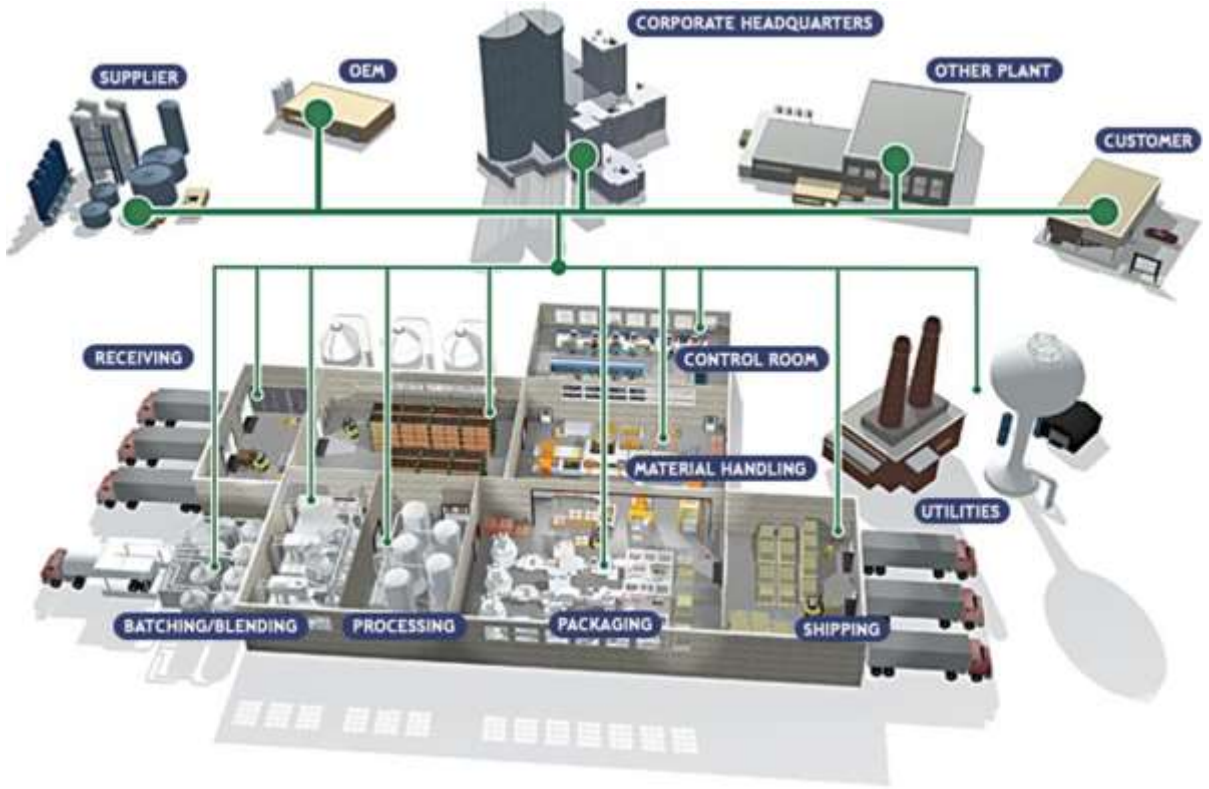
OLYMPIC
BREWERY S.A.

