

Approaches to Cyber Resilience and Supply Chain Assurance





Introductions

- Dr Max Wigley
- Head of Cyber Consulting in Leonardo's Cyber Security Division
- 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.



Leonardo MW Ltd – UK Business



Bristol

200 people

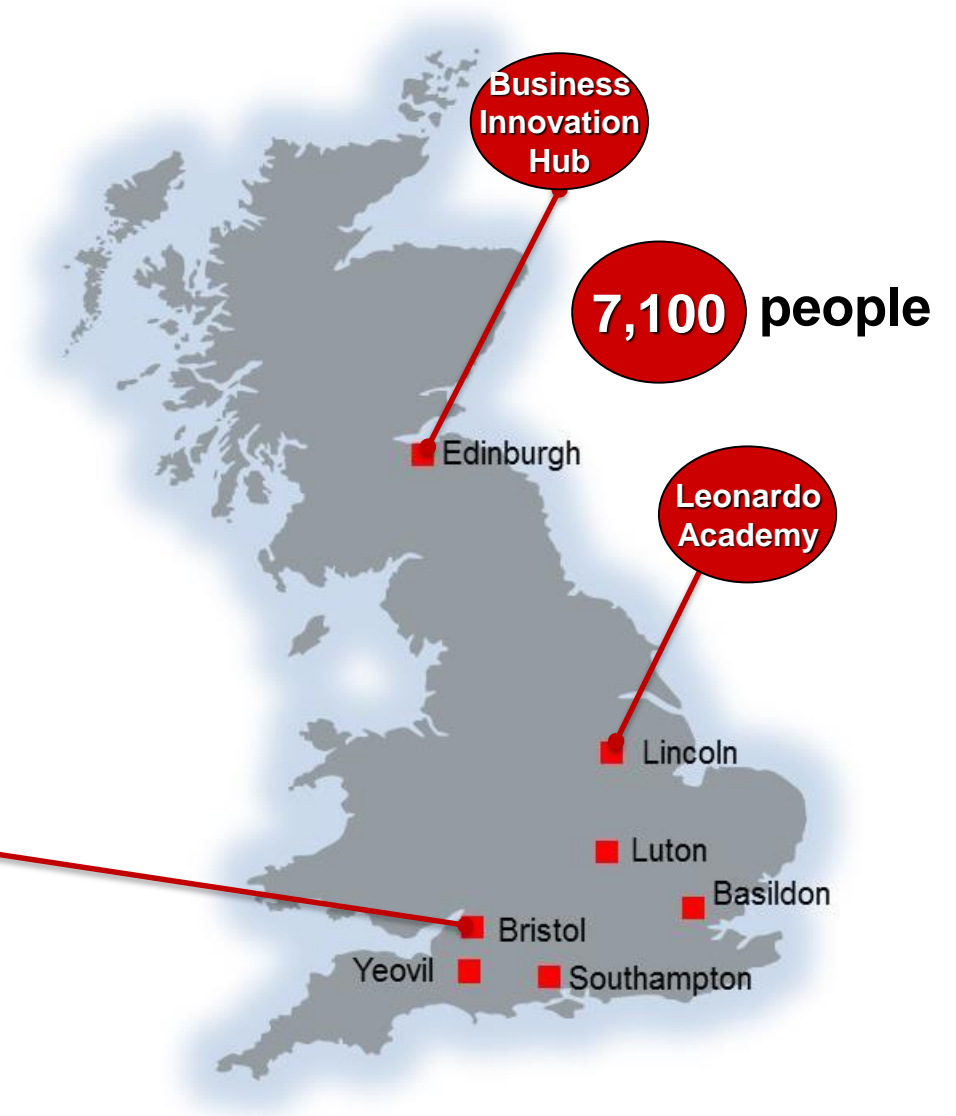
Cyber Security & ICT Solutions

- NCSC Certified Cyber Security Consultancy
- Cyber and Information Assurance
- Trusted ICT

Homeland Security & Critical National Infrastructure

- Critical Infrastructure Protection

Cyber Security





Why do we want Products to be Assured on Delivery?

