CYBER SECURITY DIVISION

LEONARDO

Adapting to the *'New Normal'*

Managing cyber risks to the Utilities Sector beyond COVID-19

11 June 2020

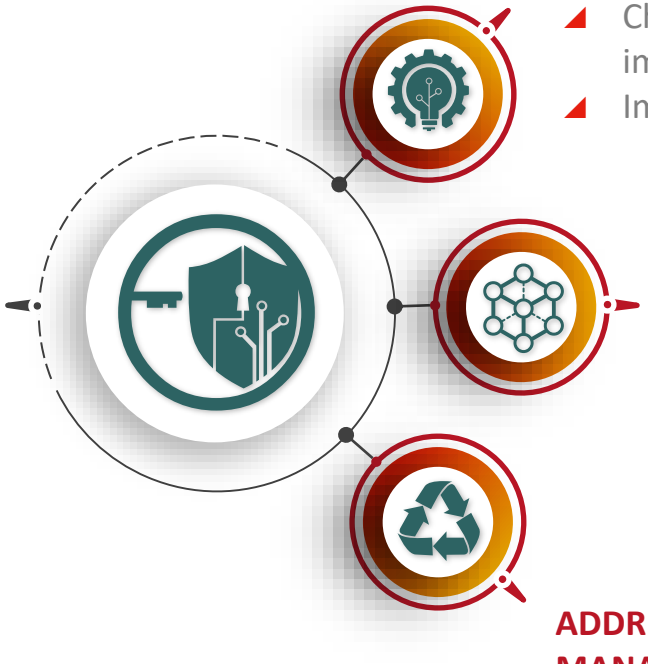
Introduction

- Dr Max Wigley
- NCSC Accredited Head Consultant and Consultancy Service Owner
- Working with customers to understand the holistic and Enterprise level Cyber Risk associated with operating complex capabilities
- Developing architectures and approaches to cyber security and business transformation that enable operation within a stated risk appetite

Dr Max Wigley
Head of Consulting
Cyber Security Division
Leonardo UK

Assured Service Provider
in association with
National Cyber Security Centre

Summary



INTRODUCTION

- Challenges facing the utilities sector: immediately and in the future
- Impact of COVID-19

SECURITY CULTURE AND HUMAN BEHAVIOUR

- What changes do we see due to COVID-19
- Optimising security attitudes and behaviours in the utilities sector

ADDRESSING THESE CHALLENGES TO SUPPORT A RISK MANAGED APPROACH FOR UTILITIES ORGANISATIONS

- Use of a robust Risk Management Framework
- Approaches to delivering Security Architecture

Leonardo Overview

Leonardo is a global high-tech company and one of the key players in Aerospace, Defence and Security worldwide

UK Divisions

Helicopters

Electronics

Cyber Security

Subsidiaries/Joint Ventures

Leonardo DRS
100% Leonardo

Telespazio
67% Leonardo
33% Thales

Thales Alenia Space
67% Thales
33% Leonardo

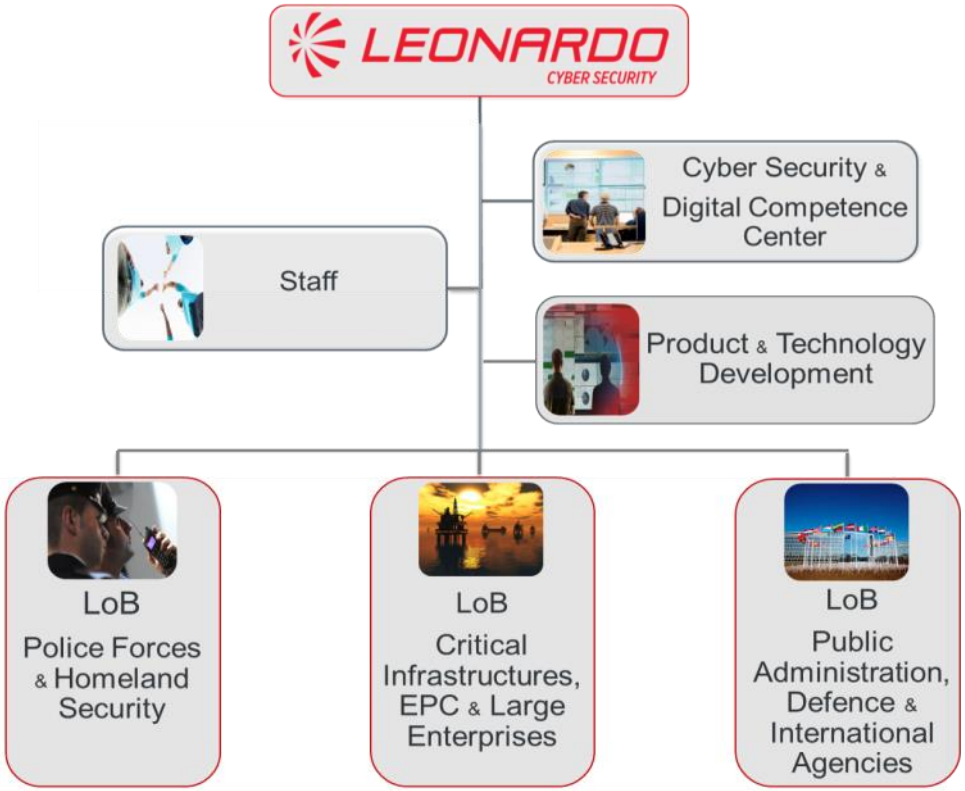
MBDA
37.5% BAE Systems
37.5% Airbus Group
25% Leonardo

ATR
50% Leonardo
50% Airbus Group

2018 Results (€bn)

12.4	Revenue
36.1	Order backlog
15.3	New orders

Leonardo Cyber Security Division



Assured Service Provider

in association with National Cyber Security Centre

Spotlight on the Current Challenge

Challenge

- Net zero, sector crowding, economic volatility, regulatory oversight

Response

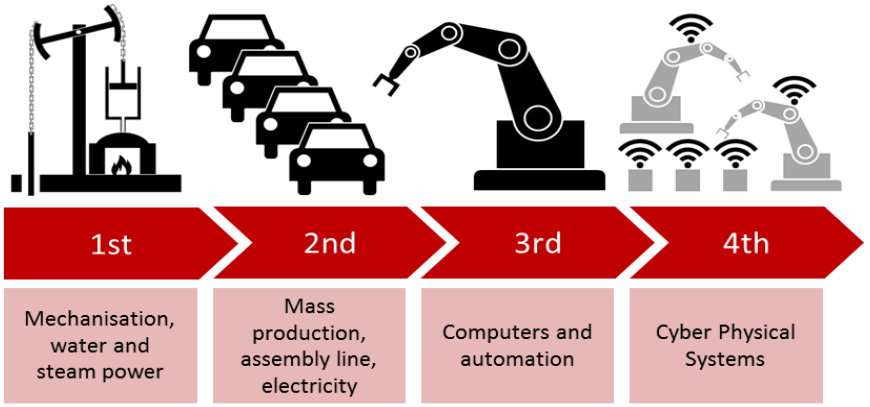
- Convergence of previously segregated operational networks and corporate IT

Enabling

- Efficiency through remote management and administration
- Ability to provide holistic performance metrics

Leading to

- Increase in organisational attack surface
- Cascading and aggregated security risk
- Significant reputational and service delivery risks

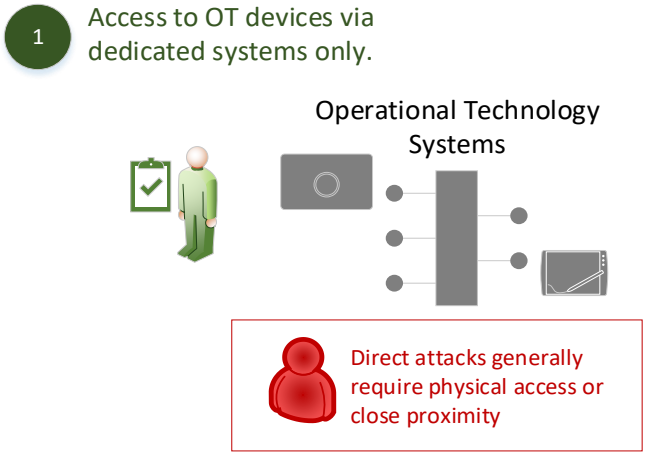


Christoph Roser at AllAboutLean.com

‘Traditional’ Operational Technology Setup

Air-gapped and Analogue deployments protected from physical attack.