Smart Factory: Securing the future
12-2-2019

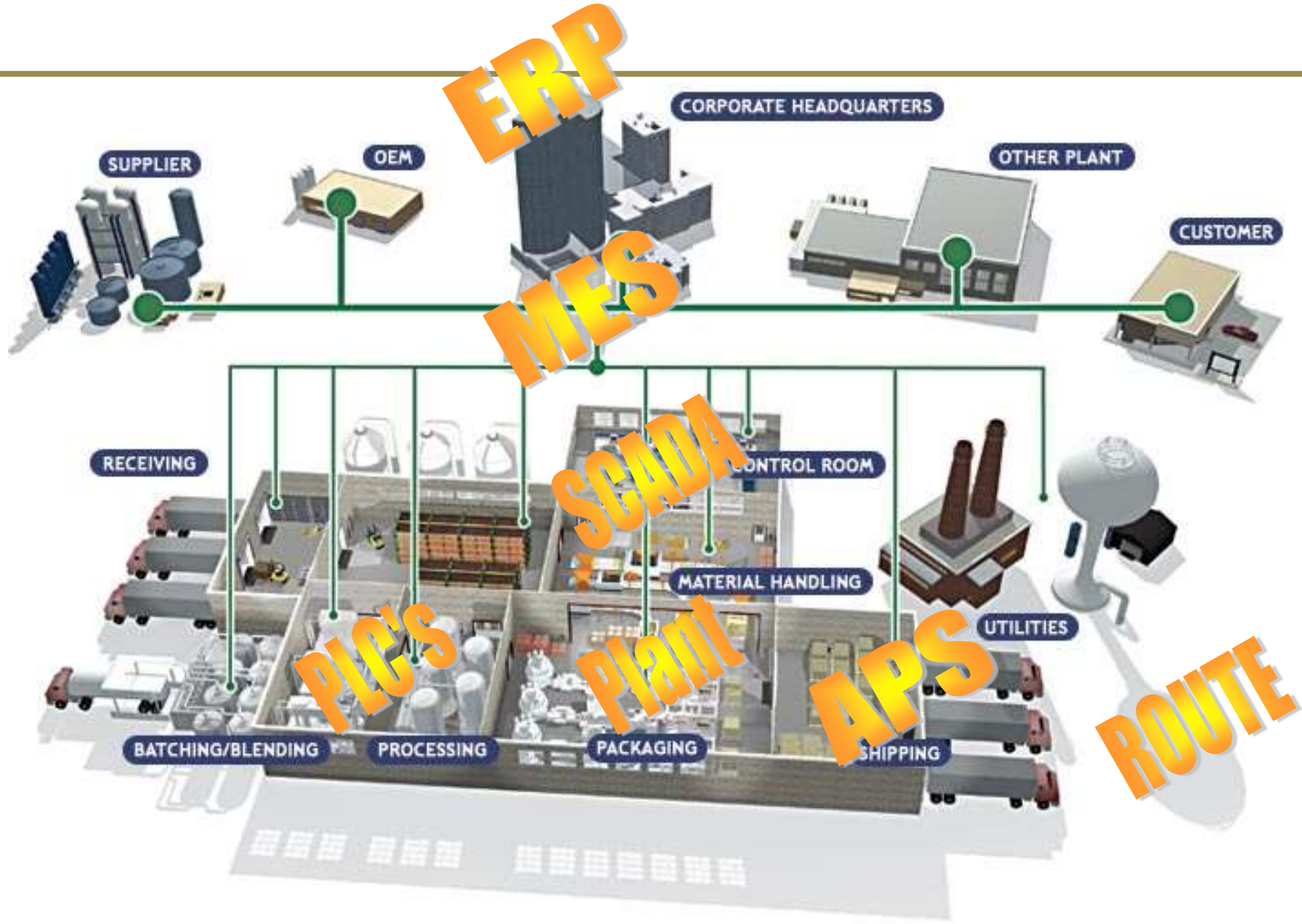
Need for Increased Security in Supply Chain processes (Why)

- Tampering and unauthorized replacement of products
- Increased Integration of IT systems
  - IT systems are interlinked. Examples are ERP for manufacturing, CRM for sales and operations, and TMS for transport management. Unauthorised access to one system can lead to access to the next one
- Increased Risk due to complexity
  - IOT
  - Control Systems
- Shift in the attack patterns
  - Increased physical security leads to attacks during the day
- Sophistication of attacks
- Inside threats increasing