Traditional security approaches too often result in changes being made to products late in the CADMID lifecycle or risks being accepted during operations

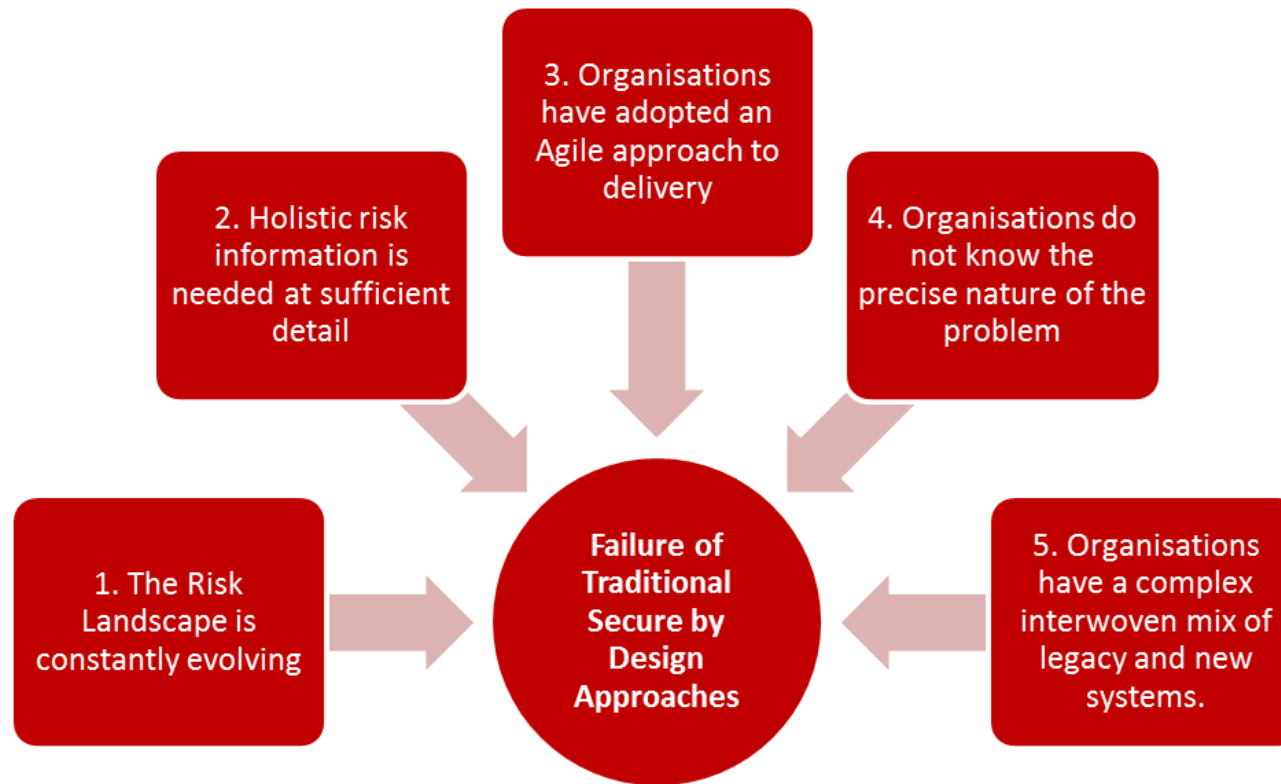
- Customers expect products and services to be “cyber assured on delivery”
- Rapidly changing digital systems need to be approached differently
- Traditional risk assessments are often out of date soon after delivery.
- An agile approach to secure by design is therefore needed.





Why do Traditional Approaches to Security Fail?

Traditional approaches are often inflexible and do not accurately describe the cyber risk