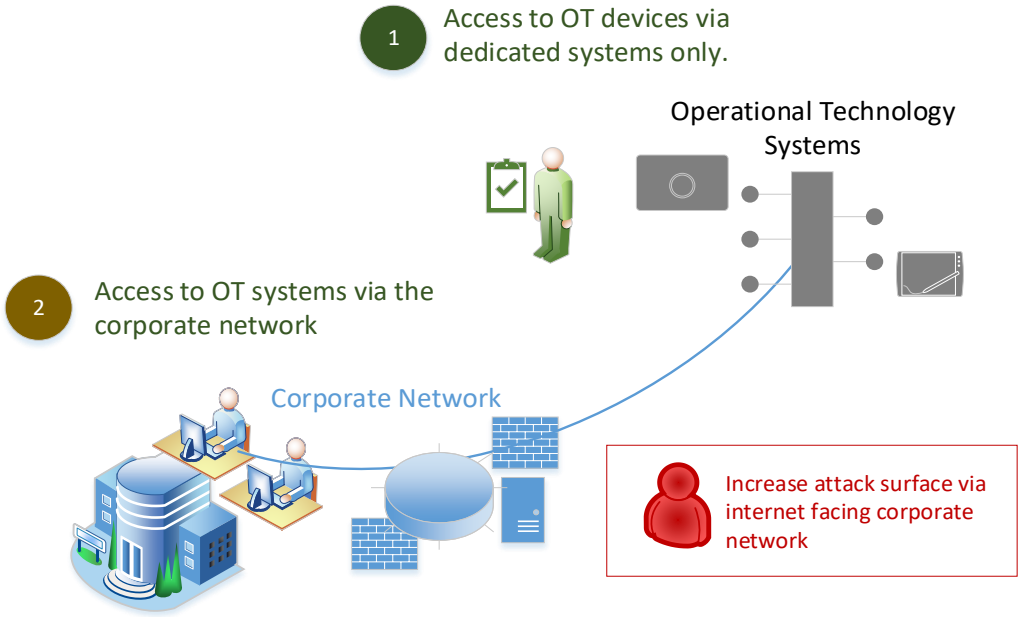
- Operational Technology estate deployments typically relied on physical air gaps and manual controls to mitigate security risks
- Threats largely centred around local or direct physical access to the environment
- Security controls designed, tested and deployed in order to counteract this physical threat



A Transition has been ongoing to support improved outcomes

Connected and Digital deployments converged with internal corporate IP networks

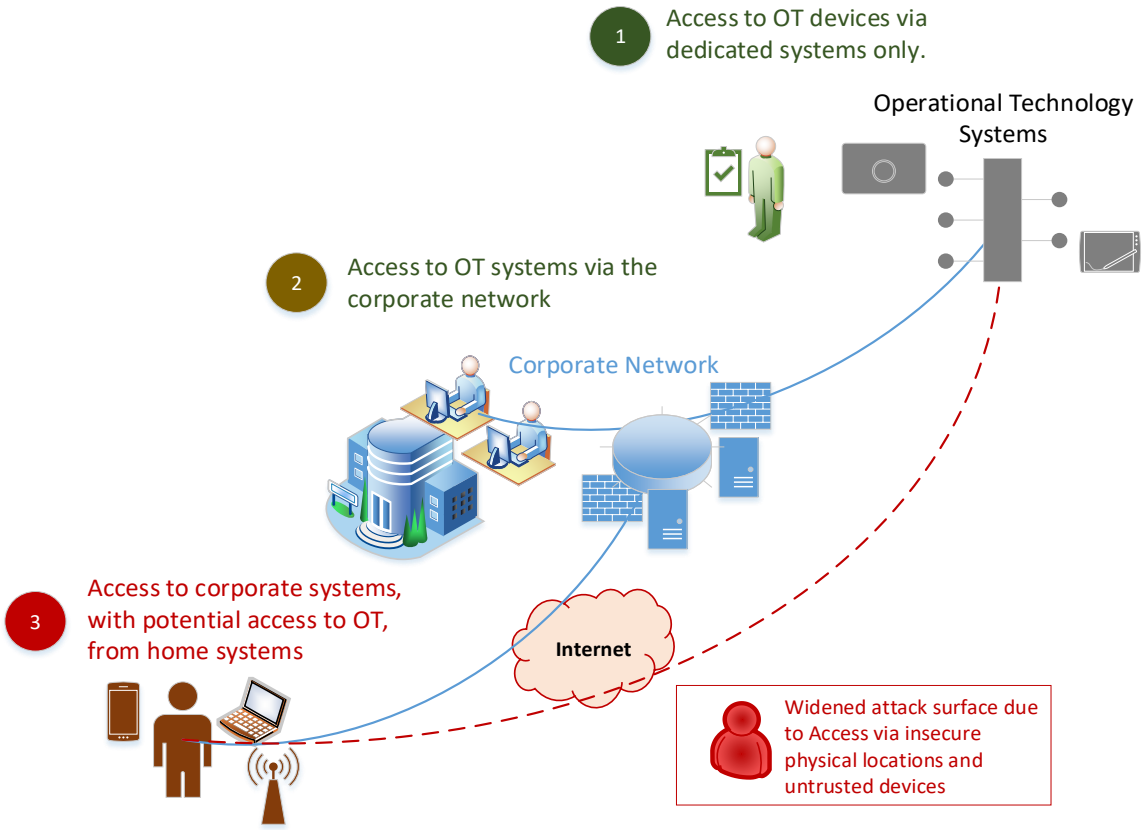
- In recent years, these systems have converged with enterprise IT estates, to enable improved efficiency, increased performance and centralised reporting
- This increases threat landscape and attack surface of the operational estate
- Risk management framework and security architecture is now mal-aligned with the technology architecture