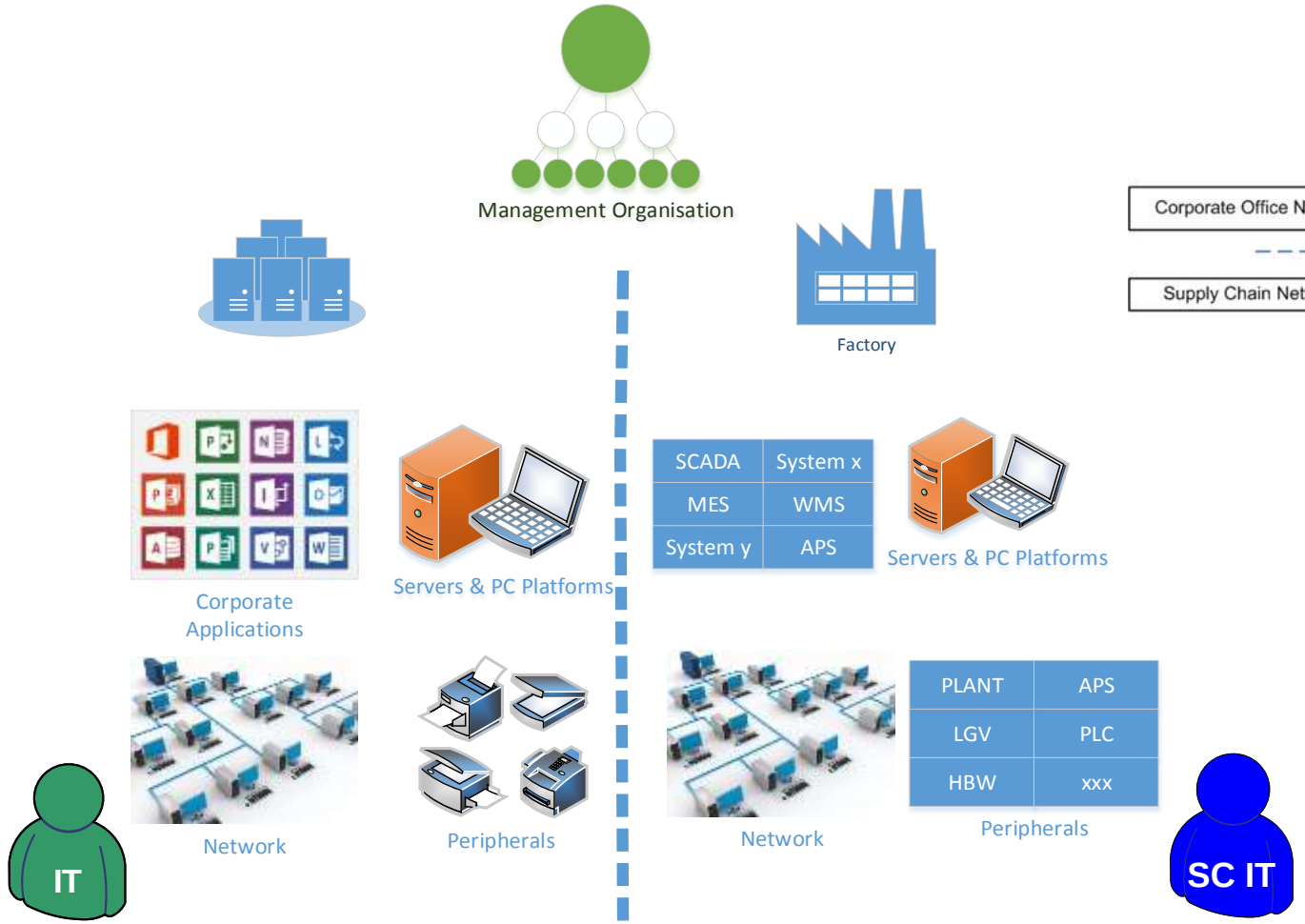


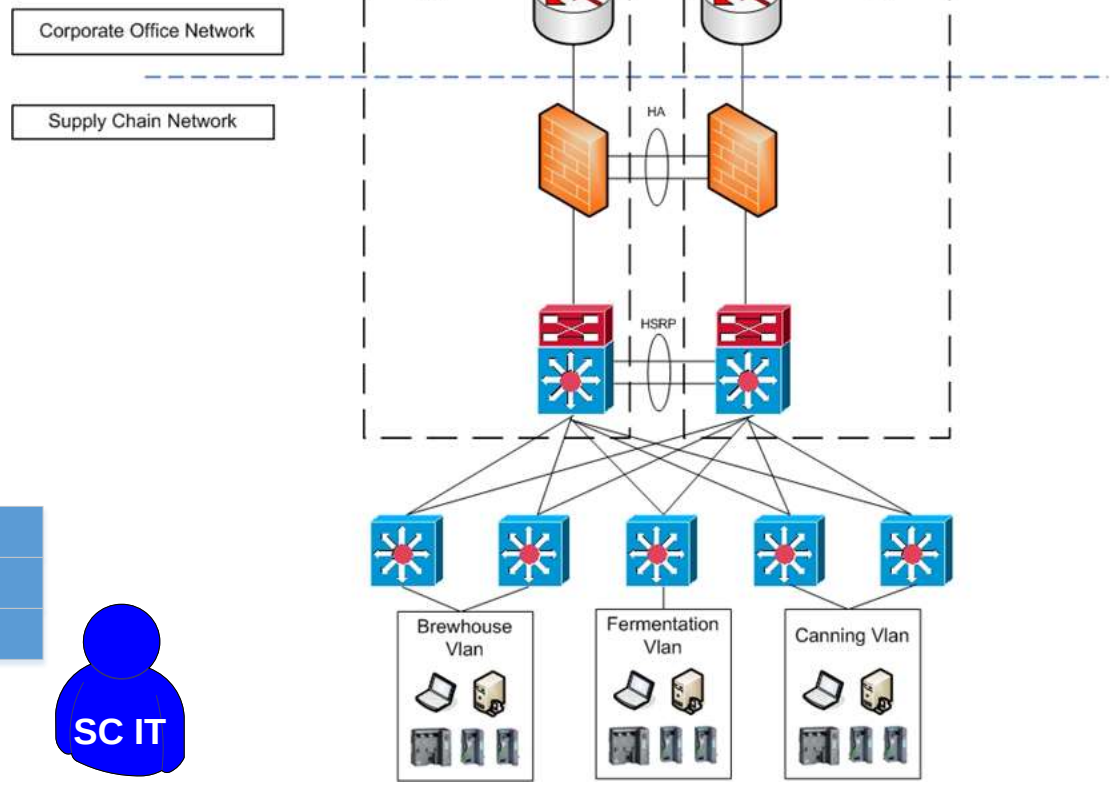
Supply Chain Process Layout

OLYMPIC BREWERY S.A.



Corporate Vs Supply Chain Environments:
