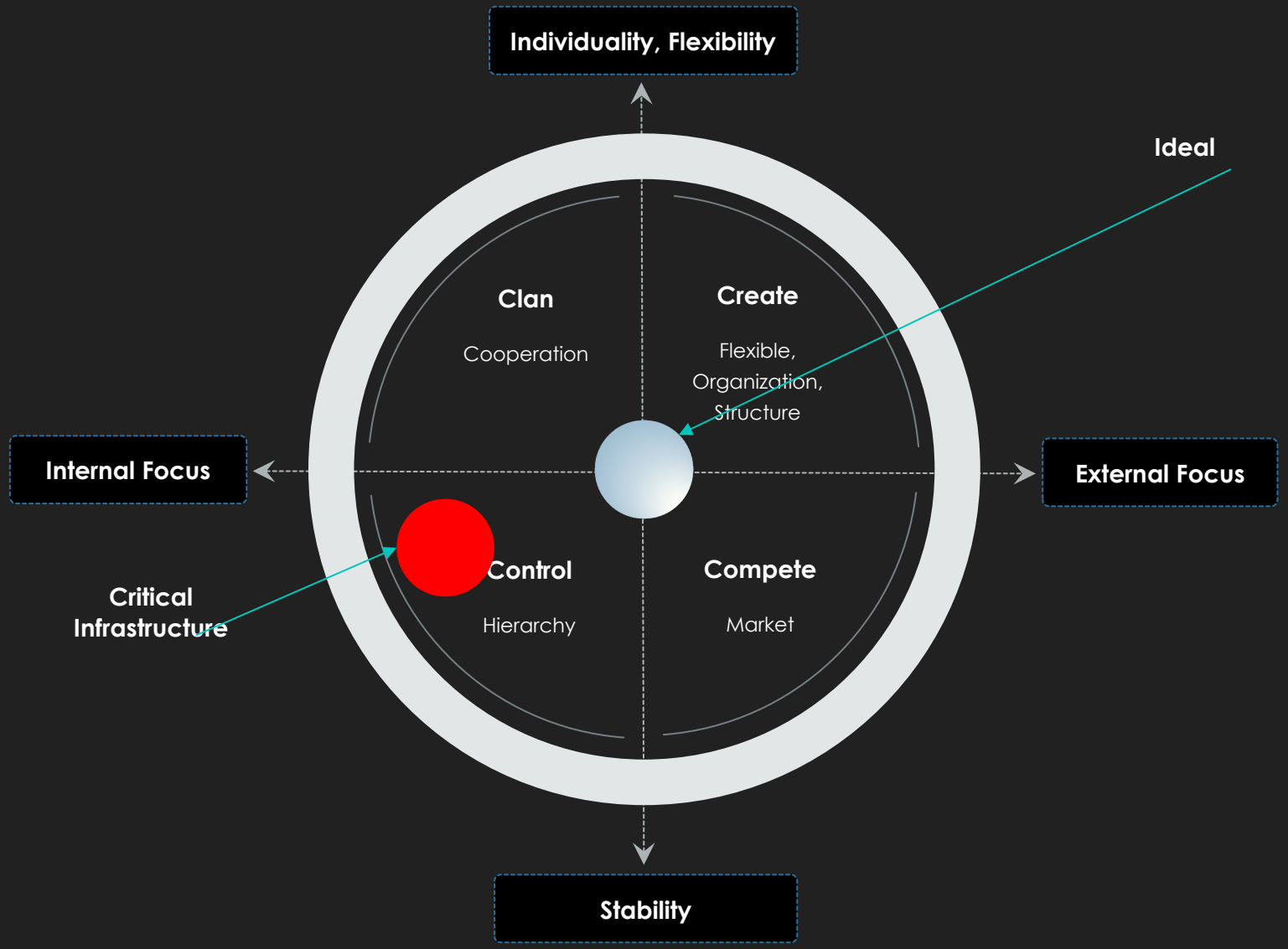


Source: A Survey of Security Tools for ICS Environment

Processes

- Conventional Engineering Approach to Processes
- Current Drivers:
  - Mission Critical System (Availability)
  - Safety and Operational Concerns
  - Uncertainty of New Technologies
- This however translates into Cyber Security technology: which is used to ensure continuation of operations

