Main Security Challenges with Convergence of IT & OT

(ISC)^2 SecureJohannesburg
6 October 2015

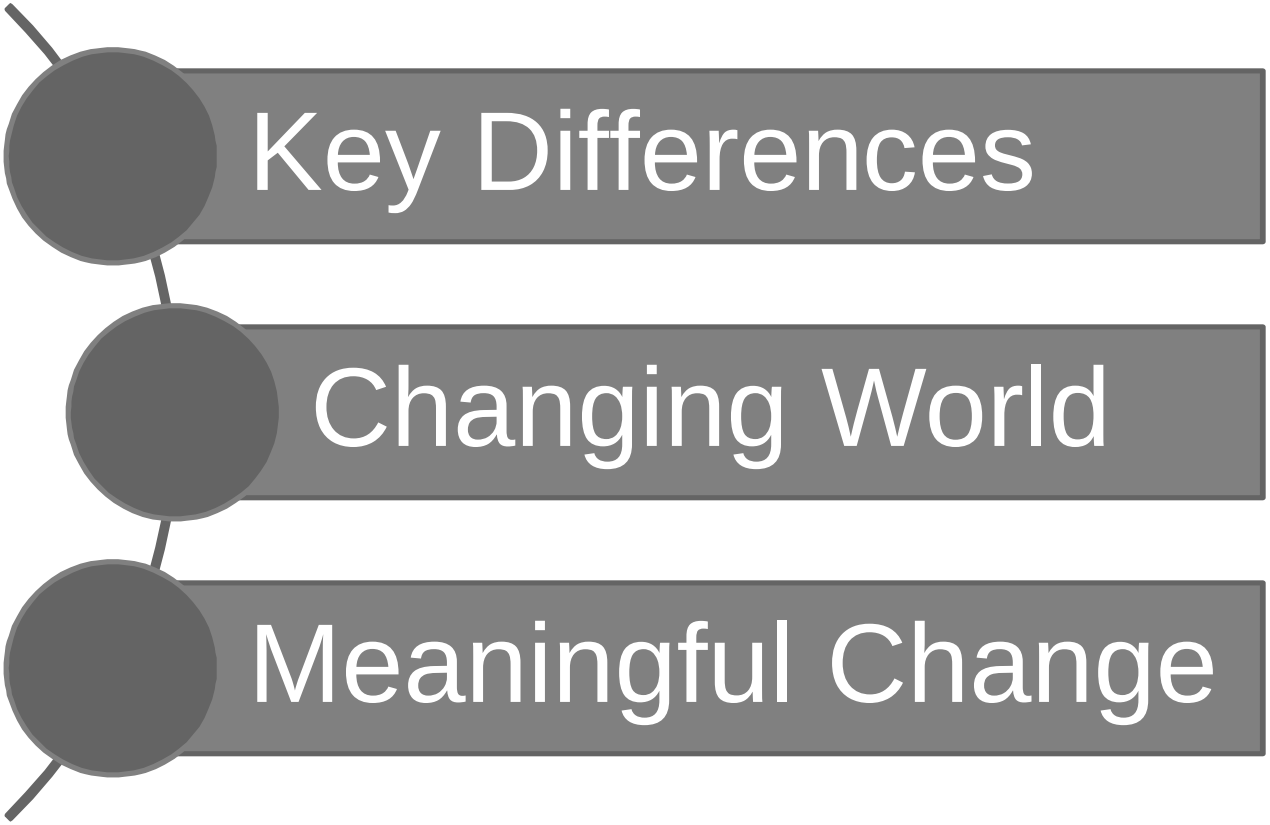
Justin Williams
Executive Director: CyberSecurity

EY
Building a better working world

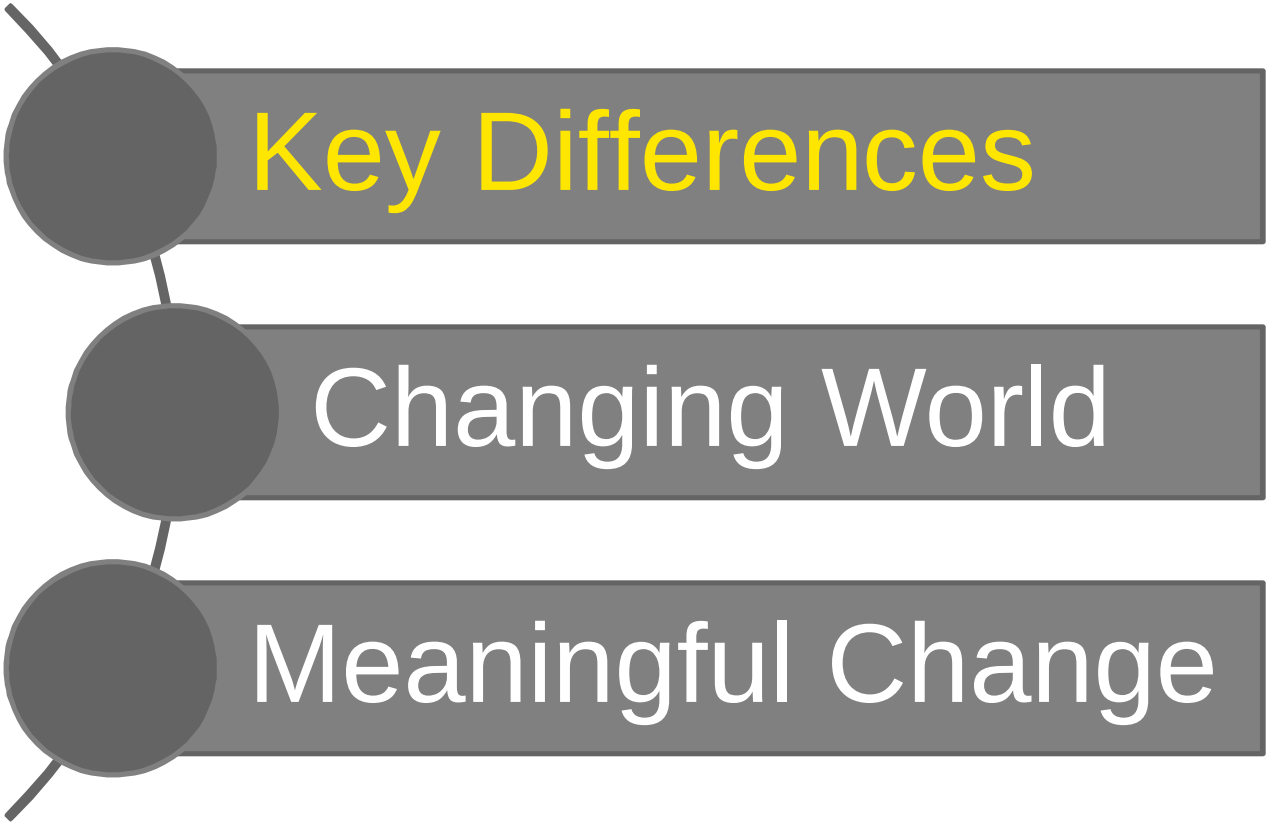
The Main Security Challenges with the Convergence of IT & OT

