SAIEE Conference 2019: "Secure Connectivity"

Cyber Secure Future: Pitfalls in Conventional Engineering Approach

Lloyd Chego

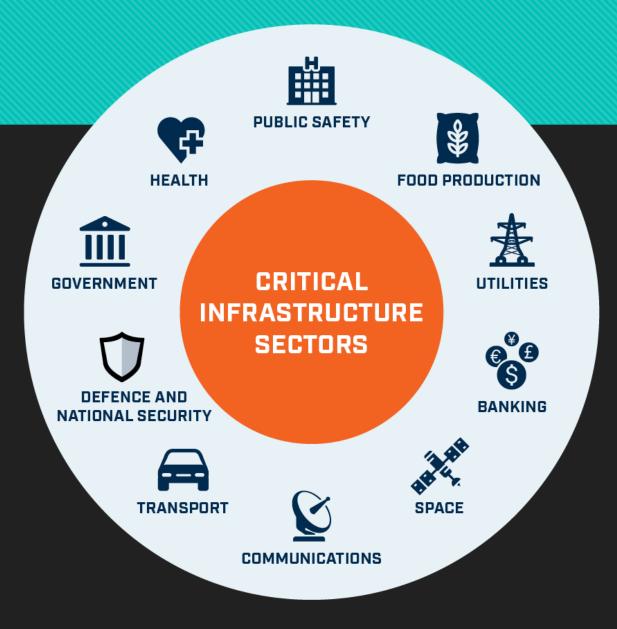
PhD(Elec)(candidate): UP; MSc(Elec): Wits, BEng(Elec): UP, Higher Cert. Cyber Security (Cum Laude): UJ

Contents

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

Introduction

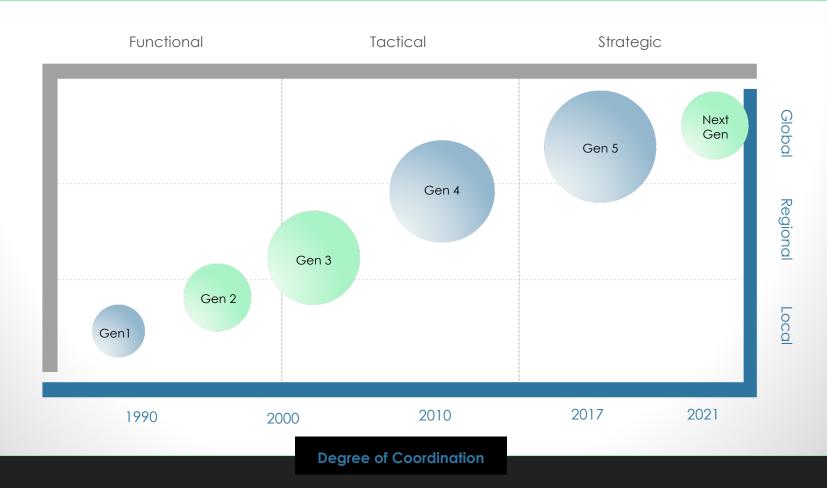
- Critical Infrastructure Focus: SA Focused
- What is conventional Engineering approach?
- What pitfalls results in this?
 - Inability to adequately respond to a Cyber Incident.
- Will focus on Processes, People and Technology



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

Evolution of Cyber Threat

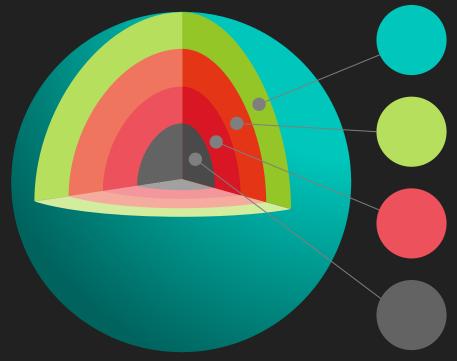
- Gen 1: 80's Viral based affacks. Mostly on Stand-alone PC's/ Systems Drove Anti-virus business
- Gen 2: 90's Network (Internet) based attacks, Firewall business
- Gen 3: 2000's Applications vulnerability exploit based attacks, Focus on Intrusion detection.
- Gen 4: Polymorphic Payloads (various forms) 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