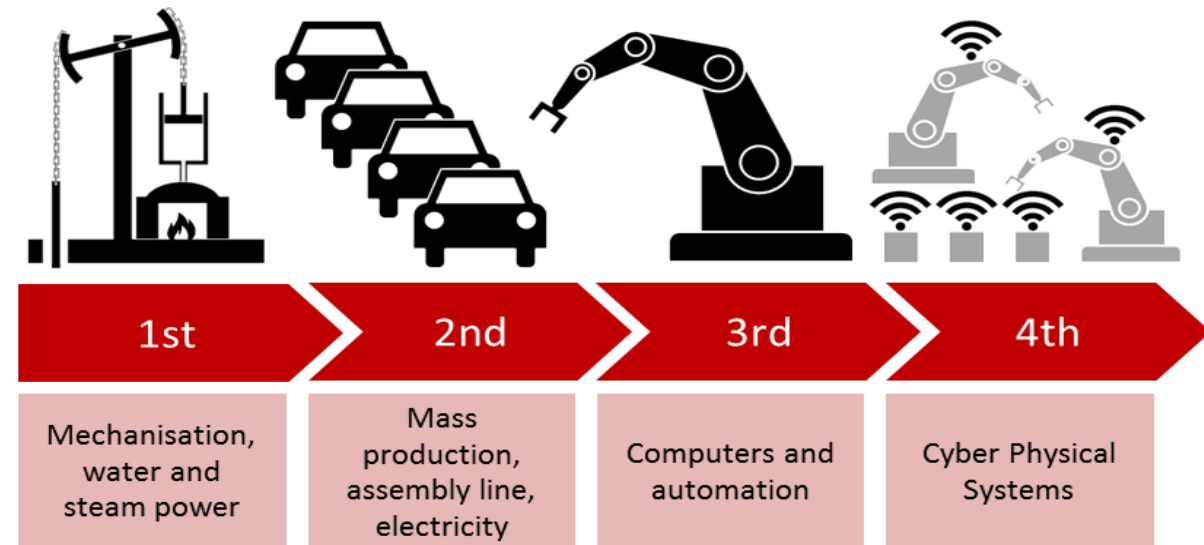




What is Cyber Resilience?

“The capability for organisations to continue to deliver services or capabilities during and after a cyber-incident, in a manner which is within the organisations risk appetite and in which critical information is protected”

- Cyber Resilience approaches assume that a breach will happen.
- Focus effort on implementing security controls that allow you to:
 - Detect attacks early
 - Contain, disrupt or monitor
 - Continue to operate
 - Safeguard assets

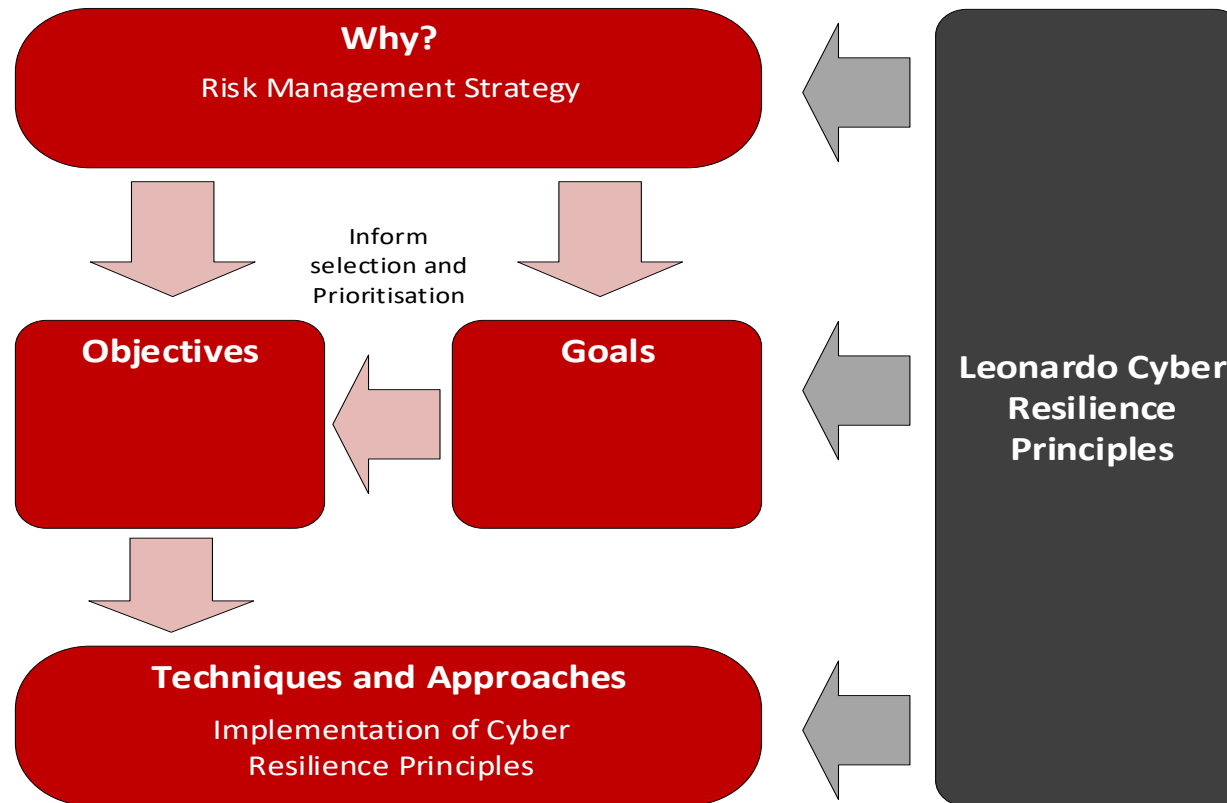


Christoph Roser at AllAboutLean.com



What does Cyber Resilience Mean for your Organisation?