Processes… Competing Values Framework (CVF)

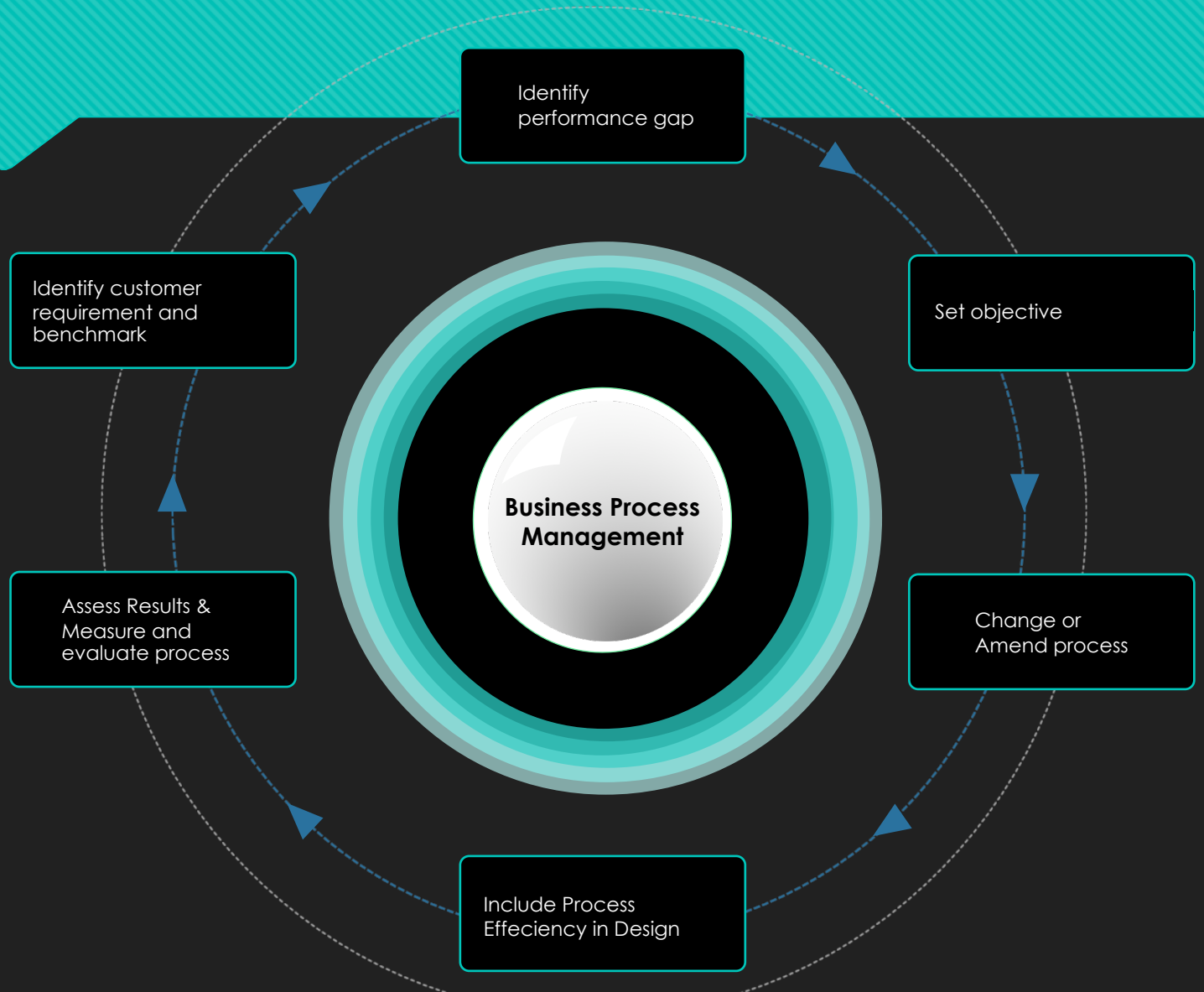


The Competing Values Framework is a theory that was developed initially from research conducted on the major indicators of effective organizations in terms of processes. (Quinn and Rohrbaugh)

