

Cyber Security Strategy

Briefing for Executives in the Civil Nuclear Sector

 **accenture**

 **context**
Part of **Accenture Security**

Agenda

1.

Introduction

2.

Security strategy
principles

3.

The role and
importance of cyber
security strategy

4.

Governance
and leadership

5.

Threat landscape &
managing risk

6.

Strategy
development

7.

Security culture

8.

What about your
strategy?

Introduction



Strategy:

A plan to achieve an objective, over a defined period of time.

A cyber security strategy provides objectives for an organisation's desired future security state, and is integrated with the business strategy.

This calls for an understanding of the current state, with the strategy setting the course for achieving the desired future state.

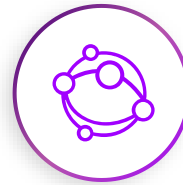
A cyber resilience strategy requires:



Understanding of organisational risk.

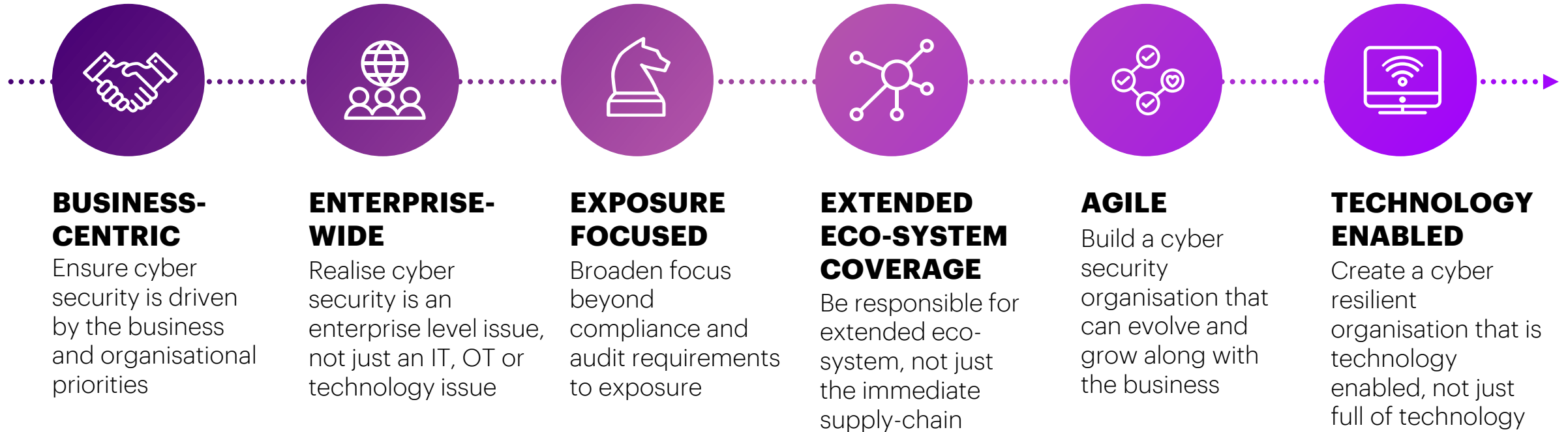


Activities to secure personnel and systems to prevent and resist cyber attacks.