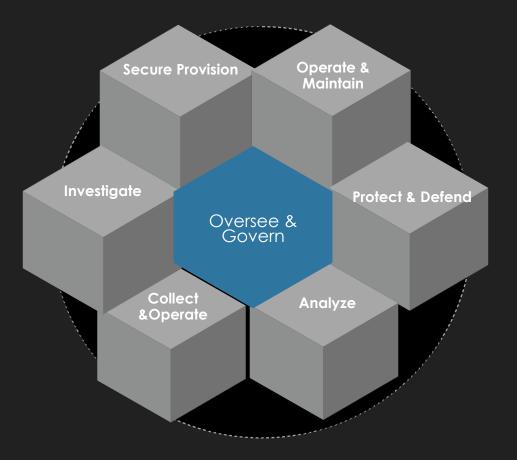
Resilience

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

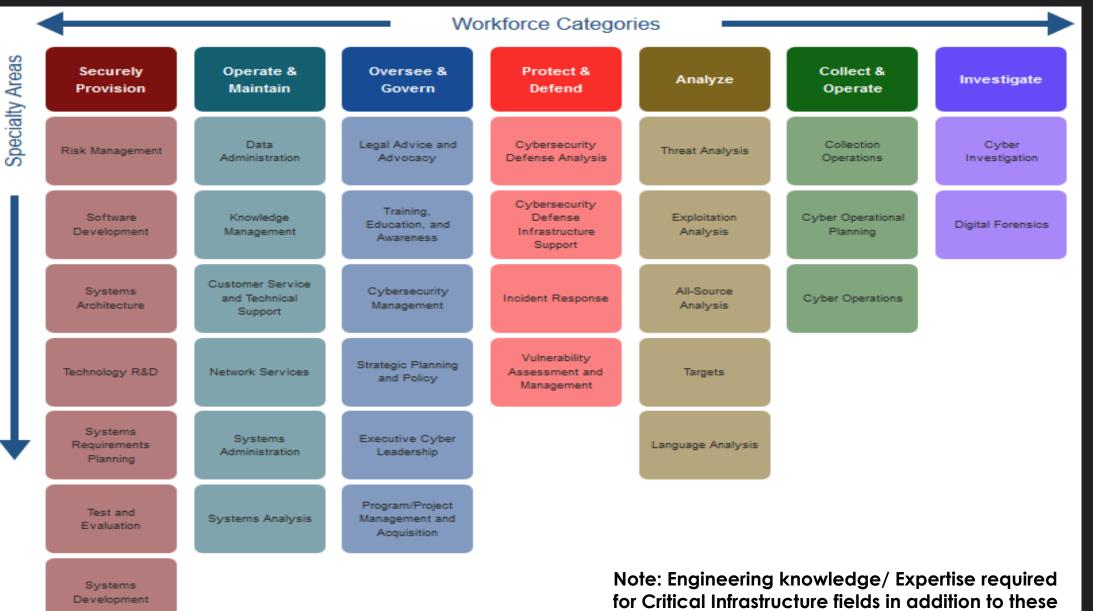
Cyber Security Value Chain

	Cyber Sec	urity Program of Worl	k		Note: 1. Every part of the Value Chain						
	Real-Time (Cyber Security Operat	ion		must be implement for a comprehensive Cyber posture						
Identify your assets	Protect your assets	Detect incidents	Respond with a plan	Recover normal operations							
Understand your assets, resources & risks	Develop and implement the appropriate measures and controls	Identify the occurrence of a cybersecurity event	Take action for detected cybersecurity event	Activities to maintain plans for resilience							
 Automated Real-time asset discovery (Visibility) Asset Management Business environment Governance, Cyber Security Strategy& Policies Risk Assessment Risk Management Strategy Planning & Planning 	 Cyber Security Architecture Access control Awareness and training Data Security Information protection, processes and procedures maintenance Protective Technology 	 Anomalies and events Security continuous monitoring Detection