Impact of COVID-19

Unforeseen and sudden disruption to both technical and cultural aspects

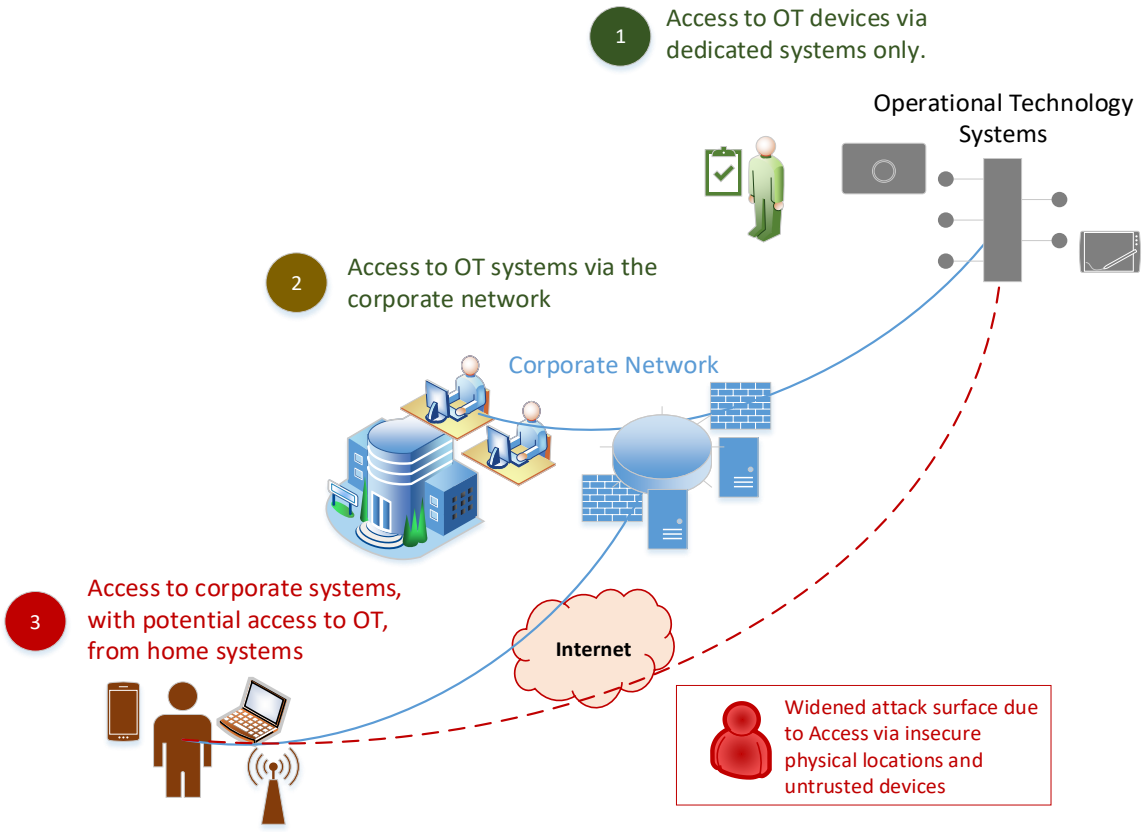
- Further changes have been implemented to support continued delivery of critical functionality
- The most obvious changes are technical in nature, e.g.
  - ❑ Implementing VPN solutions
  - ❑ Bring Your Own Device solutions



Impact of COVID-19

Unforeseen and sudden disruption to both technical and cultural aspects

- Less tangible are the behavioural changes – a broader shift in the culture and expectations
- As these changes persist, creating a '**new normal**', these changes will become embedded leading to a digital transformation of the workplace

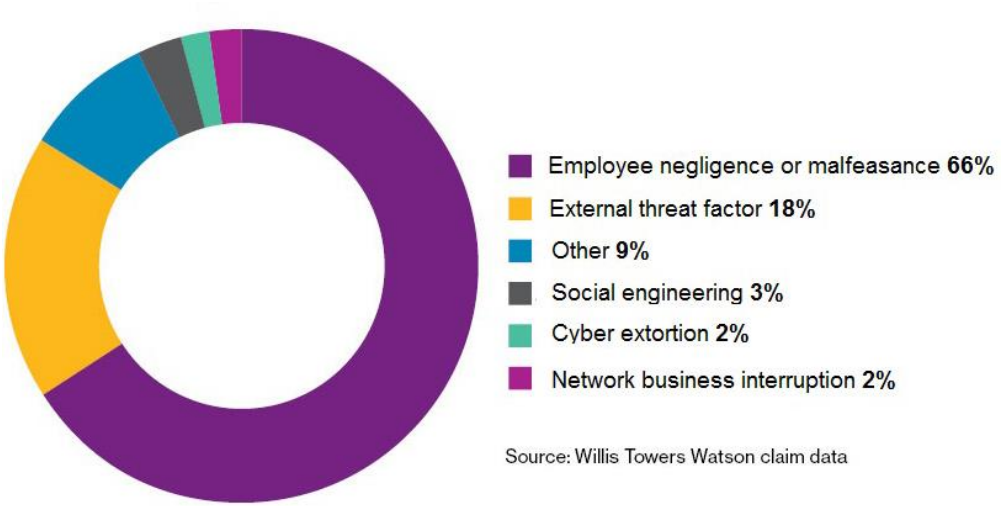


Impact of COVID-19

- In the majority of shifts in approach, the change in culture lags behind the change in technology
- In the case of changes driven by COVID-19, this pattern is reversed and technical changes are being implemented to catch up with new ways of working
- This reversal means that the ability to carefully design processes to integrate with technical solutions is significantly reduced

Understanding the Impact of Human Behaviour

Human behaviour has a major impact on avoidable cyber incidents.
We need a way to understand the root cause so that we can deliver improvements

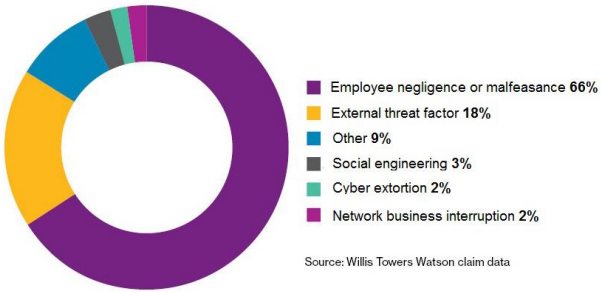


Source: Willis Towers Watson claim data

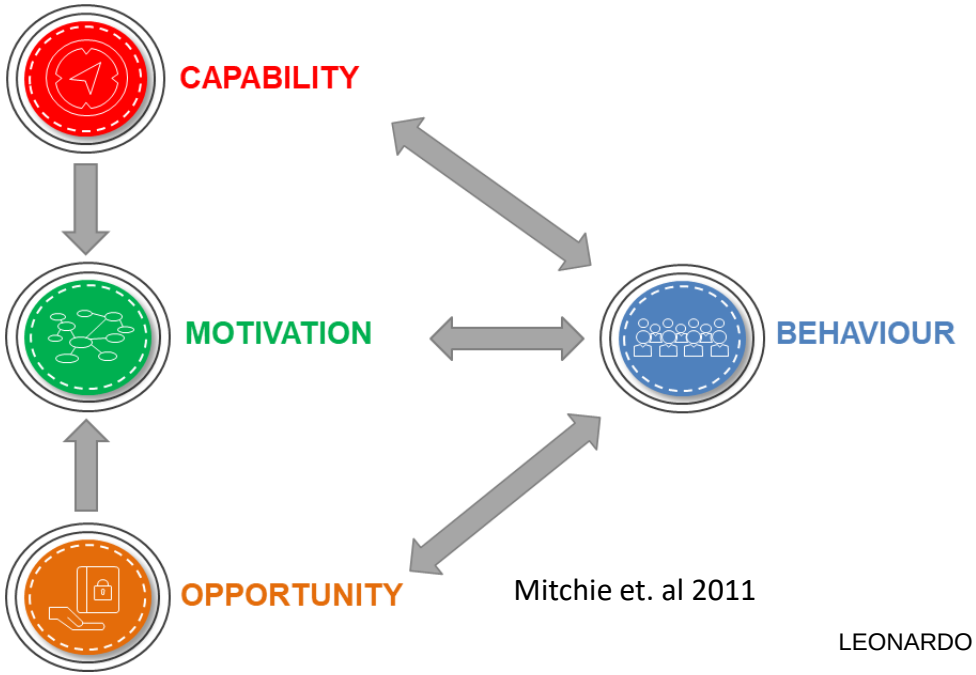
- The number varies, but there is broad consensus that human behaviours or actions are a significant cause or contributing factor to cyber incidents
- This is not necessarily malicious behaviour, it could be inadvertent, via not following a process, or following an incorrect process

Understanding the Impact of Human Behaviour

Human behaviour has a major impact on avoidable cyber incidents.
We need a way to understand the root cause so that we can deliver improvements