Physical Boundaries – Need to identify & define





Basic Principles of securing the factory

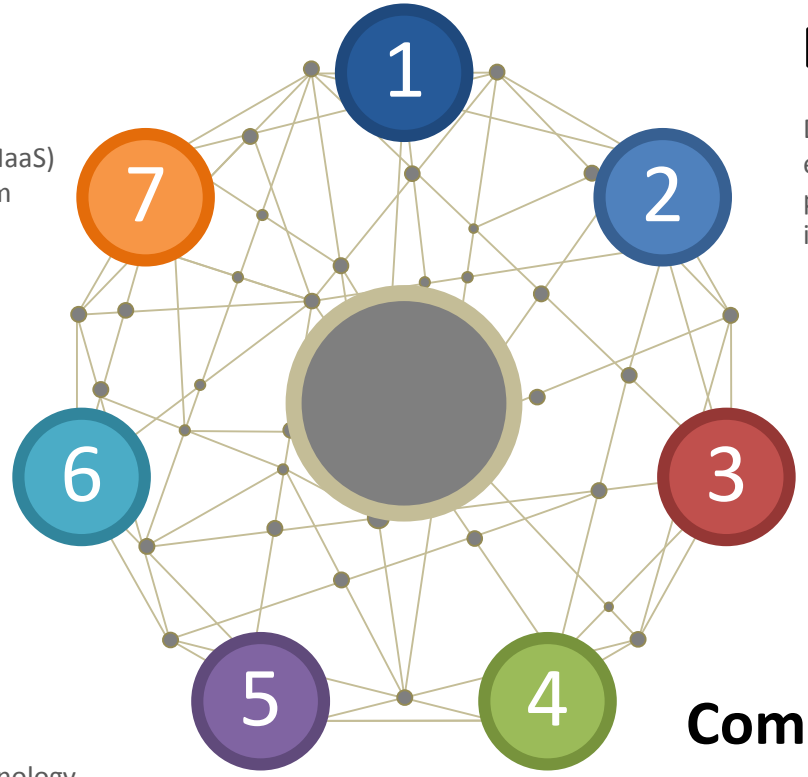
Key Elements in the first 30, 60, 90 days…