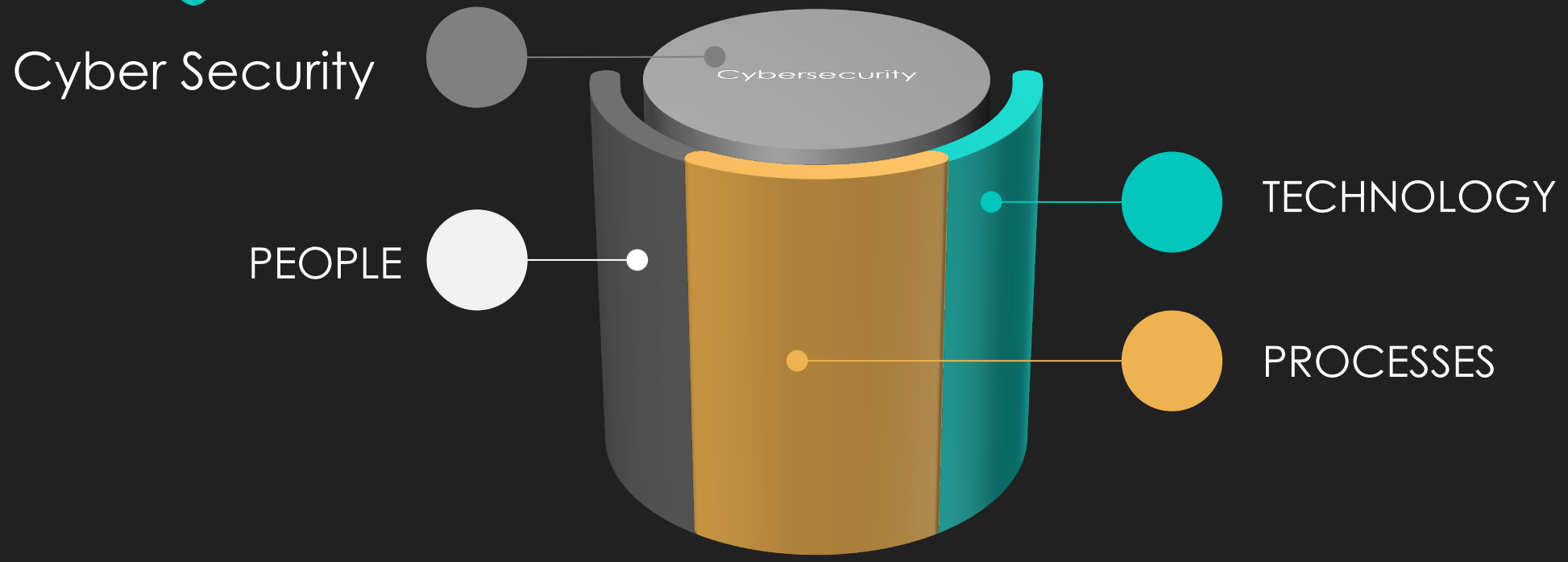
Processes…

- Drivers for Amendments of Conventional processes
  - Mission Critical System (Availability)
  - Safety and Operational Concerns
  - Uncertainty of New Technologies
- This however translates into Cyber Security technology: which is used to ensure continuation of operations

Process…


Identify performance gap
Set objective
Change or Amend process
Include Process Effeciency in Design
Assess Results & Measure and evaluate process
Identify customer requirement and benchmark
Business Process Management

Conclusion



To be Cybersecure, Conventional approaches have to amended across People, Processes and Technology for Cyber Security

END

Questions?