Delivering Cyber Resilience to increase Competitive Advantage

Version1-0

February 2019

Leonardo
430 Coldharbour Lane, Bristol Business Park, Bristol, BS16 1EJ, United Kingdom
Telephone: +44 (0)117 9880033 www.uk.leonardocompany.com

1 INTRODUCTION

There has been a lot of focus in recent years on Defensive Cyber Security. Whilst organisations invest in Cyber Defence, it is often assumed that this effort will prevent cyber-attacks from taking place.

In line with the UK Digital Transformation, the business/industrial landscape is changing rapidly, with the increasing adoption of Cyber Physical Systems leading to a transition towards Industry 4.0. Within this transition, the growing importance of interconnected systems to delivery of critical services means that managing the cyber risk effectively can deliver a significant competitive advantage.

Whilst preventative security controls can reduce the likelihood of an event occurring, it is almost impossible to decrease that likelihood to zero. Therefore alongside defence in depth and delivering secure by design, it is crucial for organisations also to invest in Cyber Resilience.

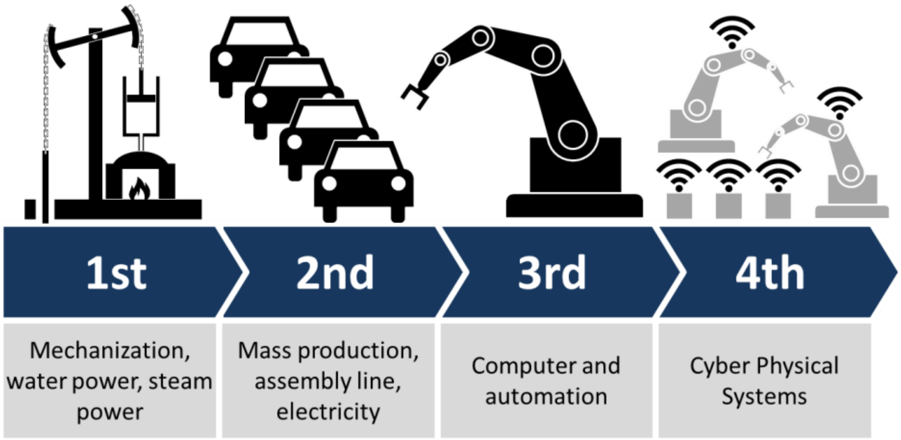
1st
2nd
3rd
4th
Mechanization, water power, steam power
Mass production, assembly line, electricity
Computer and automation
Cyber Physical Systems

Figure 1. Cyber Physical Systems are changing the industrial landscape.[1]

1.1 What is Cyber Resilience and why is it important?

Cyber Resilience is not a new concept; however there is not, as yet, a single recognised definition. Leonardo considers Cyber Resilience to be:

> *"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"*

Fundamentally, adopting an approach based on cyber resilience makes the assumption that a cyber security breach will happen. Whilst this is not to say that cyber resilient organisations do not put measures in place to deter and prevent cyber-attacks, in addition they focus effort on implementing security controls that:

a. **Detect attacks** in their early stages;

b. **Contain the adversary** – restrict adversary movement within the estate, and thereby reduce the ability to deliver their objectives;

c. Capture **actionable intelligence** of adversarial actions;

[1] Christoph Roser at AllAboutLean.com

d. Allow services to **continue to operate**, even in a cyber-affected state;

e. **Safeguard assets** - prevent the compromise of critical information assets.

Adopting an approach based on cyber resilience allows organisations to both improve their Cyber Defence, and also ensure that they can continue to operate in the face of cyber-attacks.

2 HOW DOES CYBER RESILIENCE FIT WITH EXISTING SECURITY APPROACHES?

Cyber Resilience complements and builds on existing security approaches and should be incorporated into existing Information Security Management Systems and Risk Management Structures.

Traditional security frameworks such as ISO27001 or Cyber Essentials do not explicitly consider Cyber Resilience, focussing more on the protection or management of information from a perimeter security perspective. Whilst they cover elements of the principles outlined below, and certification to these standards is a positive step towards appropriate management of risk to an organisations services and information, it is important to understand that their focus is generally on prevention of Cyber Incidents and recovery from Cyber Incidents, rather than the resilience of critical functions. Cyber Resilience approaches therefore sit alongside and complement Defensive Cyber Security measures.