- In critical infrastructure shared across public and private sector organisations, we have seen an increase in interconnections between operational technology (e.g. SCADA, ICS etc.) and information technology.
  - Previously air-gapped systems which control key processes with potential loss of life consequences when compromised, are now exposed to the organisation's internal networks and sometimes even the public internet. Most of these systems are managed entirely differently than typical IT assets, and by a distinctly different organisation.
  - The two top priorities in OT are up-time and safety, making things such as patching and even monitoring much more complicated than in IT. Currently, as with so many matters related to information security, the operational technology security conundrum is too often dismissed as a technical challenge.
- This presentation will zoom in on the main organisational and often political challenges that will need to be overcome prior to successfully addressing the technical and process changes required for combining IT and OT in a more unified approach to cyber security

Today’s journey



Today's journey



Key Differences IT vs OT

IT

- Security is old hat
- Mature processes
- Have frameworks, policies & standards (ISO, COB CIS,NIST etc)
- Skills where re
- Real-time v ron
- Patche
- Se figured
- g in place

OT

- Bu ult engineers
- on security
- of maturity
- o defined frameworks
- Lack of skills in their environment
- Heads in the sand
- Systems Unpatched
- Insecure Configurations
- Unmonitored

Key Differences IT vs OT

IT

- 8 to 5 desk jockeys
- Don't "get" operations
- No responsibility for human life & environment
- Happy to work in undefined states
- Undue faith
- Reboot with apology
- Daily or weekly change window

OT

- 24 x 7 mission critical ops
- At the coalface, one with the operations
- Understand magnitude of responsibilities
- Work with the defined
- Everything must be proven
- Little scope for mistakes
- One or two changes windows a year (maybe)

- Mature security approach
- Knowledge widely available
- **The information is protected (confidentiality first)**

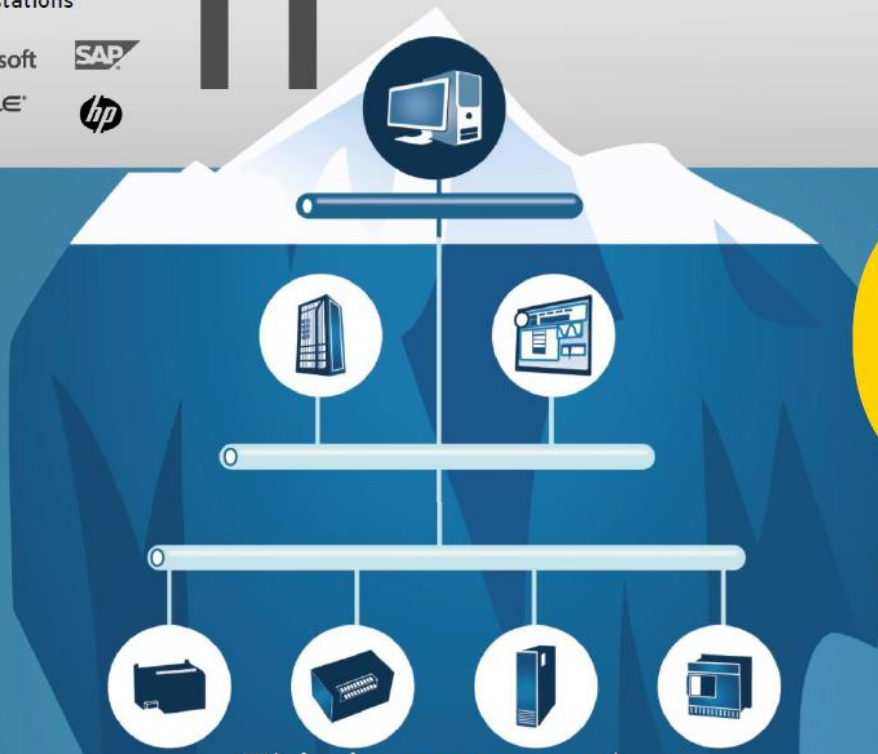
Main components

- Application servers
- Database servers
- Workstations

Vendors

Microsoft SAP ORACLE hp

IT



This is an area where **budget is 10 times bigger** than in IT!