Build

- Build the appropriate capabilities, organization setup to deliver the program.
- Ensure Management On Board

Monitor & Respond

Implement a SIEM (In House or SIEMaaS) and Security Incident Response Team



Educate

Define the requirements of an education and behavioral change program and engage with internal/external experts

Evaluate

Evaluate results and adjust appropriately the requirements & program

Fix

Fix the basics – unsupported equipment, reduce/control privileged users and patching backlog

Implement

Implement the immediate technology changes, begin POC activities and define wider program deliverables

Comply

Sign off the 'Minimum Standards' and ensure there is a clear understanding of **impact of non-compliance**

Building the detailed ‘Minimum Standard’ for each discipline

Each discipline will have a detailed Minimum Standard for their key deliverables – to be developed by the Security team and agreed with each Discipline lead, and Supply Chain

Disciplines & responsibilities

Digital Workplace
- PC’s
- Tablets
- Mobile devices
- Tools
- Process & governance

Networking
- Internet
- DMZ
- Enterprise
- Extranet
- Supply Chain
- Datacentre

Security & Access Management
- Tools & services
- Process & governance
- Audit & compliance
- Security Architecture
- Intelligence

Hosting
- Tools & Services
- Process & governance
- Operating systems
- Databases
- Middleware
- Application servers

Applications
- Application development
- Application administration
- Tools & services
- Process & governance

Digital Workplace

General	Device inventory	All devices must be registered in [redacted] with all relevant data.
	Software inventory	All software must be registered and managed through [redacted]
	Administrator privileges	O365 admin level must be based on least privilege and must have MFA. Local Administrator must be managed by Microsoft LAPS with unique passwords and one month rotation. Local Administrators group must be managed by GPO
	Email protection	O365 Exchange protection and advanced threat protection
	Audit logs & monitoring	High-risk/VIP users must have f[redacted]client installed
	User administration	Password resets Conditional Access control enabled for O365 MFA verification upon suspicious activity VPN profiles
PCs (Windows)	Configuration	Windows hardening policy via GPO Machine certificate must be deployed and current
	Endpoint protection	[redacted] must be installed and up to date with the latest signatures.
	Patching	Minimum patch level n-1 for OS and applications
	Browser protection	Browser policy enforcement via GPO
	Software policy	Only approved software installed
	VPN/Proxy	VPN or proxy client always-on
	Encryption	Full disk encryption must be enabled
	Synchronisation policy	Full synchronisation allowed No centrally managed backup of disk
Tablets	Mobile device management	[redacted] must be installed or device enrolled in In-Tune
	Configurat[illegible]	[illegible] In-Tune

Best Practice - The risks of loss or interruption of service can be managed through the following good practice examples:

OLYMPIC BREWERY S.A.

- Include network services in service catalogue
- HA resilient network design features and functionality should be considered, factoring in the system criticality and risk.
- Risk assessment process and service catalogue must include risks from a lack of high availability. Either accept risks or invest in HA.
- Network redundancy/resilience - multiple cables/paths, spanning tree, resilient routing, vrrp, hsrp
- HA network designs - HA router pairs, HA dual firewalls, HA teamed server NICs, HA Core switch pairs,
- Clear roles and responsibilities for systems end to end
- Well documented systems
- Spare hardware on site
- Regular, tested, fast and efficient backup and restore technologies and processes
- Running hot, warm or cold standby versions of the device
- Testing and Change management and rollback processes
- Knowing your network environment & technologies & risks
- Power - Multiple PSU's per chassis, resilient dual mains supply, battery backup, generator backup
- Managing security risks

OLYMPIC

BREWERY S.A.

Thank you!