processes SIEM/SIMS Intrusion Detection Cloud Access Security Broker 	 Response planning Communications Analysis / investigations Mitigation Improvements Business Priority aligned response 	 Recovery Plans Business continuity and disaster recovery Improvements Communications Integration and partnership 							
		People									
		Processes									
Security Strategy& Policies protection, processes and procedures • Cloud Access Security Broker • Business Priority aligned response partnership • Risk Assessment • Risk Management Strategy • Planning & Planning • Protective Technology • Cloud Access Security Broker • Business Priority aligned response partnership • Planning & Planning • Protective Technology • Cloud Access Security Broker • Business Priority aligned response partnership											

Key Functional Areas Derived

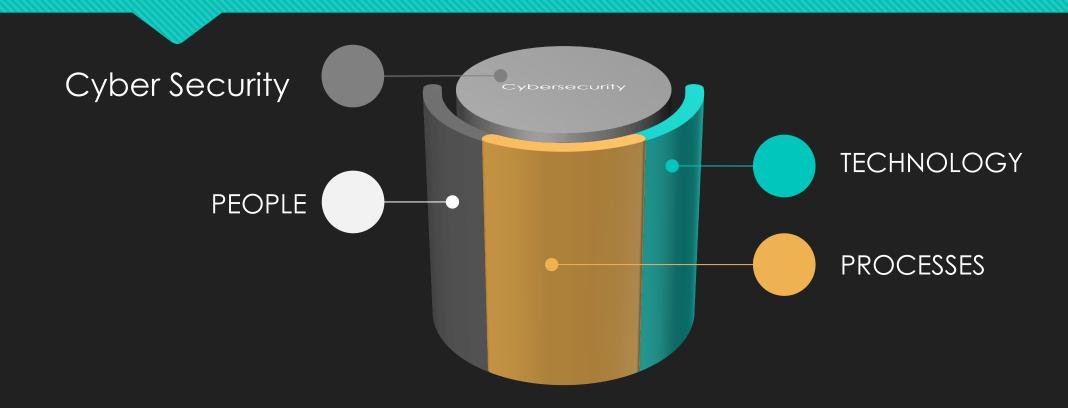


Critical Areas



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

Focus on People, Processes, Technology



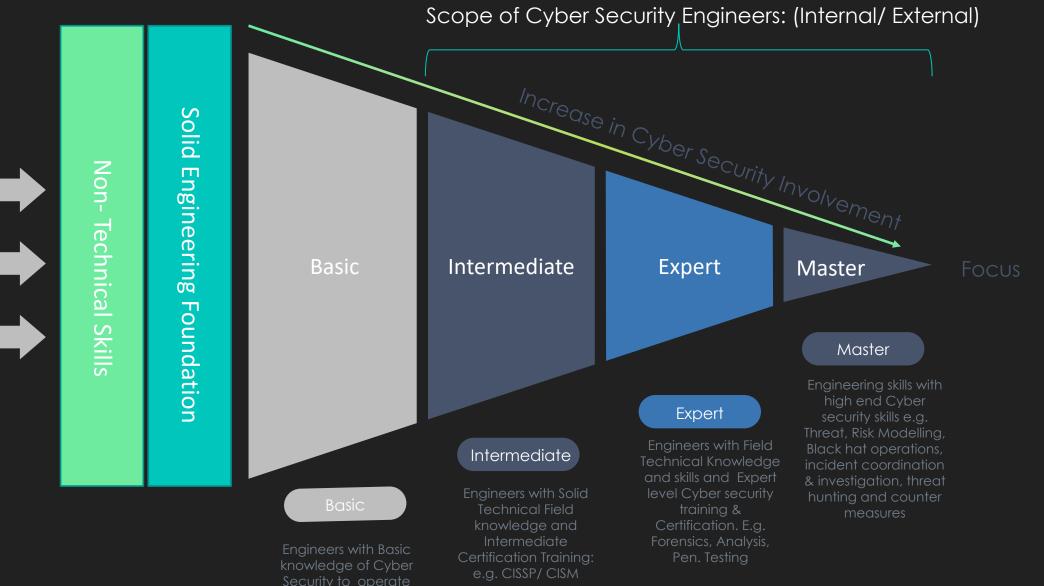
Barriers Resulting in Conventional ways



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)