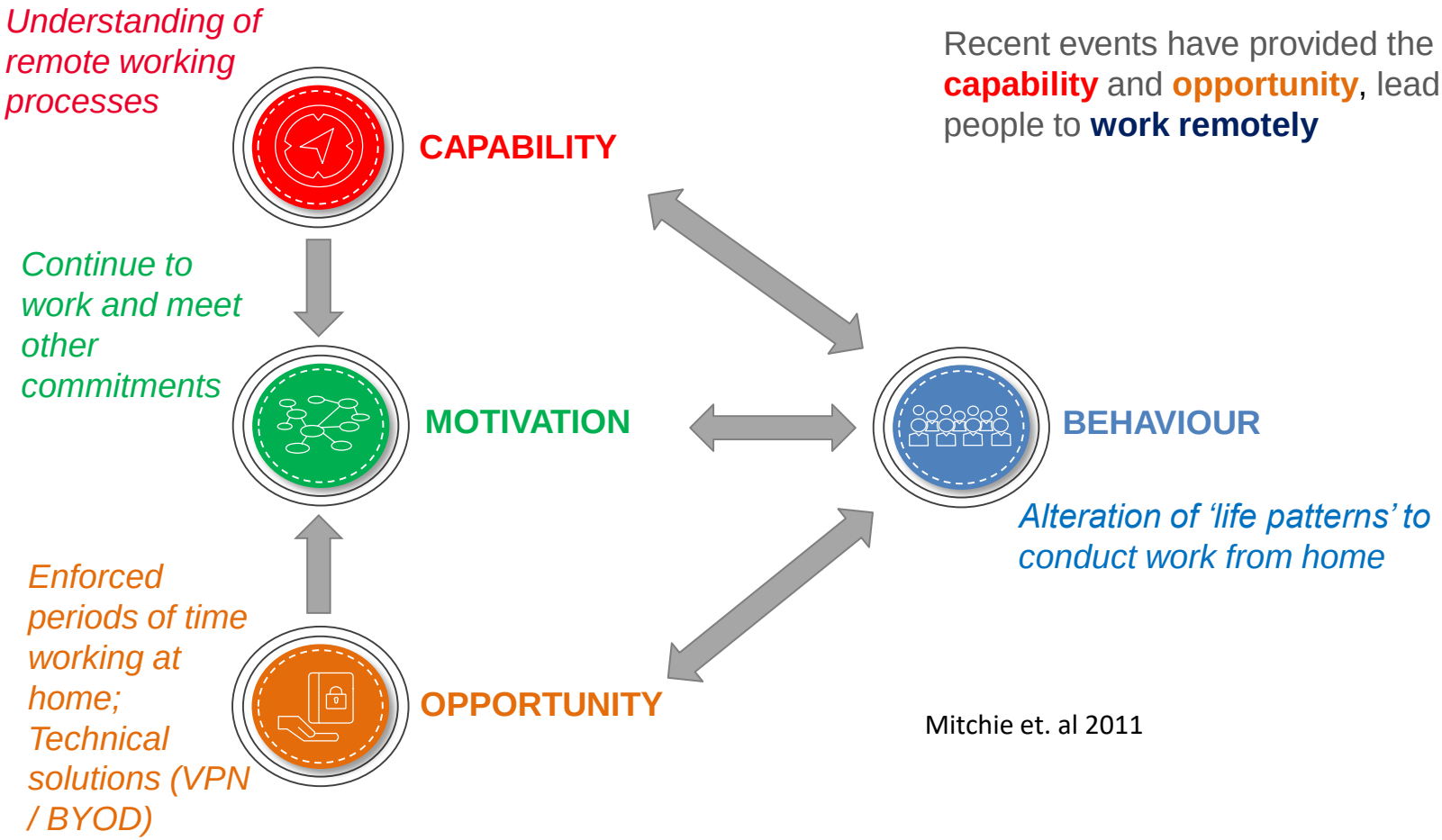


- The COM-B model provides a way to understand the root cause of behaviours, enabling targeted actions to deliver positive change
- Simply delivering more online training is unlikely to achieve the desired effect



Mitchie et. al 2011

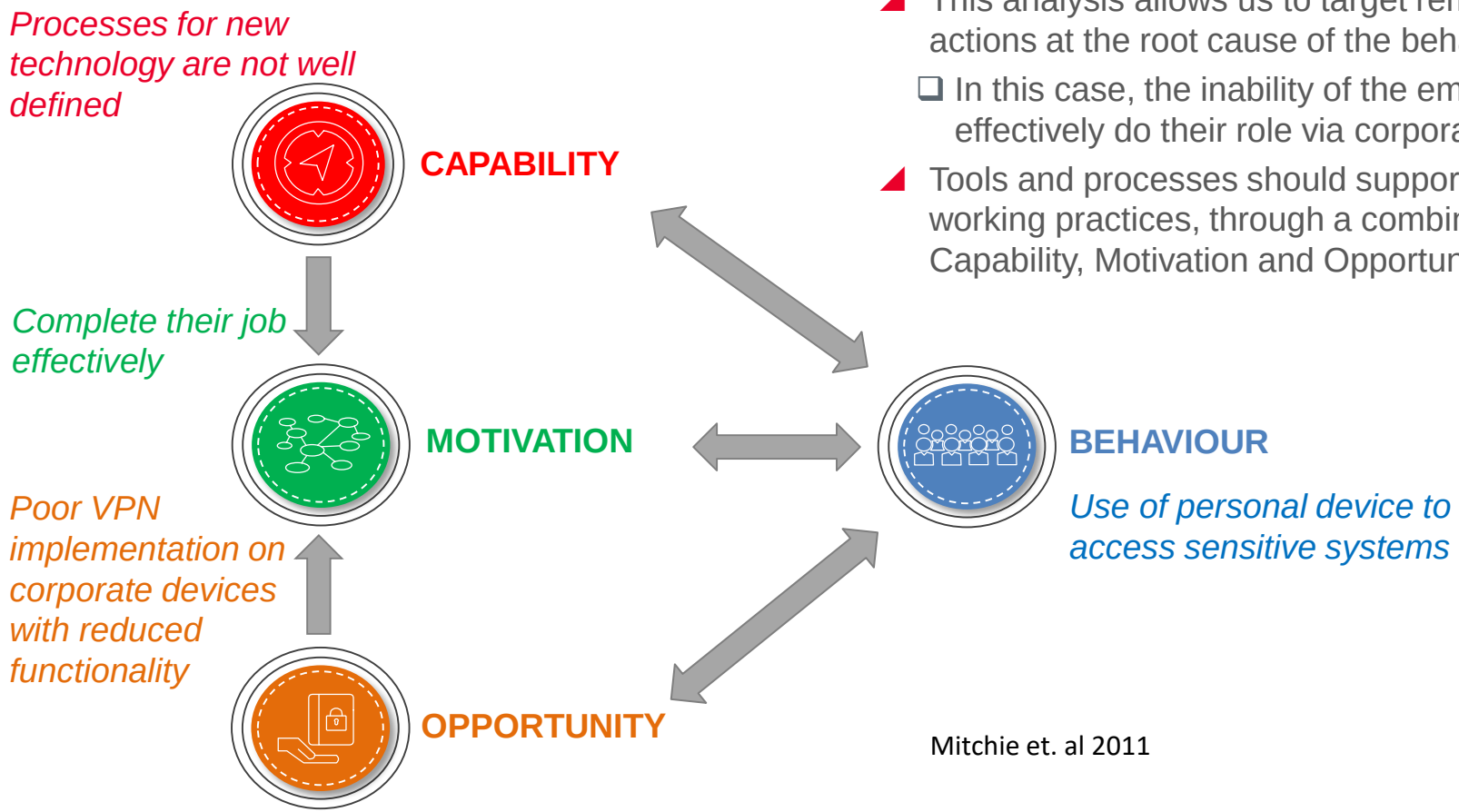
How does this apply to the COVID scenario?