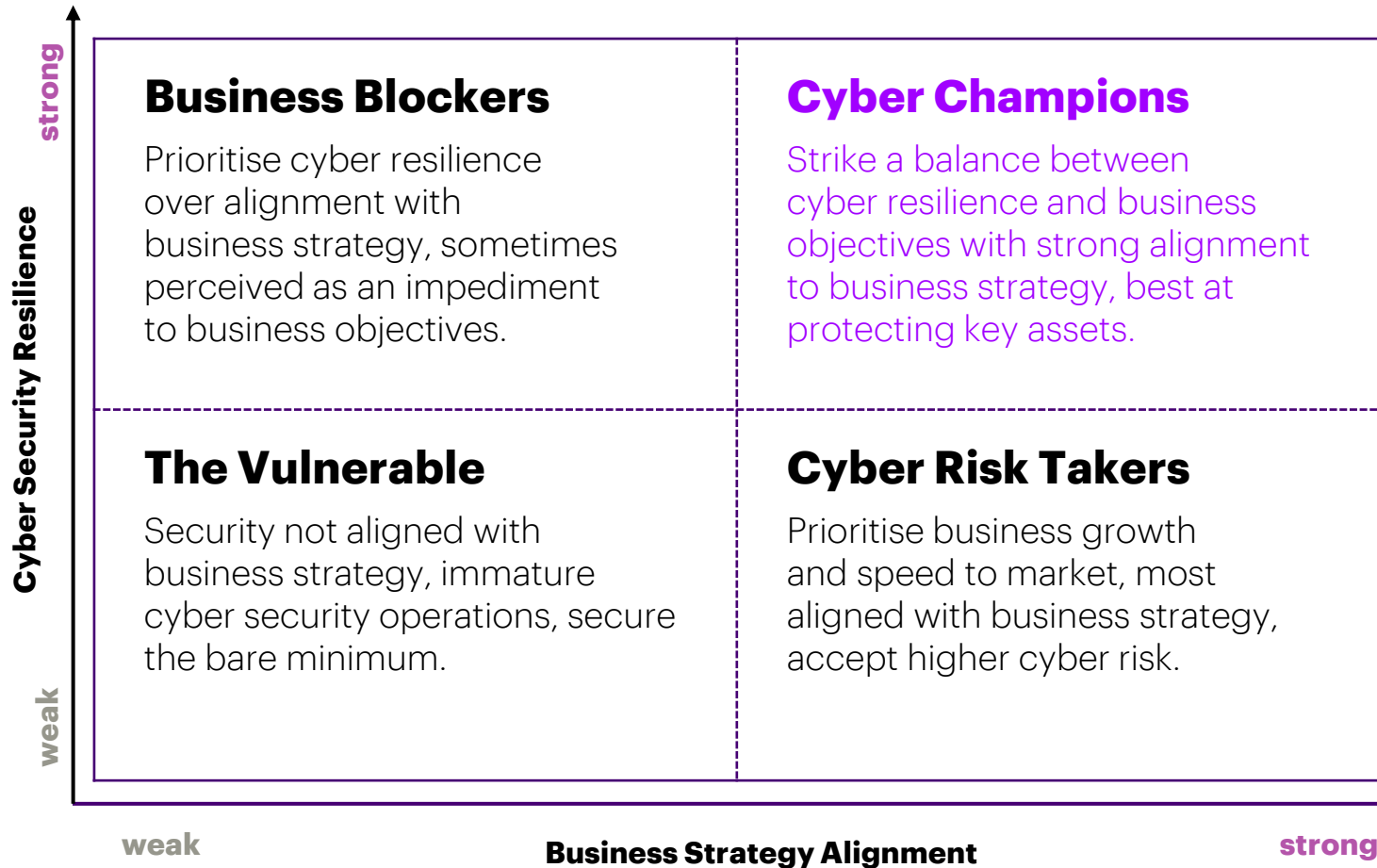
Preparation to ensure sufficient resilience in the event of a cyber attack, to minimise the impact and enable recovery.

Cyber resilience strategy guiding principles



Where are we today?

Accenture State of Cyber Security Resilience Survey 2021



Source: Accenture State of Cybersecurity Resilience 2021, security executives (N=3,455: Cyber Champions N=172, Business Blockers N=522, Cyber Risk Takers N=885, The Vulnerable N=1,876)



We identified four levels of cyber resilience, including an elite group of

Cyber Champions

Measurable data from clients - the benefits of alignment

Accenture State of Cyber Security Resilience Survey 2021

	Cyber Champions	Business Blockers	Cyber Risk Takers	The Vulnerable
Stop more attacks: Number of attacks that breach security	1 in 6	1 in 4	1 in 2	1 in 2.3
Find breaches faster: % breaches found in < 1 day	55%	50%	11%	15%
Fix breaches faster: % fixed in 15 days or less	100%	96%	30%	30%
Reduce breach impact: % breaches with no impact	72%	64%	23%	24%

Source: Accenture State of Cybersecurity Resilience 2021, security executives (N=3,455: Cyber Champions N=172, Business Blockers N=522, Cyber Risk Takers N=885, The Vulnerable N=1,876)

The role and importance of a cyber security strategy



The cyber security strategy:

1. Sets organisational intent and describes what outcomes are to be delivered
2. Defines the cyber risk appetite/tolerance & identifies threats to the organisation
3. Ensures that cyber security capability is proportionate to the risk to the business
4. Ensures adherence to relevant good practice and industry mandatory baselines
5. Is a regulatory requirement for dutyholders

Security governance

Governance establishes and maintains the cyber security framework, with supporting process to ensure the security programme aligns with organisational objectives.