OT

- Newly recognized area of concern
- Specific industrial knowledge
- Different approach to security
- **The process is protected (Availability first)**

Main components

- Control servers
- **PHD** servers
- Data historians
- Alarm system servers
- **HMI** (Human Machine Interface
- Engineering workstations
- **RTU** (Remote Terminal Unit) stations
- **PLC** (Programmable Logic Controllers)

Vendors

ABB Wonderware Schneider Electric Rockwell Automation SIEMENS Honeywell YOKOGAWA ALLEN-BRADLEY

The **process control** systems operate between the business systems requirements for real time access to data about production processes forced Control Systems to interconnect with business networks and other external systems, which generated **major security issues.**

Global OT Advisory Services Center

Key differences IT vs OT : NIST 800-82 r2 (modified hazar.org)

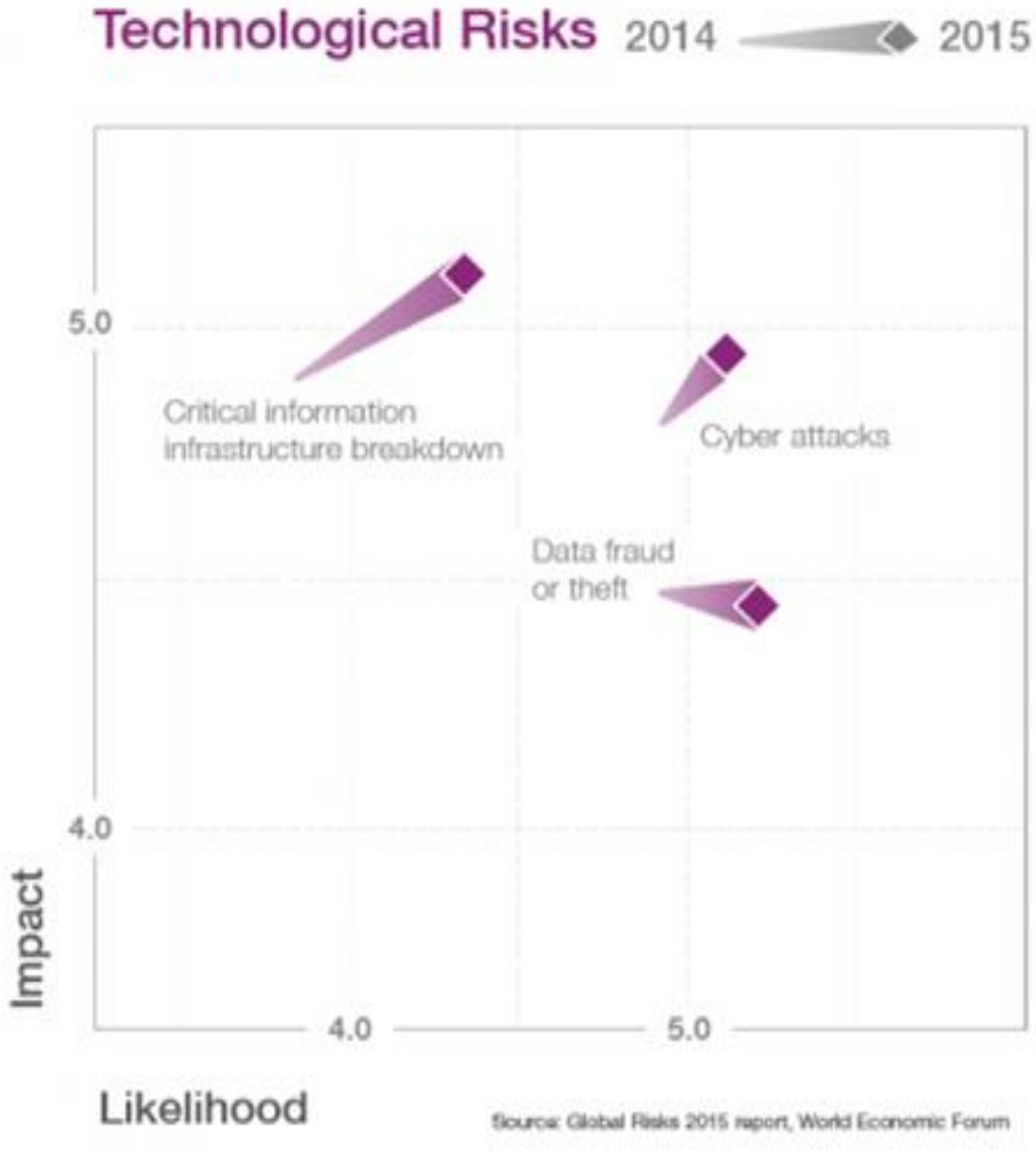
Category	IT Systems	OT Systems
Primary Players	▸ CIO ▸ Computer Science Grads ▸ “WinTel Geeks” ▸ Younger generation	▸ Engineers ▸ Technicians ▸ Production managers and staff ▸ Older staff who moved “up through the ranks” from line operator to technician
Primary Focus	▸ Data confidentiality and integrity is paramount ▸ Automating business processes ▸ Information management and manipulation	▸ Safety and protection of the process ▸ Response to human and other emergency interaction is critical ▸ Controlling physical processes
Component Lifespan	▸ Lifetime on order of 3-5 years	▸ Lifetime on order of 15-20 years
Security Approach	▸ **Confidentiality**, Integrity, Availability	▸ **Availability**, Confidentiality, Integrity
Performance Requirements	▸ Non-real-time ▸ High throughput demanded ▸ High delay and jitter may be acceptable	▸ Real-time ▸ Response is time-critical ▸ High delay and/or jitter is not acceptable