2.1 Relationship to the Security Lifecycle

Cyber Resilience is not simply putting in place measures to respond in the event of an attack – adopting cyber resilience requires controls across the whole security lifecycle:

a. **Prepare** – designing and implementing controls for Cyber Resilience in line with the principles in section 3;

b. **Secure** – managing your estate and ensuring the Cyber Resilience controls are effective and up to date;

c. **Detect** – monitoring systems for unusual activity;

d. **Respond** – providing effective containment and investigation options in the event of a breach.

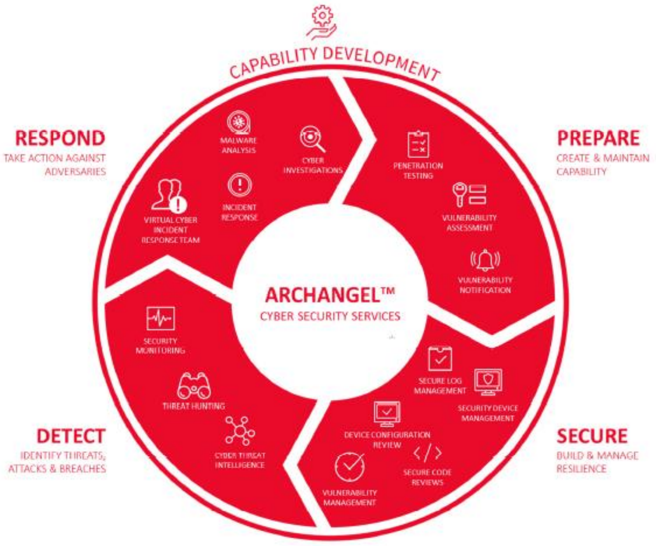

Figure 2. Leonardo Cyber Capability Model

Gaps in any of these areas of the security lifecycle will reduce the overall effectiveness of security controls in other areas. It is therefore crucial to adopt a holistic approach in line with an overall security strategy.

Leonardo's cyber capabilities and services are aligned both to the NIST Cyber Resilience Framework (see 2.2. below), and our own Cyber Resilience Principles set out in section 3.1.

2.2 Goals and Outcomes of Cyber Resilience

Ultimately Cyber Resilience aims to allow organisations to maintain operations in a secure manner during a cyber security incident.

NIST SP800-160 volume 2[2] defines four goals of cyber resilience, intended to shape the overall approach.

a. **Anticipate** - Maintain a state of informed preparedness for adversity;

b. **Withstand** - Continue essential mission or business functions despite adversity;

c. **Recover** - Restore mission or business functions during and after adversity;

d. **Adapt** - Modify mission or business functions and/or supporting capabilities to predicted changes in the technical, operational, or threat environments.

NIST SP800-160 allows organisations to define the outcomes they want to achieve and then the Cyber Resilience Techniques that can be used to deliver these. This can then be linked back to the organisational risk management / security strategy, which in turn allows activities to be assigned to an organisations goals and for benefits to be tracked.

Figure 2 below illustrates how defining an approach to Cyber Resilience fits into the overall risk management strategy. The strategy will inform the definition and prioritisation of an organisations cyber resilience goals and objectives. It should contain the way in which the Cyber Resilience Principles set out below are to be applied. These in turn allow appropriate techniques and approaches to be defined in order to implement the principles and meet the organisational goals.

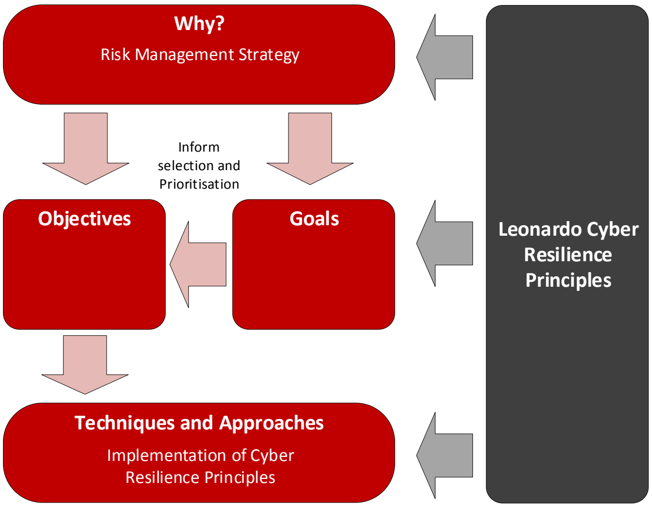
Why?
Risk Management Strategy
Inform selection and Prioritisation
Objectives
Goals
Techniques and Approaches
Implementation of Cyber Resilience Principles
Leonardo Cyber Resilience Principles