Senior stakeholders set the desired goals and outcomes by managing risk and determining the level of acceptable risk.

Outcomes include:

Strategic alignment –
with organisational
vision and mission

Risk
management

Delivering value through
balanced, prioritised and
proportionate investment
in activities

Measurement with
monitoring and reporting
(KPIs), and enabling 'course
correction'

“ **Security governance is the means by which you control
and direct your organisation's approach to security.** ”

Source: <https://www.ncsc.gov.uk/collection/risk-management-collection/governance-cyber-risk/security-governance-introduction>

Importance of governance & leadership

1. Leadership and culture - 'setting the tone'
2. Direction setting and allocation of responsibility to senior management
3. Alignment and integration of cyber security strategy with wider organisational goals and objectives, in particular risk and business strategy
4. Approval of the strategy, including decisions, implementation, operational progress and implementation ensuring alignment to business strategy to support business objectives
5. Leadership holds primary accountability for discharging legal, regulatory and mandatory requirements – with personal risk
6. Delivery and demonstration of due care and diligence

Cyber resilience and leadership - challenges



Cyber resilience and cyber risk management are critical challenges for many organisations.



The board and the top level executive often report they lack the tools and competencies to manage cyber risks the way they manage other risks.



The need for a common vocabulary is often noted as an issue.



Creating a shared understanding and frame of reference for security. Case studies or stories can make information relevant, supported by access to specialist advisors.

State of Cyber Security Resilience 2021

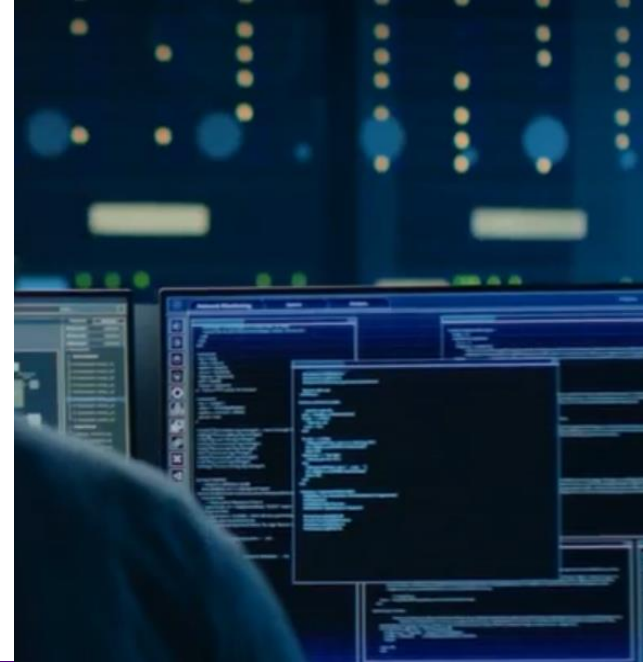
Are security and non-security executives on the same page?

	Security executives	Non-security executives
 Security effectiveness: My organisation is well-protected from cyber threats.	57%	32%
 Spending: Estimated percent of IT budget spent on security in my organisation.	12%	34%
 Attacks in my organization: • Number of attempted breaches • Number of attempted ransomware attacks	885 227	36 35



Source: Accenture State of Cybersecurity Resilience 2021, security executives (N=439) and non-security executives (N=50)
United Kingdom N=489

Threat landscape



Terrorism

Nation State

Supply Chain

Insider Activity

Crime

Force Majeure

Human Error

Hacktivism

Sabotage

**Corporate
Espionage**

Risk assessment and risk appetite



Risk assessment

“ The organisation takes appropriate steps to identify, assess and understand security risks to the critical systems supporting the operation of essential functions. This includes an overall organisational approach to risk management. ”

Source:

<https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework/caf-objective-a-managing-security-risk>

The board holds management accountable for reporting cyber risk assessment as a standing agenda during board meetings.