Key differences IT vs OT : NIST 800-82 r2 (modified hazar.org)

Category	IT Systems	OT Systems
Data	▸ Complex data types ▸ Multi-layered analytics ▸ Low data rate (10K msgs / sec)	▸ Simple data type ▸ Just-in-time analytics ▸ High data rate (1M msgs / sec)
Interfaces and Networks	▸ Web Browser ▸ Keyboard ▸ TCP/IP based ▸ Typical IT networking practices	▸ Human-Machine Interface (HMI) ▸ Sensors ▸ Coded Displays and Touch screens ▸ Serial-based moving to TCP/IP)
Change Control	▸ ITIL processes are appropriate ▸ Software changes applied in timely manner ▸ Patching procedures often automated	▸ OT outages must be planned and scheduled days / weeks / months in advance ▸ Patching reboots difficult to schedule and negatively impact productivity
Managed Support	▸ Allow for diversified support styles and vendors	▸ Service support usually via one vendor
Component Location	▸ Usually local ▸ Easy to access ▸ In controlled temperature environment	▸ Components can be isolated, remote ▸ Require extensive physical effort to gain access ▸ In high/low temperature, high-humidity environments

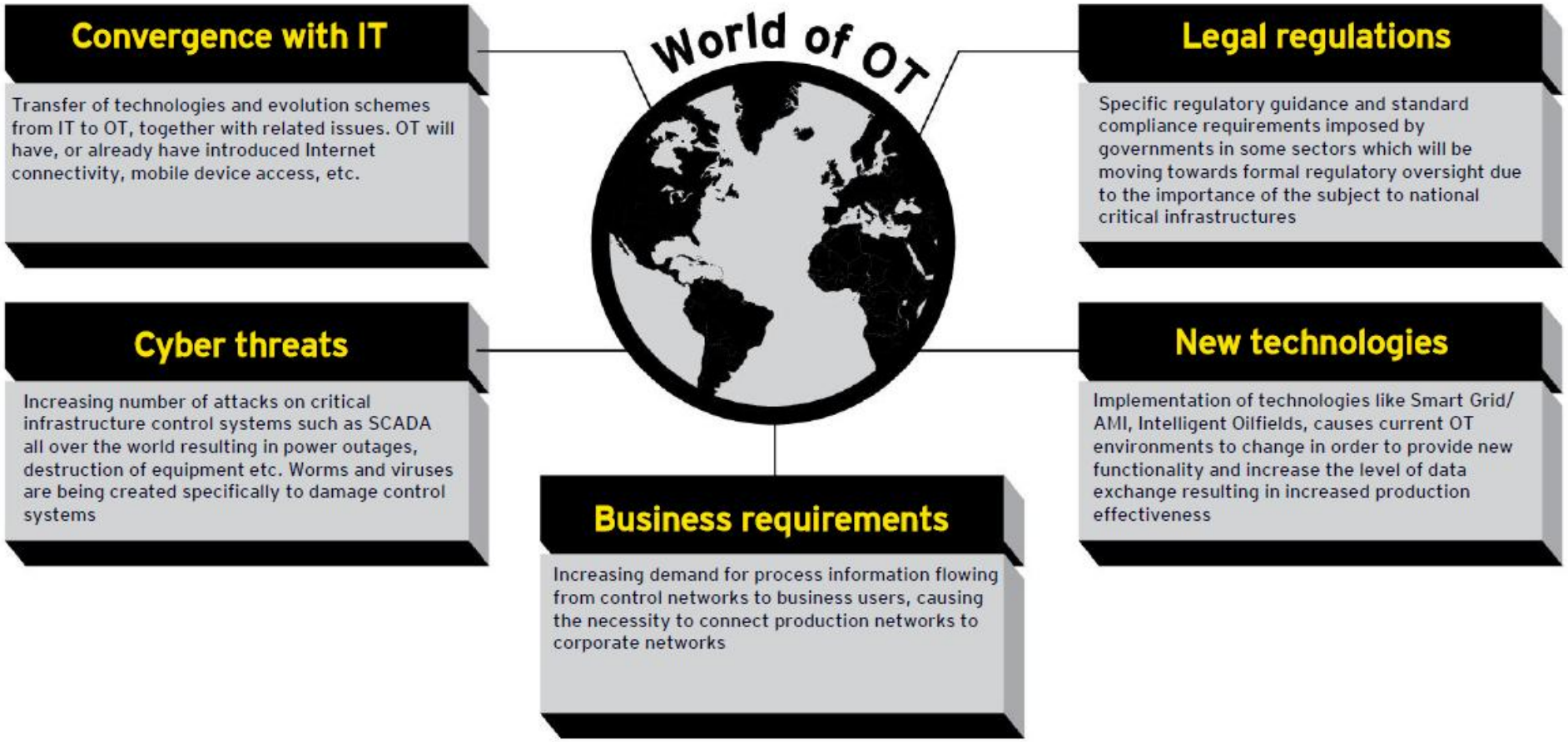
Today's journey

WEF Global Risk 2015 :
Changing Global Risk Landscape



Increasing Pressure : The Boards are asking questions