Figure 3. Relationships between Cyber Resilience Constructs (NIST SP800-160[1]) and Leonardo Cyber Resilience Principles

[2] NIST SP800-160 Vol 2 - Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems

3 HOW CAN ORGANISATIONS DELIVER CYBER RESILIENCE?

As with any transformation or capability development, adopting Cyber Resilience is a journey which requires appropriate planning and management to ensure it is successful.

a. **Define the strategy** – as with all aspects of security, ensuring an endorsed defined strategy is in place will provide a framework within which activities are conducted, and the overall direction to ensure benefits and progress can be evidenced;

b. **Prioritise activities** based on a set of attack scenarios driven by threat and risk – it is important that any investment is shown to deliver value. Prioritising activities will ensure resilience is not over-engineered in some places and under-engineered in others;

c. **Create a roadmap** for capability development – define the sequence of activities and the associated resilience capabilities in line with the strategy and prioritisation, so that all stakeholders can understand the process and benefits;

d. **Test and Validate** controls that have been implemented to provide assurance they are effective.

3.1 Principles of Cyber Resilience

Leonardo suggests the following 6 principles to guide development of Cyber Resilience within organisations. These are not intended to replace existing cyber resilience frameworks, but to guide an organisation in setting and implementing a security strategy, and appropriate cyber resilience goals.

These Principles should be a core part of an organisational cyber resilience strategy, which should define what these mean in the context of your organisation, and how they should be applied.

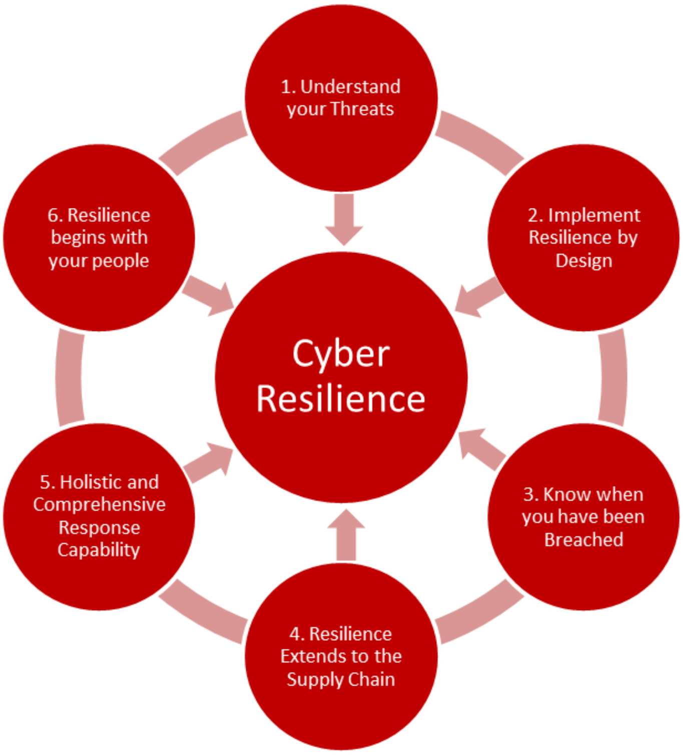
1. Understand your Threats
2. Implement Resilience by Design
3. Know when you have been Breached
4. Resilience Extends to the Supply Chain
5. Holistic and Comprehensive Response Capability
6. Resilience begins with your people
Cyber Resilience

Figure 4. Leonardo's Principles of Cyber Resilience

3.1.1 Principle 1: To Understand your Resilience Capability, you need to Understand your Threats

The first step is to understand where you are potentially exposed from a cyber perspective, who is likely to target your organisation and what their aims will be. This will allow all other controls to be prioritised and targeted at areas of risk. Leonardo adopts an approach based on attack path analysis – identifying how an adversary could use cyber exposures on your systems to deliver the cyber effect. This leads to a set of prioritised attack scenarios which are the basis for many of the other security principles. Our attack path based approach[3] to threat and risk analysis results in a deep understanding of the root cause of risks and exposures to your organisation's critical services.