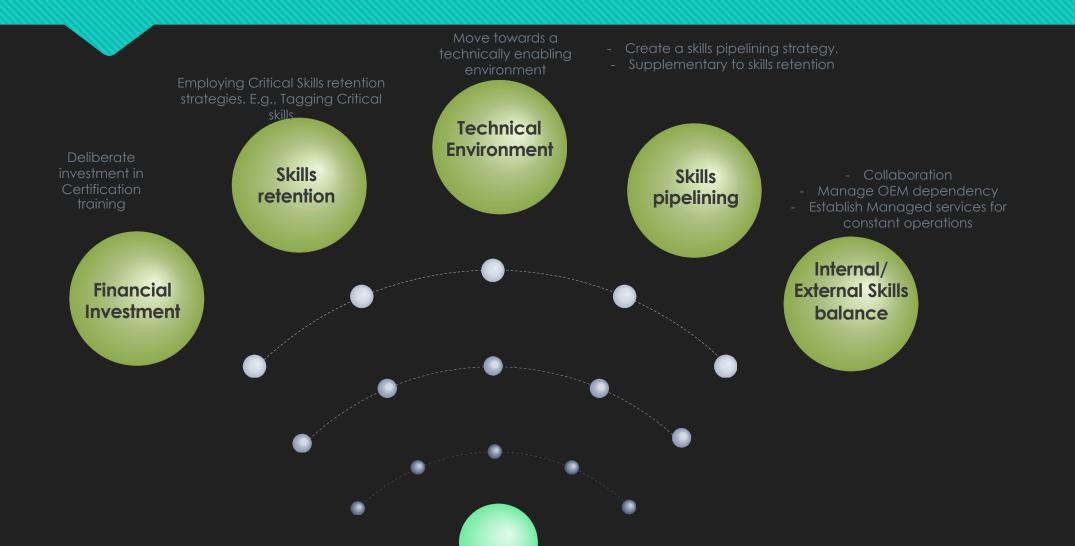
Cyber Security Training

Cyber Security Develop





People... (Goal Drivers)