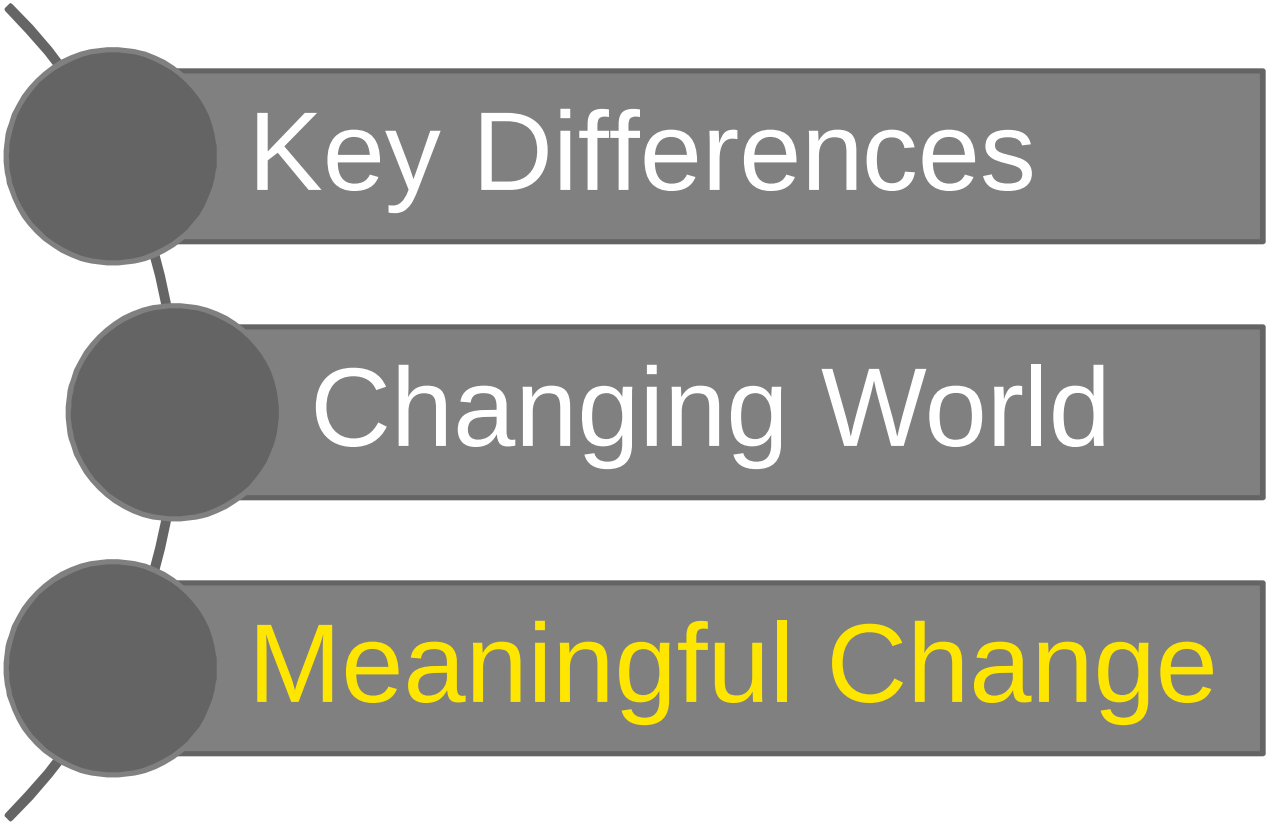
- Global Risk Assessments (WEF)
- King 3 (and talk of King 4)



Why Converge

- Because we can connect
  - OT move to IP
- Large distances : Shared WAN
  - Remote locations
  - Drive for cost savings
- Big Data / Reporting
  - Access to information generated in the OT environment
- Remote vendor support
  - Scarce skills
  - Access to out of country skills
- Updates
  - AV Servers, Patch Servers, other updates

Today's journey



Our Selected Global Case studies

How are our sites globally (incl. JV) managing their OT security?

Are our sites compliant with our security standard and legal regulations?

How to secure an obsolete system before it is replaced by new one?

How can we secure a countrywide network, connecting multiple different types of sites?

PROBLEM STATEMENT

Are we confident that we control the level of risk related to production environment?

- Security assessment
- Improvement plan
- Security baseline
- Complience assurance
- Security system & controls
- Security governance
- Security procedures
- Trained personnel
- Reporting

Fallacy

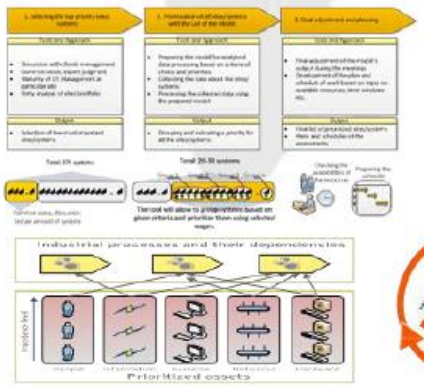
- OT is air-gapped from IT world
- OT is protected by engineers
- Vendors are ensuring safety of OT systems