Risk appetite

“ The organisation's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objective ”

Source:

https://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf

The board should regularly ensure business risk tolerance is consistent with risk appetite

Business risks relating to security - example

A number of business risks have been identified many of which are directly or indirectly related to security. Below are the selected key risks that have direct security implications

SECURITY BREACHES

The reliance on many legacy systems remains a challenge, and security breaches could bring enterprise wide impact operations, harming reputation, competitive advance and result in financial and legal penalties.

INTERNATIONAL TENSIONS

Instability across developed and emerging markets, such as dynamic legal and tax regimes, political and economic tensions may cause of international operations disruption.

SUPPLY CHAIN & INDUSTRIAL DISRUPTIONS

Operations depend on efficient distribution networks to deliver its products to consumers. Security needs to be embedded along the supply chain to prevent operation, production and distributions disruptions.

THIRD PARTY

Our operations have considerable reliance on third-party vendors in key information systems and business processing services. With greater reliance on third parties comes greater security challenges in ensuring they each comply with our security standards and policies and regulations.

COMPETITION

Competition and changing new market entrants could change the industry's landscape. This also means increased likelihood of attacks driven by competitors.

LEGAL & REGULATORY

We are subject to various local and international regulations, including data protection and information security. Failure to comply with these laws may lead to significant financial and legal penalties as well as administrative sanctions.

INTELLECTUAL PROPERTY

Protection of our current and future products and innovations as well as trademarks, patents, domain names and trade secrets and know-how is key in maintaining our competitive advantage.

REPUTATION

Our reputation and ability in maintaining a strong and trustworthy brand image is key to the business' success in the market. We have witnessed an increase in cyber activists targeting the company. Any potential adversaries and security breaches may impact our reputation and therefore our business as a whole.

Security risks and subsequent potential impacts - example

Meanwhile, the existing audit reports and risk register indicated 6 critical security gaps...



Vulnerable OT systems

that are old, many of which are not appropriately patched to protect against known vulnerabilities



Weak access controls

including the use of default admin passwords and misuse of privilege accounts



Poor information security governance

with no defined roles and responsibilities, no consistent and effective risk evaluation methodology, and absence of Security Policies



Insecure enterprise system

A particular vendor's management of enterprise security risk is not enforced in the relevant contract



Poor internal network security

with limited controls, lack of 'security in depth' principles as well as vulnerability management process in place.



Inadequate manufacturing and supply chain security

With unpatched industrial systems will leave us at risk of serious disruption

...that could result in the following business risks :

R1

Unauthorised access to sensitive information and data theft

R2

Manufacturing/ Supply Chain Disruption

R3

Reputational damage

R4

Non-compliance to regulatory requirements, fines and penalties

R5

Ransom attack, BC issues

R6

Compromised network and lateral movement

R7

Exposed entry points for attackers into the systems

R8

Physical data theft

R9

Lack of accountability and visibility over enterprise security posture

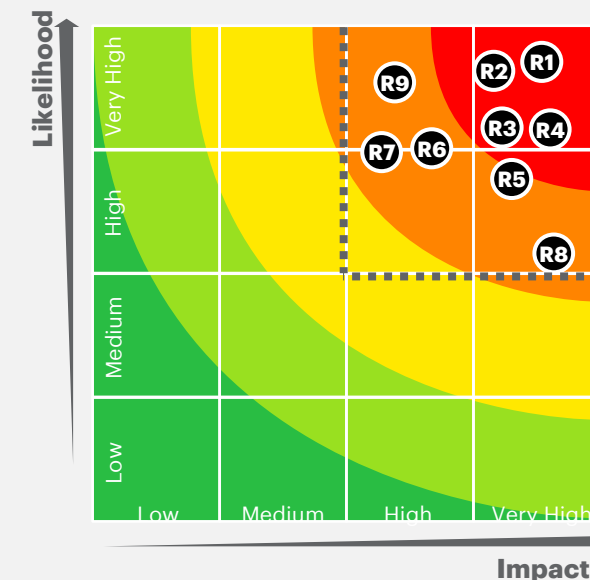
R

Very high likelihood and impact

R

High likelihood and impact

RISKS MATRIX



Elements of a good strategy

Prerequisite foundation: Purpose, vision and mission for security



01

Understanding risks, threats and vulnerabilities

02

Adopt good practice beyond compliance baselines - outcome focused to secure the business and “arrive at compliance”