Recent events have provided the **capability** and **opportunity**, leading people to **work remotely**

Mitchie et. al 2011

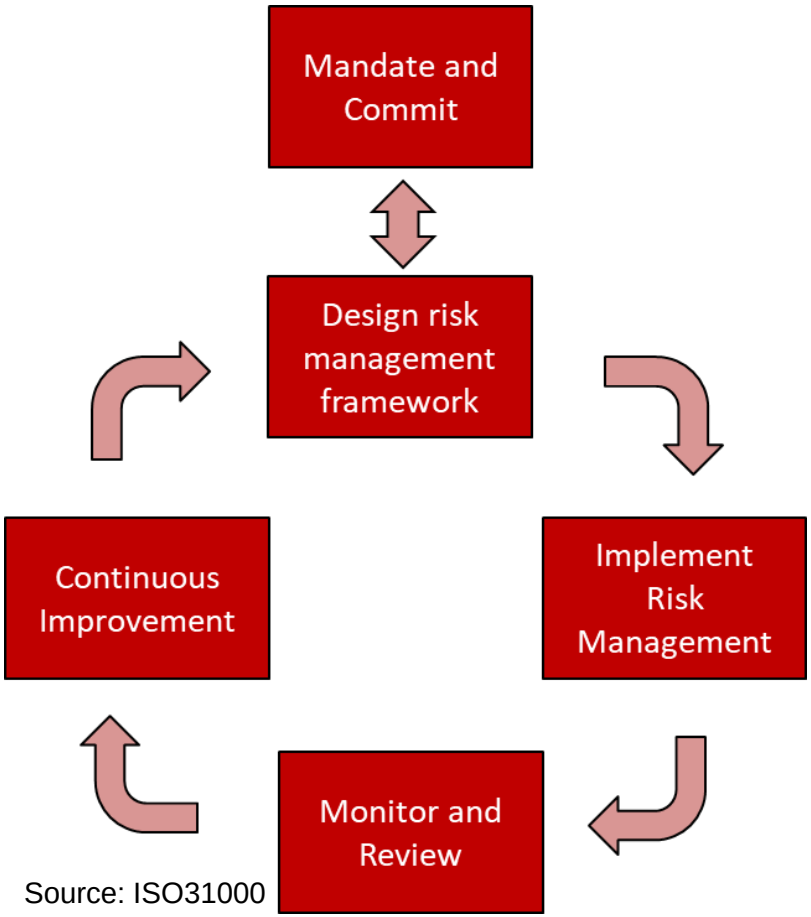
This can also be used to analyse security concerns



- This analysis allows us to target remedial actions at the root cause of the behaviour
  - In this case, the inability of the employee to effectively do their role via corporate systems
- Tools and processes should support secure working practices, through a combination of Capability, Motivation and Opportunity

Mitchie et. al 2011

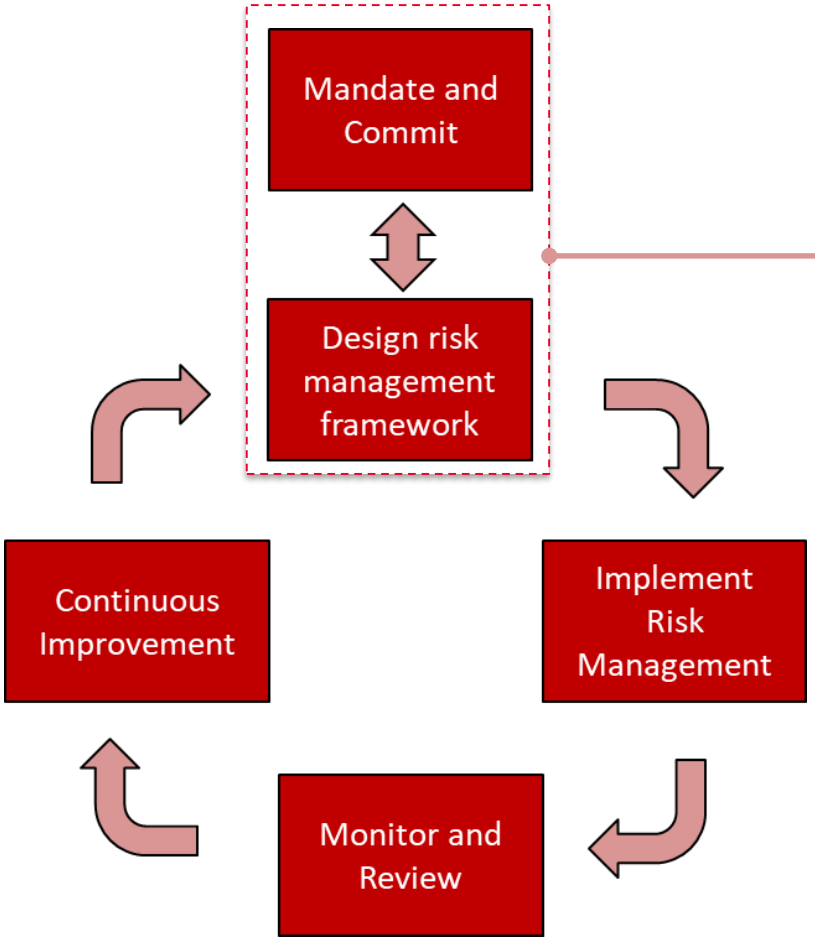
Applying a systematic, risk management framework to address these challenges



Source: ISO31000

- Ultimately, any approach needs to ensure that the Security objectives are aligned to and support those of the business
- Achieving these objectives means balancing security activities against the costs versus benefit to the business
- Such an approach requires a consistent a defined approach to managing risk throughout its lifecycle
- This enables any control, technical, physical or administrative to have clear business justification enabling wider support and adoption of security

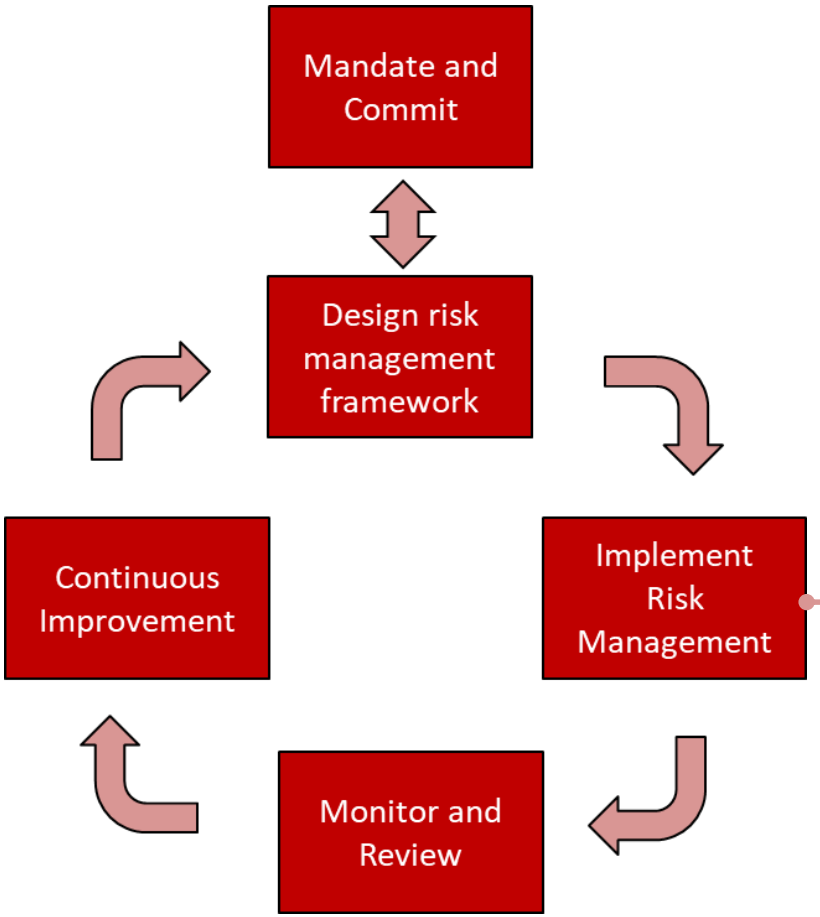
A defined and endorsed Security Strategy is a critical starting point



Develop a security strategy and Risk Management framework that aligns security activities with business outcomes.