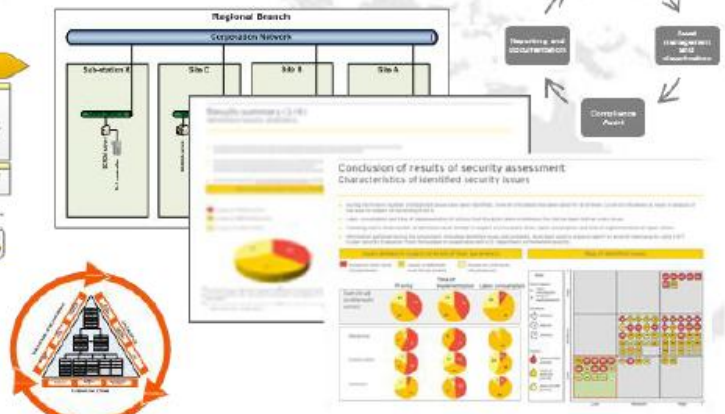
Legacy of

technologies in OT, require dedicated approach to security challenges

Lack of

OT incident response readiness





Our Selected Global Case studies

O&G enterprise covering the whole value chain, from upstream to downstream and heat & energy production

Operations in Europe, Africa & Asia

PROBLEM STATEMENT

How should we transform OT area to ensure support for development of Capital Group and boost cost effectiveness of business operations?

IT/OT Vision → IT/OT Maturity Assessment → Target IT/OT Model → Implementation plan → Implementation Support

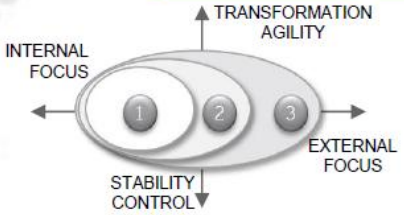
25 entities
divided into groups with different goals & scope of transformation

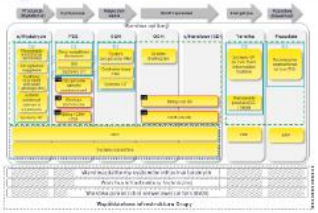
IT/OT alignment

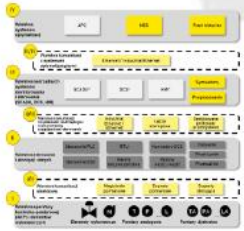
target model covering organization & technology streams and 7 strategic areas for IT and OT environment:

- VSM-based systems approach
- coherent IT & OT management
- IT & OT architecture and standards

5 strategic programs
covering organization, architecture & critical infrastructure protection







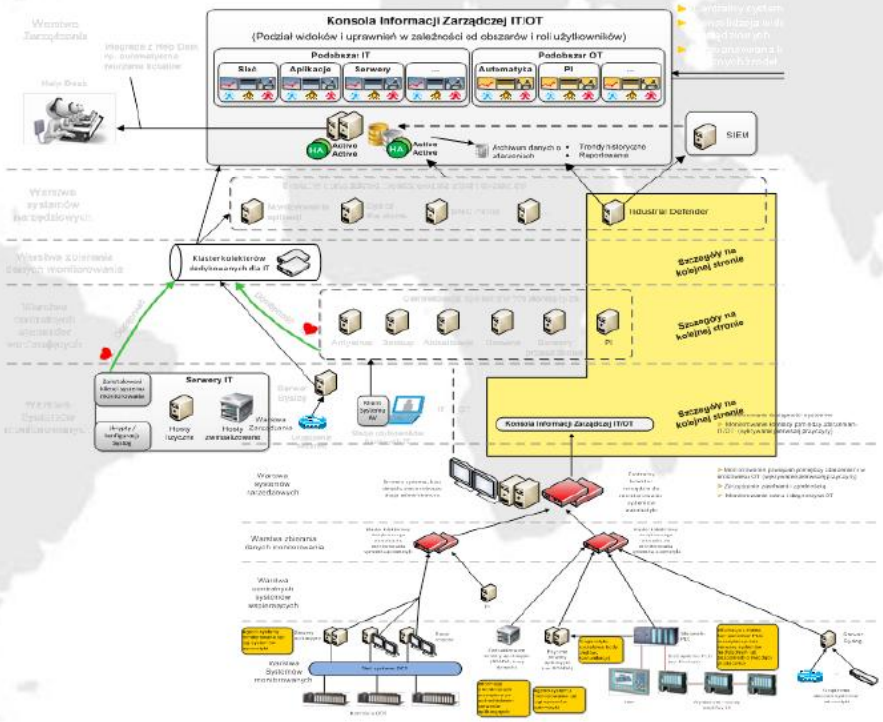
Our Selected Global Case studies

Fortune 500
Oil & Gas company
in Europe

Most advanced and one of the largest PTA production plant in Europe

PROBLEM STATEMENT

What to monitor and to how process BIG DATA from the production devices/sensors in order to deliver decision support solutions?