03

Allow strategic and equal investment in prevention, detection, and response

04

Develop a robust governance, risk, and compliance framework

05

Cultivate a positive security risk aware culture

06

Maximise security efficiency by utilising strategic partnerships

07

Foster enterprise security visibility and response agility

08

Strive for security transparency within the business – it improves security

09

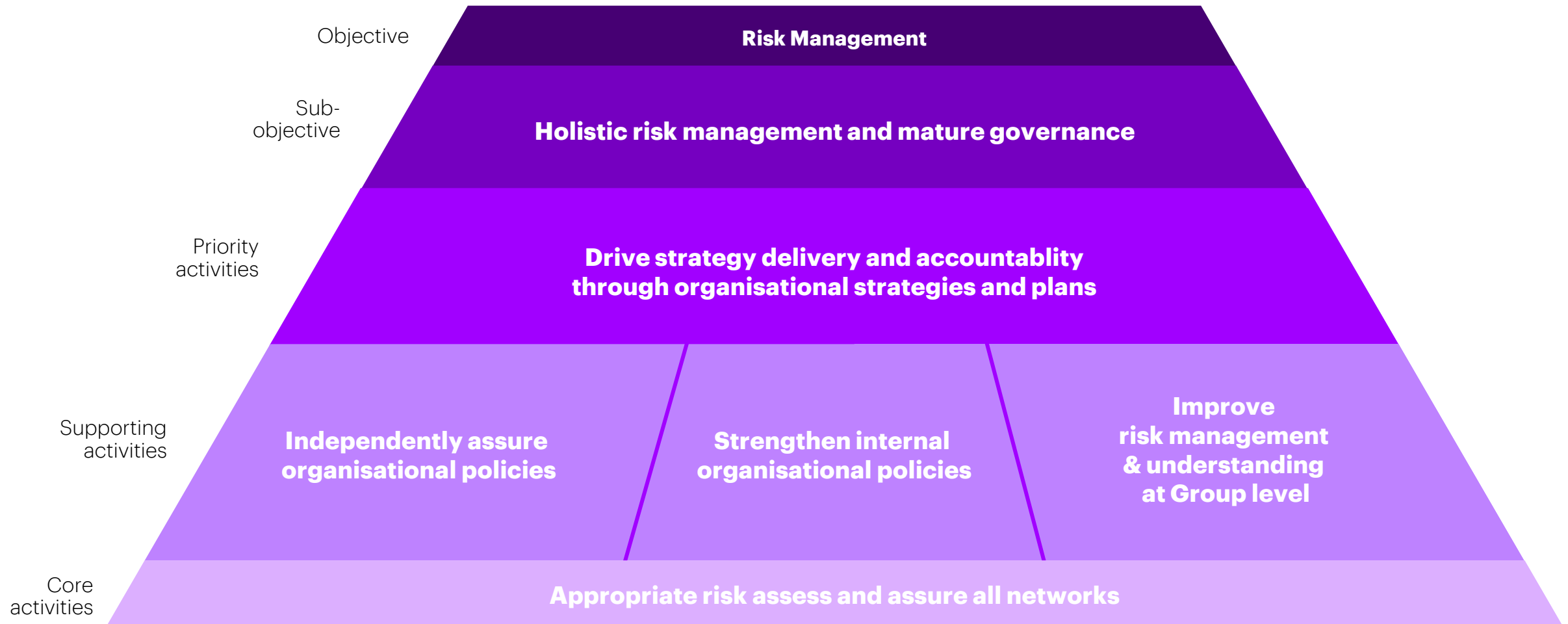
Continuous improvement & learning

10

Allocation of roles and responsibilities, including the accountable officer for cybersecurity