This will ensure that security can be an enabler to business outcomes and that senior management are supportive of security activities and the approach to security.

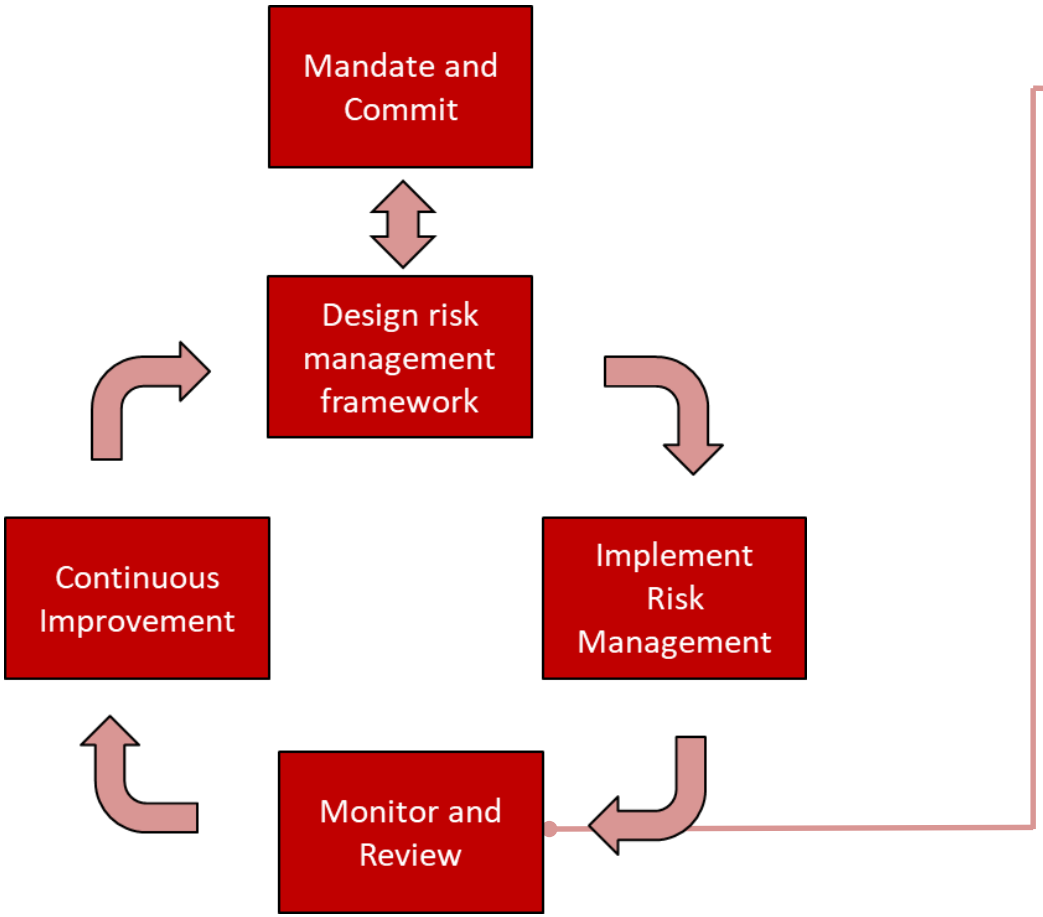
Risk Management needs to be integrated into business processes



Implement security risk management and assurance activities into business processes across their operational lifecycle.

This means integrating security into all business areas, change release, change control, configuration management are all examples of areas that require security context to be added.

Risk is not static and requires continual review

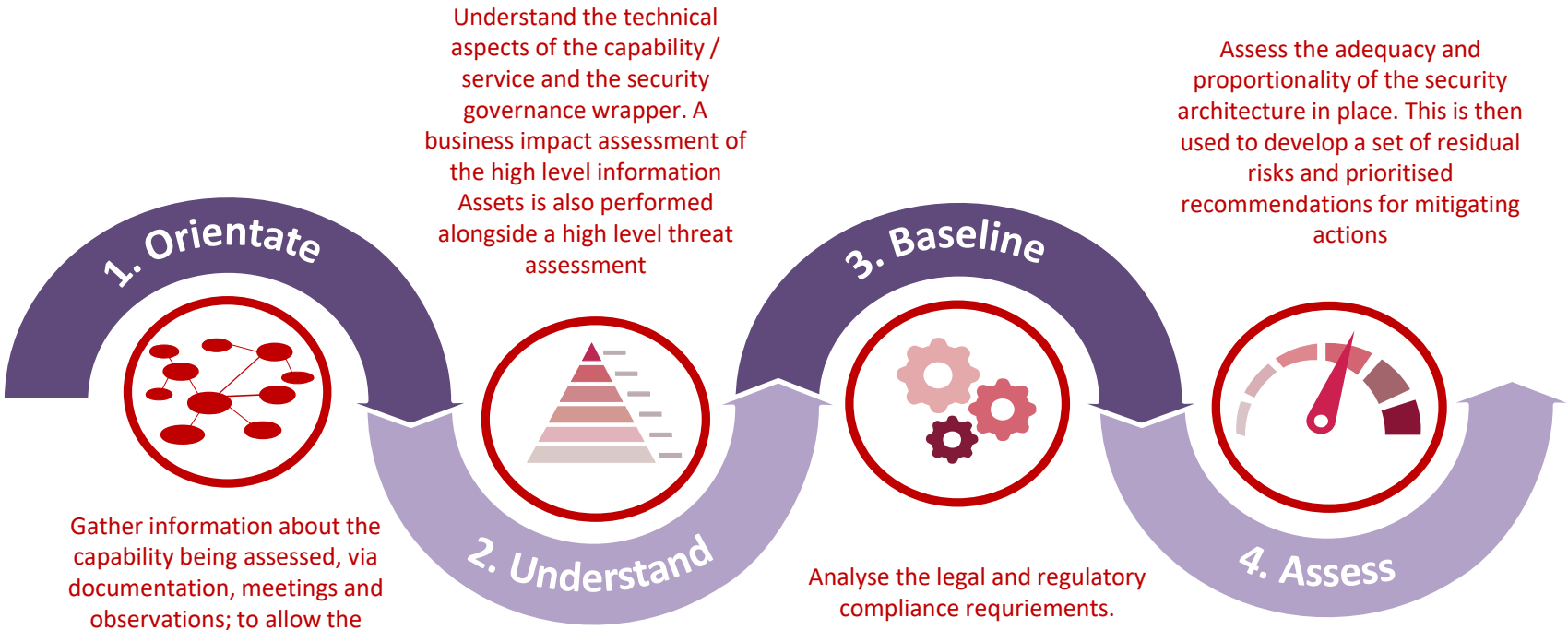


Utilising tools such as Key risk indicators, monitor changes in risk continually to understand when risk mitigation plans need to change or business impact assessments require updating.

Security steering can be formed that feature business process owners to monitor process compliance and discuss exception cases.