Before embarking on the Cyber Resilience journey, it is crucial to define a strategy along with specified goals and objectives





Cyber Defence vs Cyber Resilience

Cyber Resilience and Cyber Defence tackle different security problems. Organisations and systems need an approach based on a threat and risk assessment

What or who are we defending against when we implement “good practice” cyber defence?

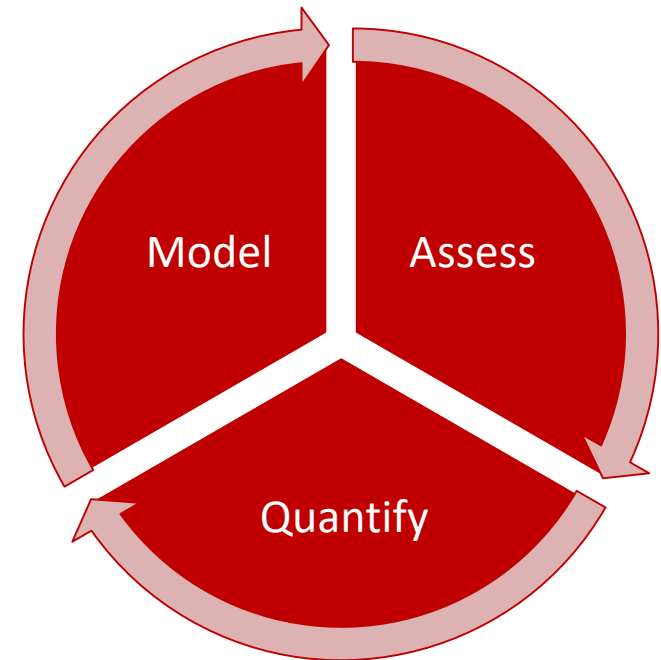




Use of an Attack Path Approach to Drive Agile Secure-by-Design

Iteratively development of security artefacts allows up to date risk information at all times

- It is not realistic to require a completed design to commence security assurance
- Iteratively develop attack paths, risks and security controls
- Embed security within the design team
- Provide accurate risk information at all times to support decisions



How does Supply Chain fit in?

Modern supply chains are complex and distributed and can be used to deliver a cyber effect, or for intelligence gathering.



Direct Supply Chain Attacks

Adversary aims to access sensitive information, or compromise critical services

Indirect Supply Chain Attacks

Adversary attacks a supplier to gain intelligence




How do we know if Suppliers Present Risk?


A holistic approach is needed. Current approaches focus on sensitive information, meaning that the risk picture can be incomplete

Supply chains can provide or hold one or more of:


- Sensitive Information
- Critical Services / Capabilities
- Critical Identifiable Information



How exposed are you if one of your suppliers is compromised?



How many companies does your procurement process release sensitive information to?