Data integration and processing optimization architecture

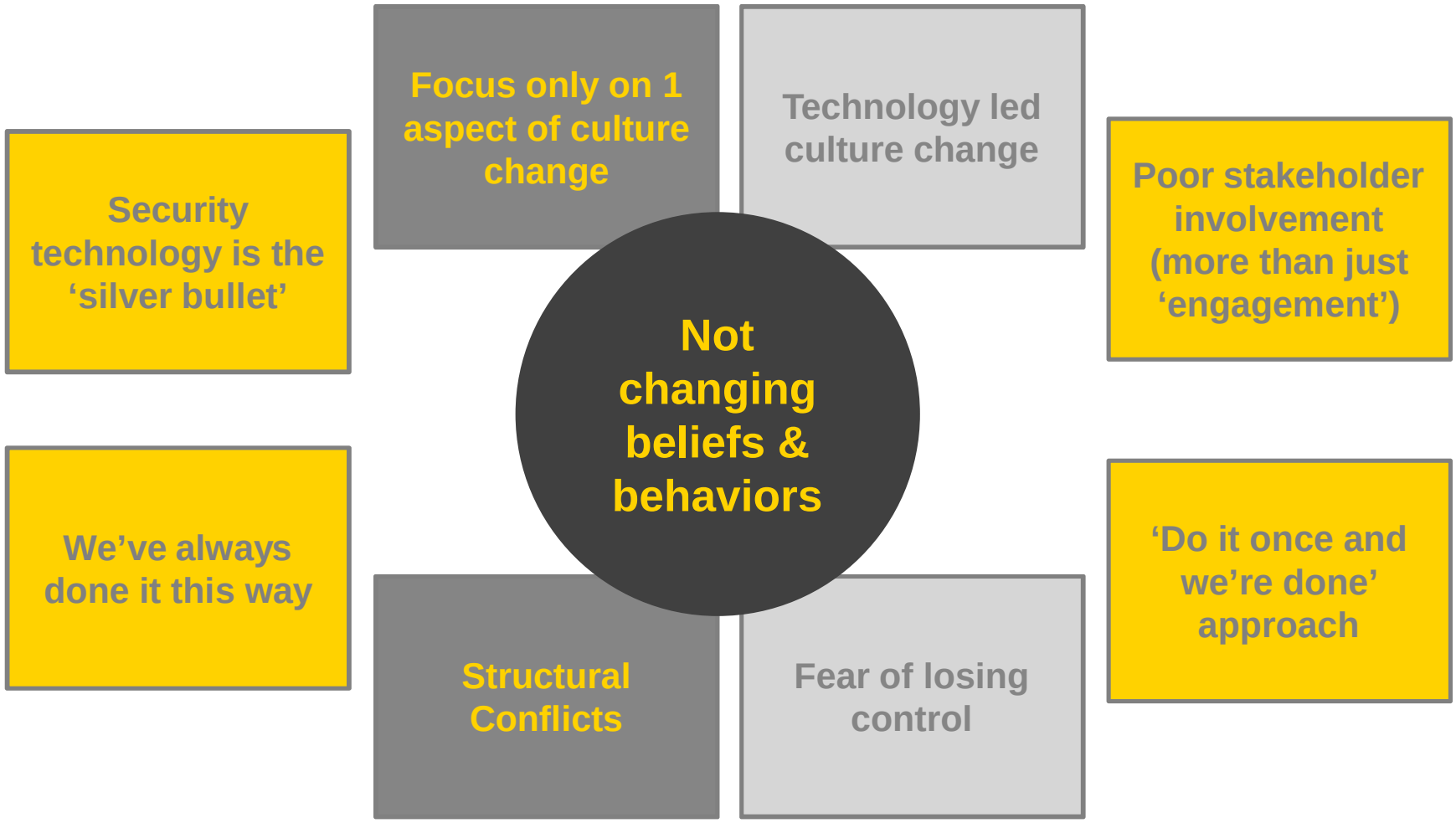
joining data sources, such as:

- PLC's
- DCS Controllers
- SCADA servers
- operators workstations
- network equipment
- custom solutions

to support critical business decisions as well as allow for advanced **preventive maintenance**

EY

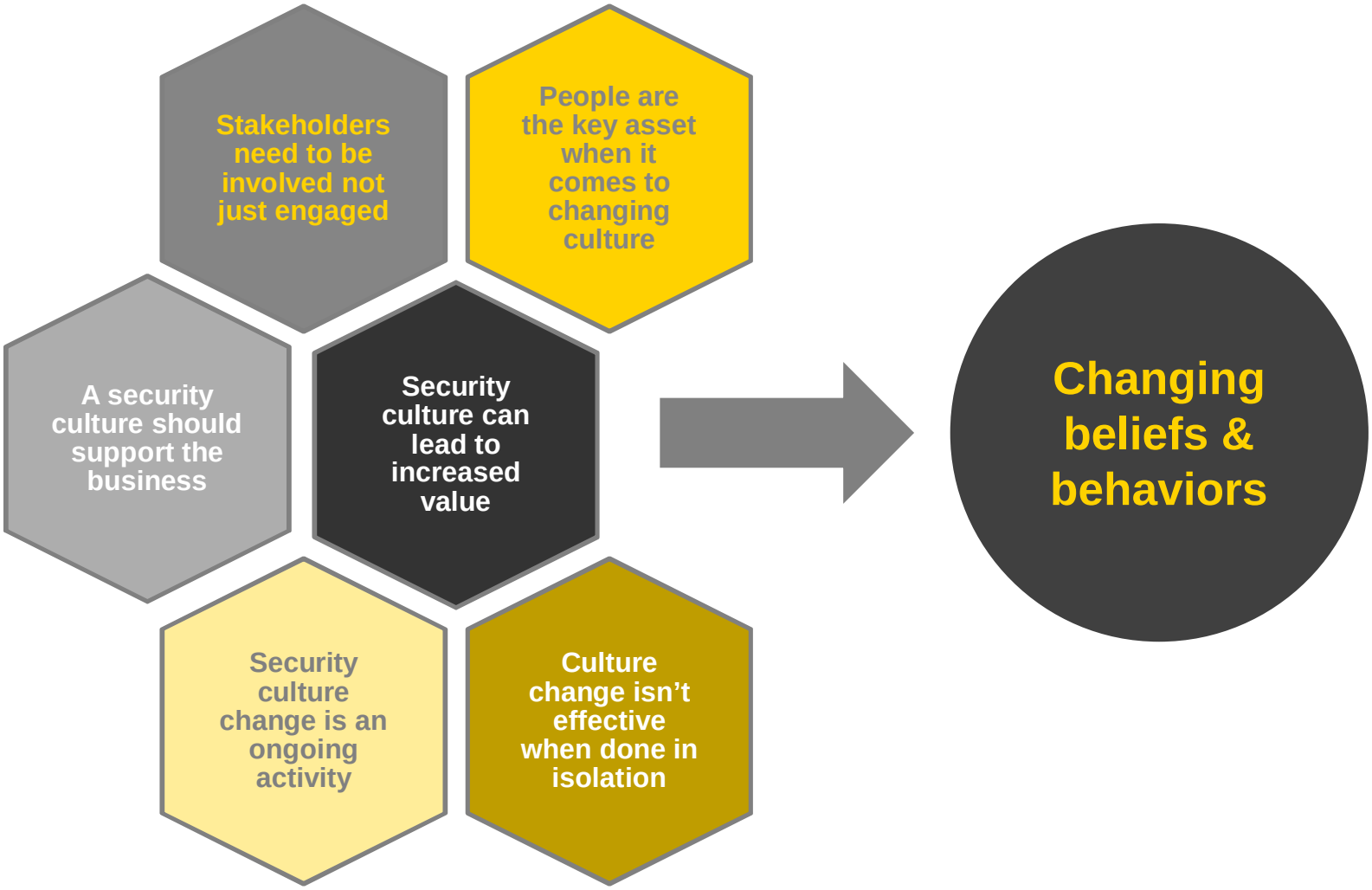
Why haven't organisations been successful in merging their IT/OT security culture to date?