3.1.2 Principle 2: Strategy and Technology should be Resilient by Design

Designing systems based on the underlying assumption that they will be compromised represents a shift in thinking; however this shift is crucial to ensuring that when an attack does occur that services continue to operate and the ability of an adversary to deliver their aims is limited. Organisations may wish to consider the following as part of an approach based on Resilience by Design:

a. **Adopt a Layered Approach** - as micro-services become more prevalent and estates are geographically dispersed, creating a strong perimeter behind which to put critical information and services is increasingly infeasible. Start from the assumption that the adversary will compromise your network boundary and implement controls to prevent lateral movement. For example, approaches could include:

    (1) Secure internal services with TLS;

    (2) Implement network segregation, isolating critical information stores and capabilities;

    (3) Make use of virtualisation and containers to isolate applications and services – especially those which are externally facing, reducing the impact of a compromise;

    (4) Require robust authentication, even within the network boundary.

b. **Manage Trust and Interactions** - start from a position of distrust and only allow interactions within your network which are properly authenticated and which are permitted for legitimate business transactions.

    Understand the interactions that are required both internally and externally within your network and block those which are not expected. Start with the key attack scenarios and work down the priority list.

c. **Implement Appropriate Redundancy** - understand what components are crucial to delivery of services and ensure that these have appropriate protection against failure.

Our Security Architecture Service[4] helps customers to design and implement appropriate controls to manage risks to their critical services.

[3] https://www.digitalmarketplace.service.gov.uk/g-cloud/services/288471076391375

[4] https://www.digitalmarketplace.service.gov.uk/g-cloud/services/924725993656423

3.1.3 Principle 3: Understand when you have been Breached

Once you have understood what key attack paths and scenarios present the biggest risk, you need to know when or if these scenarios are occurring. Understand what these attack scenarios would look like on your estate and monitor for this activity.

Organisations can use the MITRE ATT&CK^{TM} framework to help build this capability. MITRE ATT&CK helps you identify the Tactics, Techniques and Procedures used by an adversary to achieve particular goals and allows monitoring solutions to target these. Our Security Monitoring Assessment[5] helps customers identify the base events to collect and the SIEM rules required to detect key attack scenarios.

3.1.4 Principle 4: Cyber Resilience Extends to your Supply Chain

In modern distributed systems, critical information assets and capabilities are often held or delivered by third parties. It is critical to understand the risks associated with use of supply chain and implement cyber resilience controls as part of the overall organisational approach.

See https://www.uk.leonardocompany.com/-/secure-supply-chain for a more in depth discussion on supply chain security.

3.1.5 Principle 5: You need a Response Capability that is Holistic and Comprehensive

In order to continue to operate with a compromised estate, you need an appropriate response capability. The adversary does not care about your internal organisational structure, or who looks after what areas of your estate and therefore your response must be holistic and cover all areas.

a. **The response capability must be pan-organisation -** prepare for Cyber Incidents to occur and include all elements of the organisation in the response. Adversaries do not care about your internal organisational structure, so your response needs to be holistic. Consider running a set of cyber exercises[6] to provide assurance that the holistic response will be effective.

   This consideration extends beyond your organisational borders. Leonardo recently described how both suppliers and customers should be involved in a robust response capability[7].

b. **Response capability must be comprehensive and empowered** – the response needs to cover every corner of your estate and cover both managerial and technical aspects. Pre-authorisation is needed to allow the necessary containment or active defence actions to occur. This will ensure you can understand the adversary and feed back into threat intelligence and security monitoring to prevent a recurrence of the same incident again.

3.1.6 Principle 6: Resilience Begins with your People

All capabilities are socio-technical in nature and any approach to Cyber Resilience must consider not just the technology but also the people and process elements. In many cases humans are the

[5] https://www.digitalmarketplace.service.gov.uk/g-cloud/services/145501896278634

[6] https://www.digitalmarketplace.service.gov.uk/g-cloud/services/788487617439223

[7] https://www.uk.leonardocompany.com/-/customers-part-of-supply-chain-risk-management

weak link so any cyber resilience efforts must include appropriate mechanisms for driving the required behavioural change within the organisation.

4 CONCLUSIONS

As the UK and Global industries transform towards increasing reliance on Cyber Physical systems, organisations who adopt Cyber Resilience will thrive and can deliver a consistent high quality service to customers. Cyber Resilience offers a genuine differentiator to boost competitive advantage as customers are increasingly cyber-aware.

Cyber Resilience sits alongside and complements traditional defensive approaches to implementing security controls. It allows organisations to continue to operate critical services during a cyber attack, whilst also safeguarding critical assets. Leonardo has experience guiding organisations through developing Cyber Resilience, and has set out 6 principles to help achieve this.

We have a track record in delivering appropriate Cyber Resilience capability for organisations through Cyber Vulnerability Investigations, Security Monitoring Assessments, Incident Response services and Cyber Training / Culture assessments.