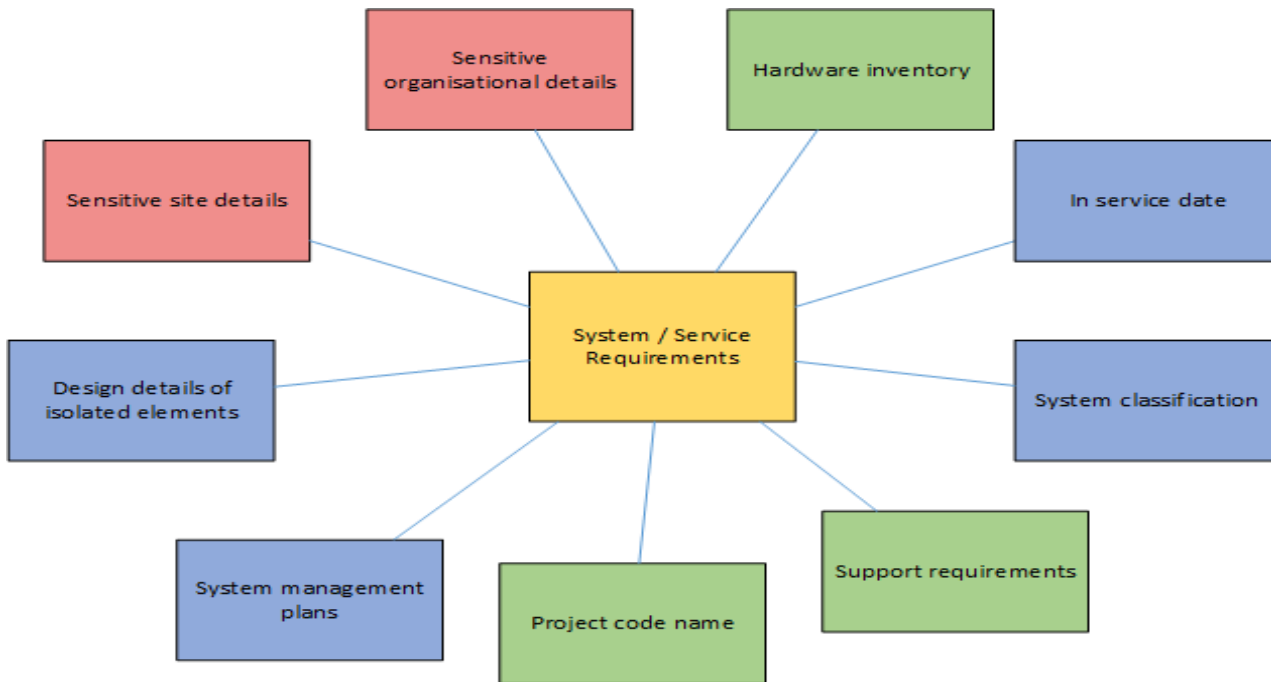


How much sensitive information do your suppliers hold?



Sensitive Information is Released Inadvertently in Procurement Documentation

The risk associated with information release during procurement processes needs to be understood – balancing competition and security.