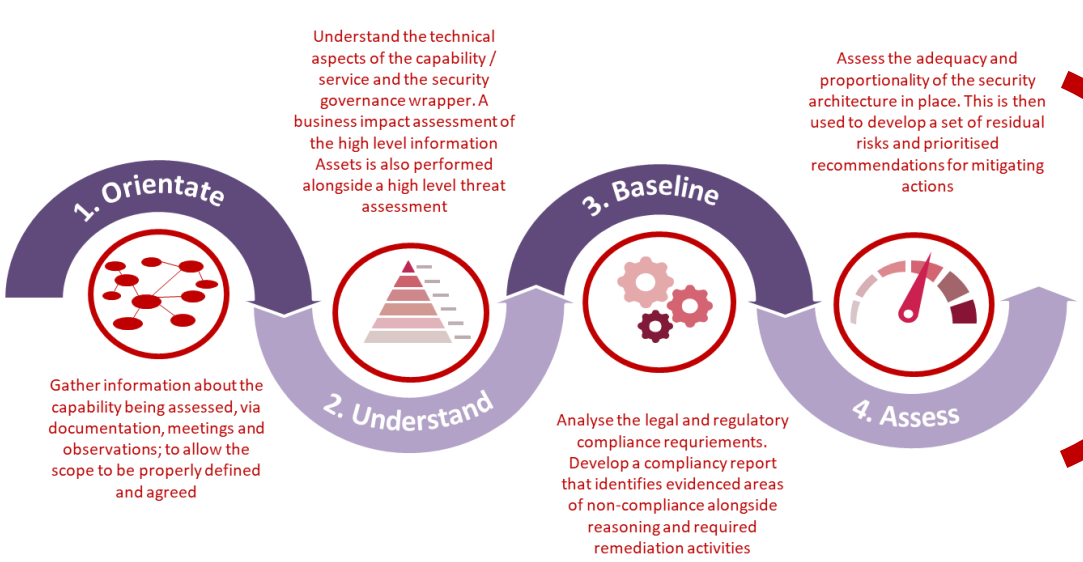
Service Risk Assessment

A robust risk assessment process will support assessment of the impact of changes



Service Risk Assessment - Benefits

A robust risk assessment process will support assessment of the impact of changes

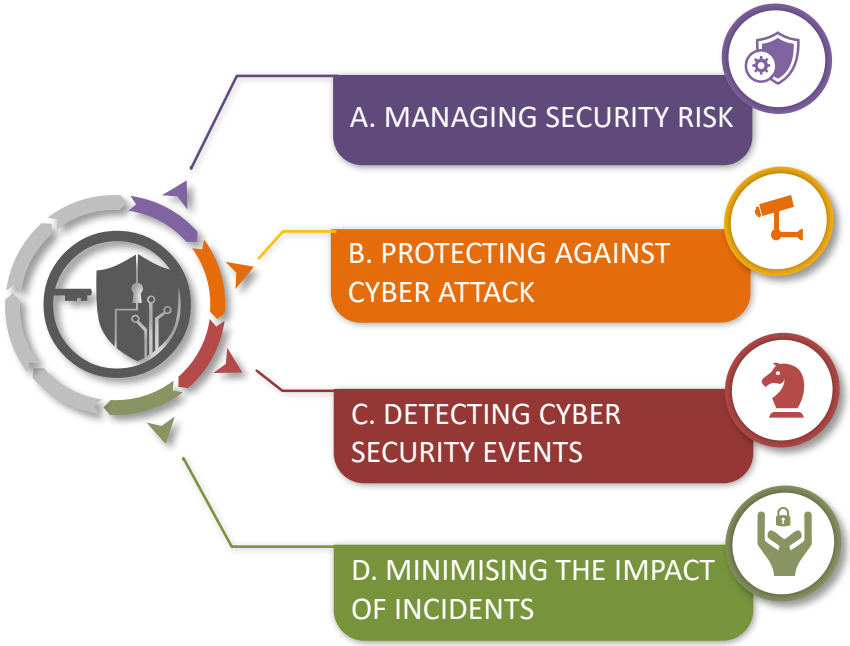


Understanding of key cyber security risks

Understanding gaps security architecture and risk management framework

Quantification of the impact on compliance obligations

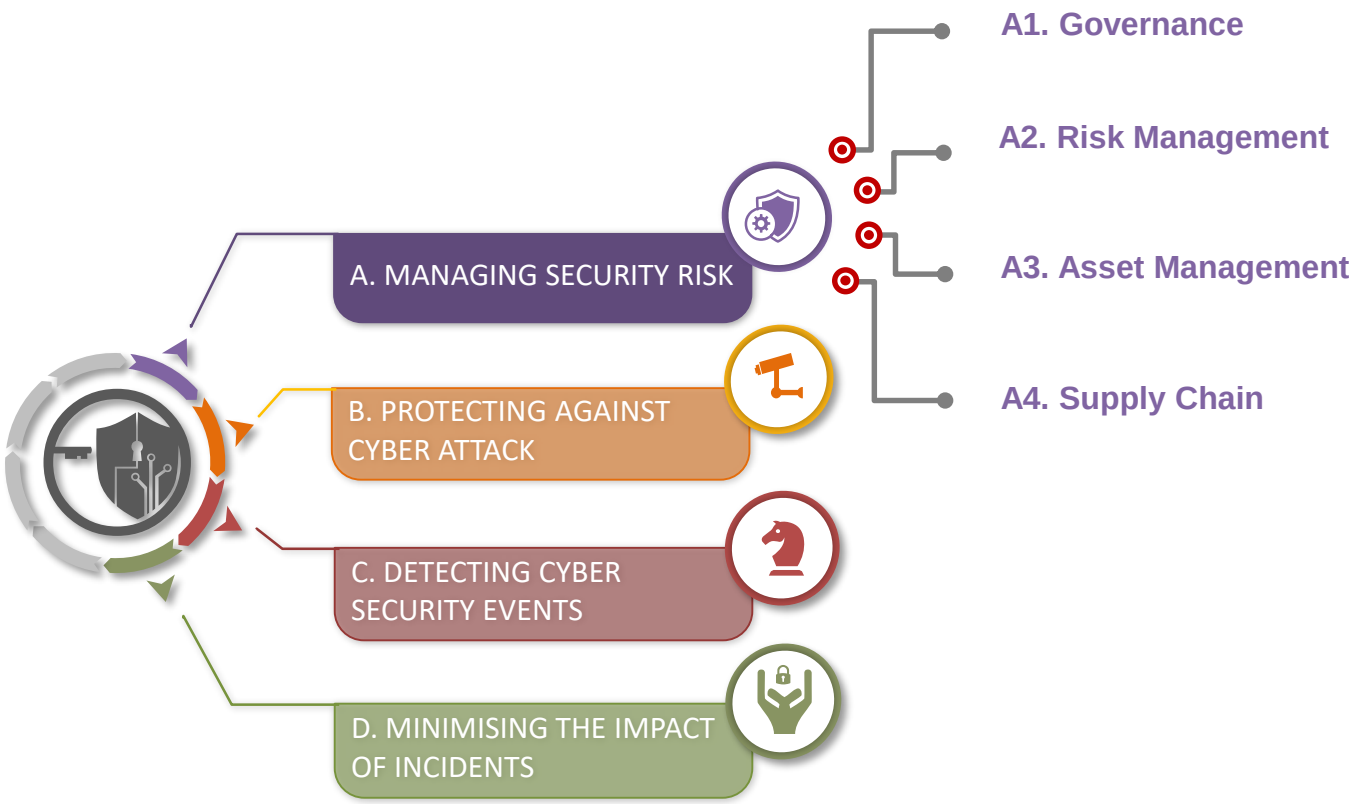
NCSC Cyber Assessment Framework



- NCSC Cyber Assessment Framework provides an approach to understanding operational cyber security maturity
- Especially relevant to Utilities as it is designed to cover both enterprise IT as well as Operational Technology systems