(ISC)^2 : Main Security Challenges with convergence of IT & OT

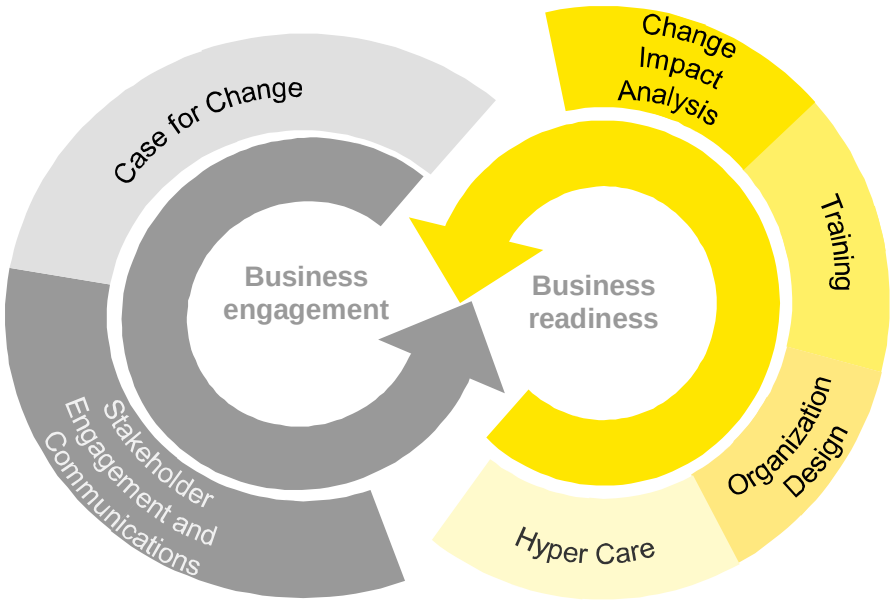
EY

Developing a strong business orientated security culture is key to tackling the cyber threat



(ISC)^2 : Main Security Challenges with convergence of IT & OT

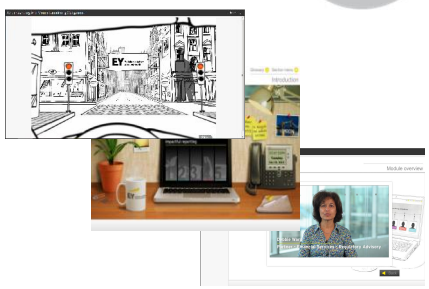
Business engagement and readiness: Two halves of the whole that is Business Change

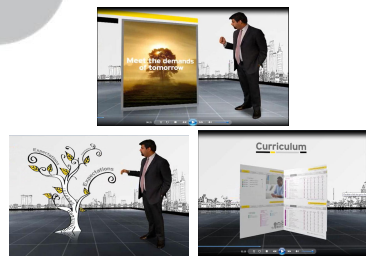


Getting the business engaged and ready for upcoming changes is one of the biggest obstacle you might face. True change management actually consists of two parts: Engaging people, and then getting them ready. Doing this will create a sustainable change.

- Think of **business engagement** as an election campaign you have to win. You need to overcome significant opposition and obstacles with the right candidate/leadership/campaign communication.
- Equally important is getting the **business ready** for the change by aligning people, systems and processes to the new way of working, new behaviors, etc.

There is no ‘one size fits all approach’ for delivering effective culture change





Working Together

- Accept there are no quick fixes
- Work to strengths of each function
- Clear delineation of responsibilities
- Combined Roadmap to success
- Cultural Change / Alignment
  - Engage in new ways of working
  - Marriage not a buyout
  - Taking time to understand key challenges of each discipline

Questions

- Justin Williams: Executive Director, Cybersecurity
  - 083 279 0998 / 082 772 9881
  - Justin.williams@za.ey.com

Thank you

EY

Building a better working world