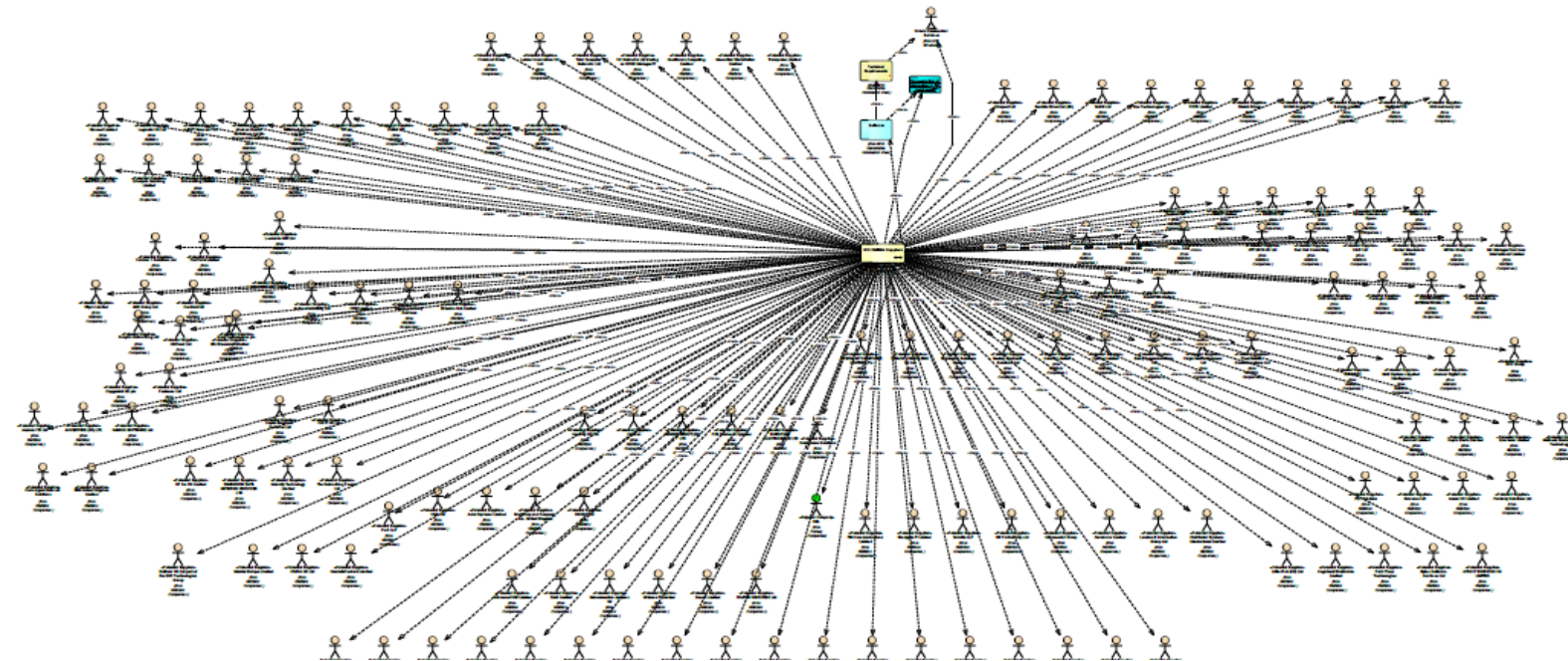


- Adversaries want a high success rate
- Much information is available from open sources
- Information obtained via supply chain adds refinement and understanding



How widely is information disseminated?

Organisations need to be aware of the scale of information release via chosen procurement approaches, and consider the aggregated risk of this for a product / capability.



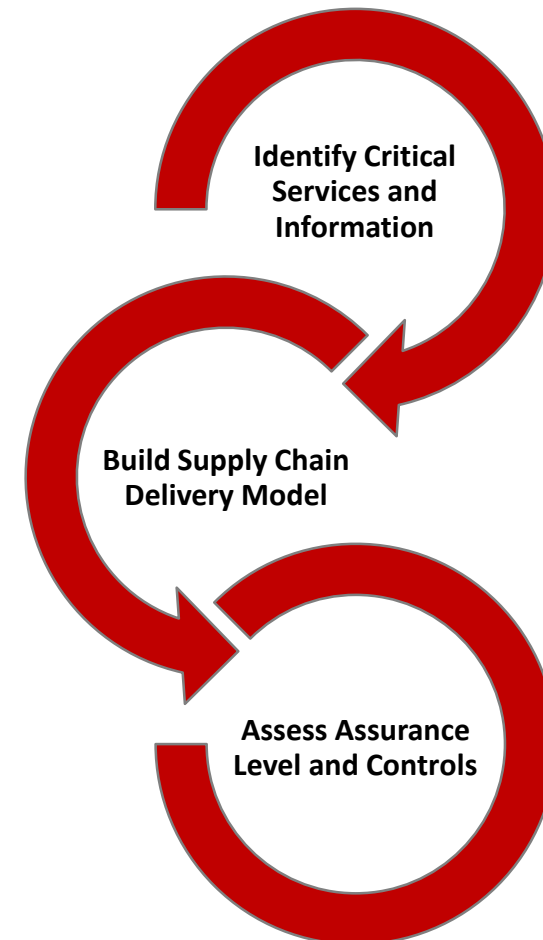
- Framework procurements release information widely
- Many recipients have no interest in bidding
- Approaches must cover more than just those organisations on contract



What Assurance do you have over Supplier systems?

Ultimately risk owners want to know where in the supply chain they are exposed, and what action needs to be taken.

- Adopt a Systems Engineering approach to understanding supply chains
- Consider sensitive information, critical services and critical identifiable information
- Approach to assurance / security proportionate to risk
- Identify gaps, risks and any actions required





Risk is not a Dirty Word

Security risk needs to be managed alongside other risk areas such as safety and programme risk. Key is understanding what risks you are accepting and how you are managing them.

- Digital Transformation does not need to be “risky”
- Security risk should be treated alongside other programme risks
- Ignoring or not assessing risk is not an option
- In the digital transformation, security can genuinely be an enabler:
 - Helping organisations find ways to do digital business without exceeding the risk appetite.





Summary and Conclusions

As the digital transformation proceeds, there is an opportunity for security to act as a genuine enabler. We must adapt our approaches to support improvements in capability

- Traditional approaches to security have often failed to deliver good business outcomes
- Need a flexible approach to deal with agile projects
- Cyber Resilience is not just another word for cyber security – need to find the right mix of defence and resilience
- Any holistic approach should include the supply chain
- Key is understanding the flow of information and capabilities, and a proportionate approach to assurance at each point
- As the digital transformation proceeds, there is an opportunity for security to act as a genuine enabler to support improvements in capability



THANK YOU FOR YOUR ATTENTION

leonardocompany.com

Max Wigley
max.wigley@leonardocompany.com

07825 541434