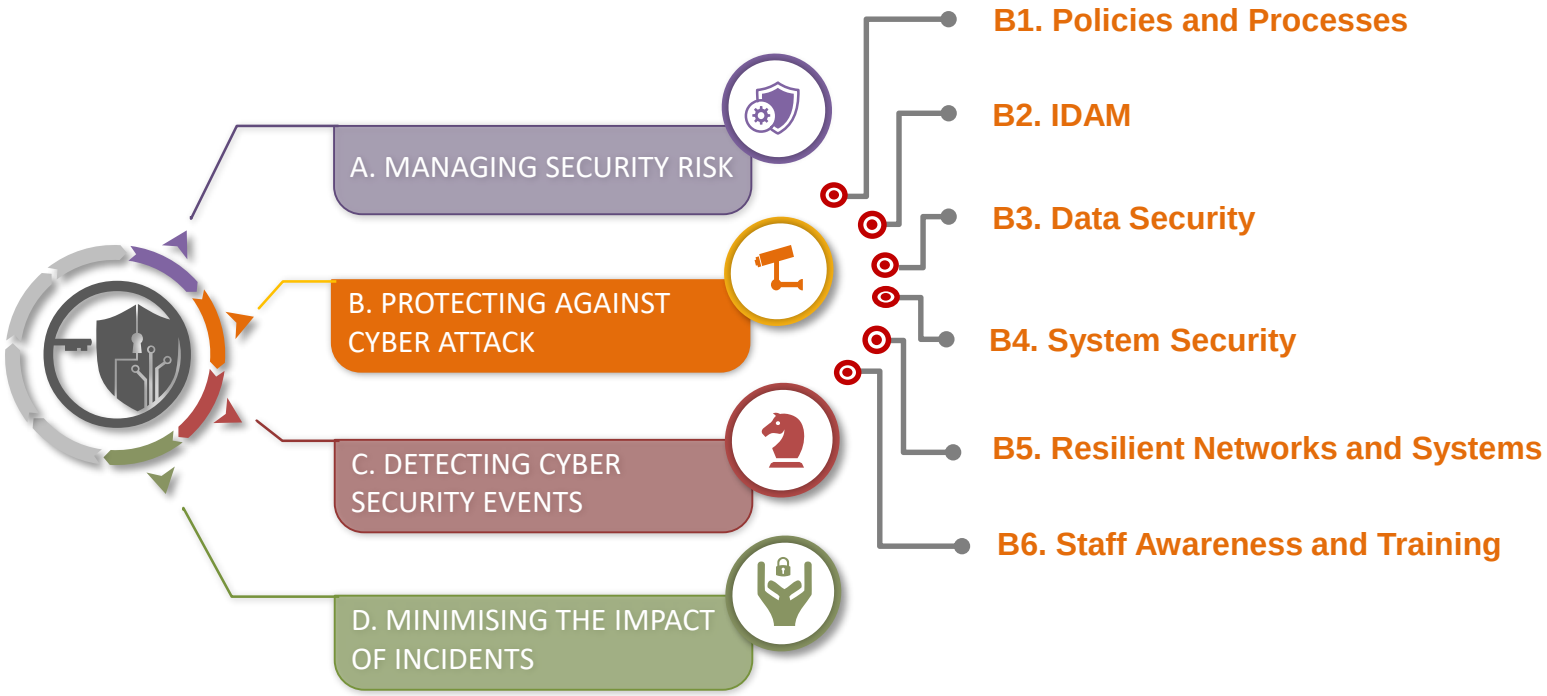
https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework

NCSC Cyber Assessment Framework



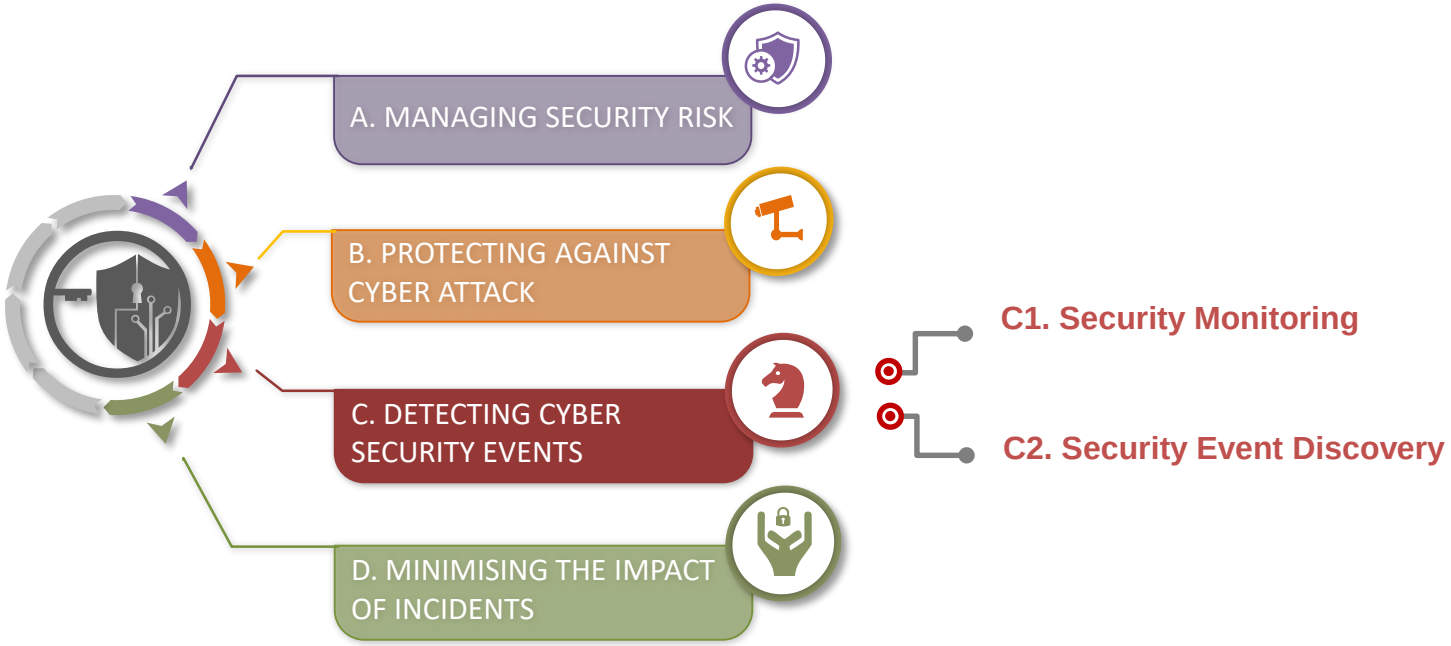
https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework

NCSC Cyber Assessment Framework



https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework

NCSC Cyber Assessment Framework



https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework

NCSC Cyber Assessment Framework

https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework

Concluding Remarks

COVID-19 has resulted in rapid changes to organisational culture and technology

In the Utilities sector, this has driven forward the trend of increased connectivity to Operational Technologies

In the case of COVID enforced changes, the normal pattern of user behaviour lagging behind technological changes is reversed

This makes an understanding of the drivers of security behaviours especially important, alongside targeted actions to improve these

A retrospective assessment of the risks to critical services and capabilities will provide assurance that risks remain in line with your risk appetite, and that you remain compliant with obligations

More widely, organisations should adopt an approach to security that delivers Operational Resilience, in line with business objectives

THANK YOU

leonardocompany.com

Contact details

Max Wigley

Head of Consulting,
Leonardo Cyber Security Division
Email: max.wigley@leonardocompany.com
Tel: 07825 541434

Richard Quinlan

Head of Sales and Business Development,
Leonardo Cyber Security Division
Email: richard.quinlan@leonardocompany.com
Tel: 07500 915444

Scott Bartlett

Manager Consultant,
Leonardo Cyber Security Division
Email: scott.bartlett@leonardocompany.com
Tel: 07854 029477

leonardocompany.com