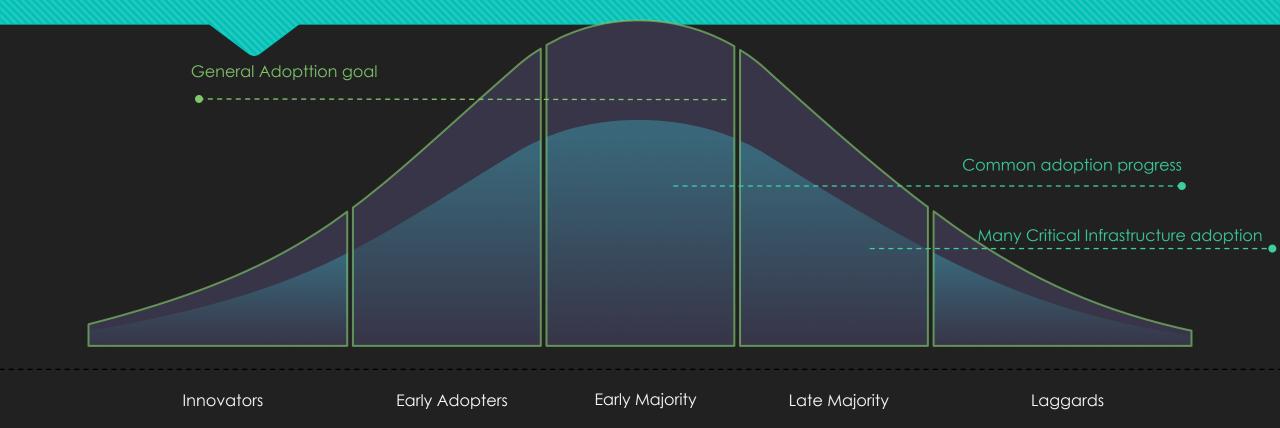




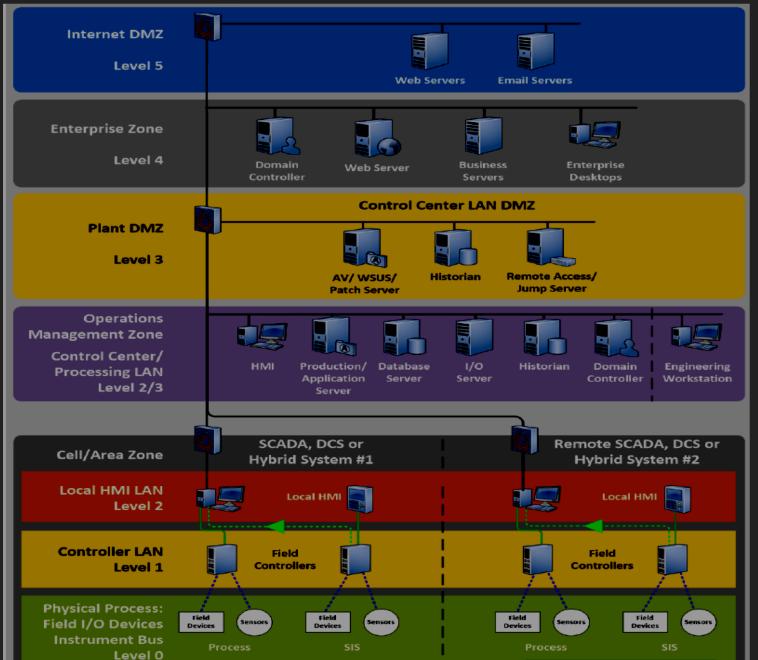
• Conventional Engineering Approach to Technology

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

Technology... Technology Adoption

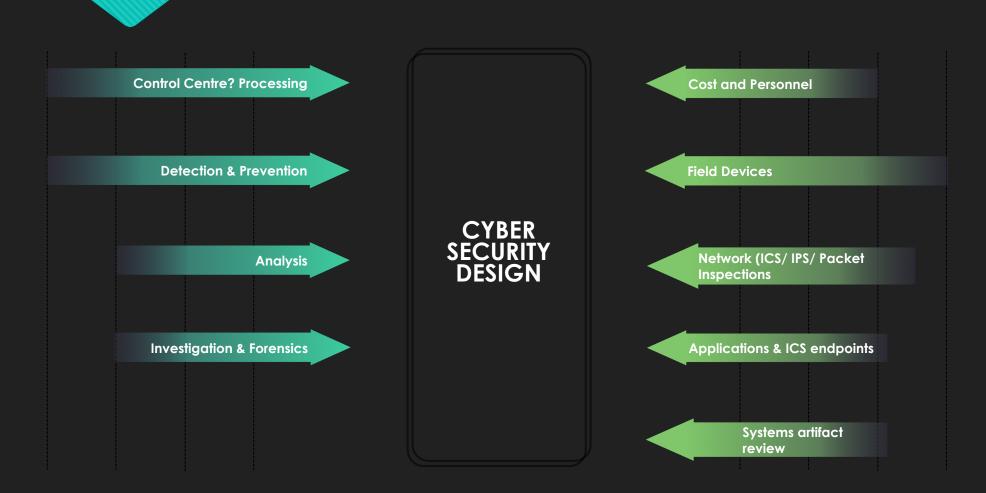


Technology... Design & Architecture Driven Implementation



Source: A Survey of Security Tools for ICS Environment

Technology... Design & Architecture Driven Implementation



Technology... Matrix

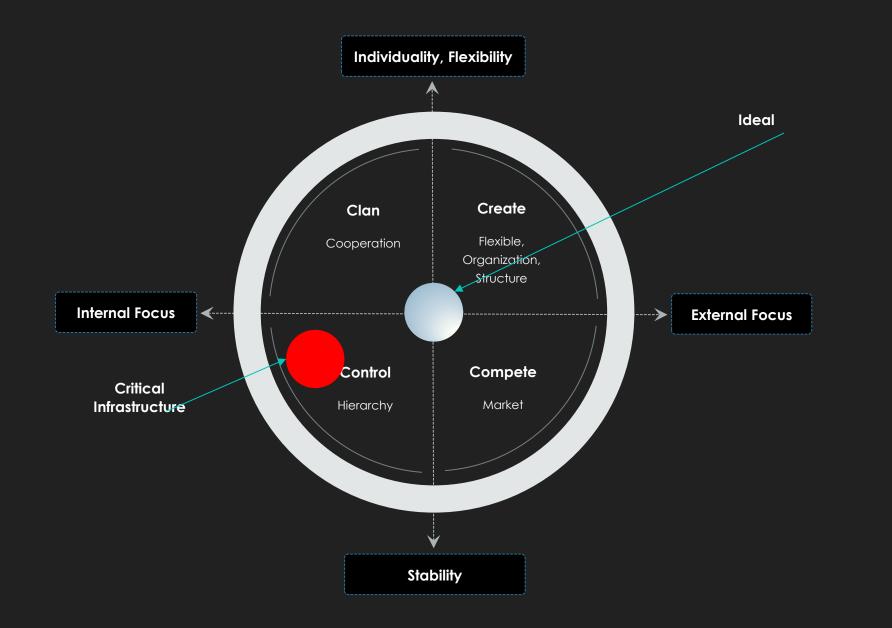
	Enterprise				Control Center						Local HMI LAN							Field		Devi	ces		Transport				Acquisition			Coverage			1		
										T													Т			Т	T							Ť	1
	IOC Detection	NTAD	Outlier Analysis	Log Review	SAR	RE Analysis	IOC Detection	NTAD	Outlier Analysis	Log Review	SAR	RE Analysis	IOC Detection	NTAD	Outlier Analysis	Log Review	SAR	RE Analysis	IOC Detection	NTAD	Outlier Analysis	Log Review	SAR	RE Analysis	Effernet	FII I B Mich	Backplane	USB	Commercial	Open	University	Enterprise	Control Center	HMI Field	
	10	11	4		10	10	15	18	80	6	13	10	13	27	6	6	14	11	10	23	6		2	4	36	29			29	14	5	36	44	52 30	
ABB Cyber Security Benchmark																																			
AlienVault Unified Security Management SIEM]
Binary Ninja]
Binwalk																																			
Bro]
Centrifuge																																			
CheckPoint Software - SandBlast																																			1
CHIPSEC																																			1
Claroty																																			1
CodeDNA																																			1
ConPot																																			
CyberX XSense																																			1
DarkTrace ICS																																			1
Digital Ants																																			1
Dragos																																			1
Elastic Stack																																			1
fcal									1																										1
FireEye IOC Editor																																			1
FireEye IOC Finder																																			1
Fortinet-Nozomi Networks																																			1
Graylog																																			1
GridPot																																			1
Hex-Rays IDA Pro																																			1
Hopper Disassembler																																			1
Hyperion																																			1
Indegy Platform																																			1
MB Connect Line mbSECBOX																																			1
McAnjee																																			1
MSi Sentinel and MSi 1																																			1
N-Dimension Solutions n-Platform 340S or 440D																																			1
Nessus																																			1
Nextnine ICS Shield																																			1
OSSEC																																			1
Plaso - Log2timeline																																			1

Source: A Survey of Security Tools for ICS Environment



- 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)

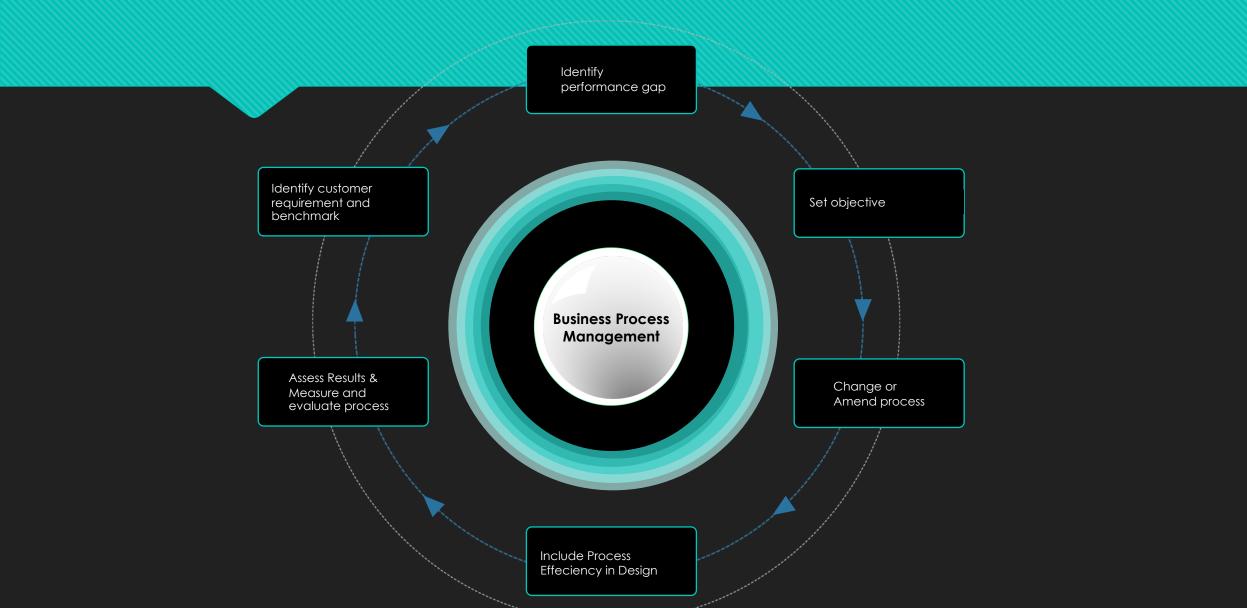


The Competing Values Framework is a theory that was developed initially from research conducted on the major indicators of effective organizations in terms of processes. (Quinn and Rohrbaugh)

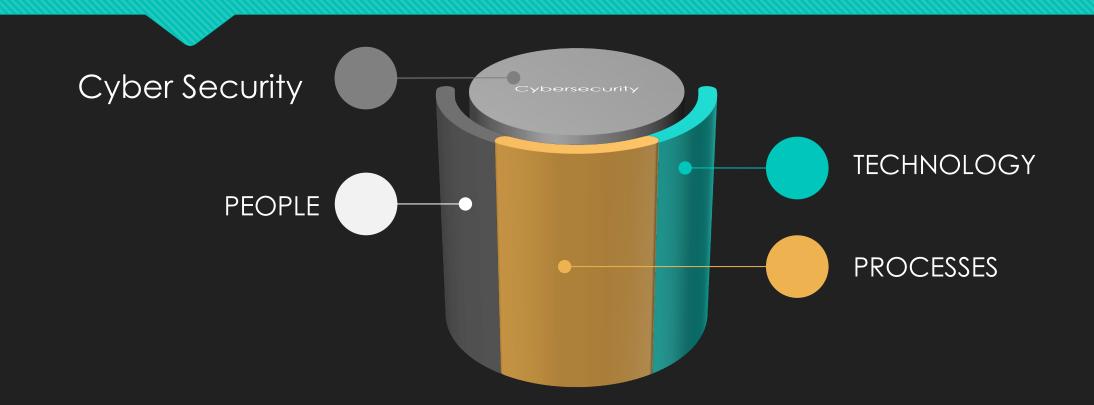
Processes...

- 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...



Conclusion



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



Questions?