Setting the strategy objectives with programme activities

Priority objectives are set with cascading objectives and activities



Risk Management objective, with sub-objectives and supporting activities – Source Draft BEIS Civil Nuclear Cyber Strategy 2022

Determining current state & future state using cyber security frameworks & maturity models

National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) functions

Identify – Develop an organisational understanding to manage cyber security risk to systems, people, assets, data, and capabilities

Protect – Develop and implement appropriate safeguards to ensure delivery of critical services

Detect – Develop and implement appropriate activities to identify the occurrence of a cyber security event

Respond – Develop and implement appropriate activities to take action regarding a detected cyber security incident

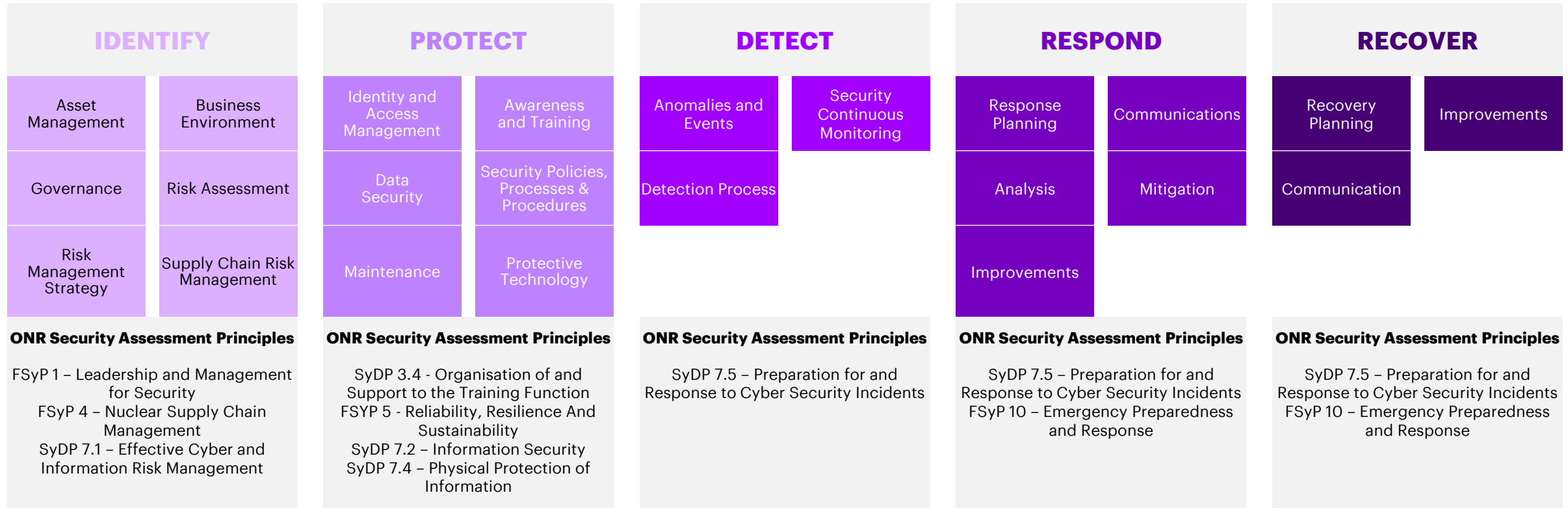
Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident

Assessing capability – a maturity model

Optimising	Fully managed capability that demonstrates consistency, integration with business processes, and continuous improvements for enhanced effectiveness
Managed	Consistently demonstrated capability that is integrated with the business, proactively managed and measured for effectiveness, but may not be continuous improved.
Defined	Sufficiently demonstrated capability that is integrated with some areas of the business but not proactively managed or measured for effectiveness.
Repeatable	There are documented, repeatable processes that may or many not produce consistent results .
Reactive	There are inconsistent processes that are likely not documented, consistently demonstrated, communicated, or aligned with the business.
Very Limited Capability	Very limited or no capability

Cyber security frameworks and resilience: programme pillars

Mapping NIST Cyber Security Framework to ONR Security Assessment Principles



Balancing cyber activities to enable response and recovery from an incident, not only to prevent one.

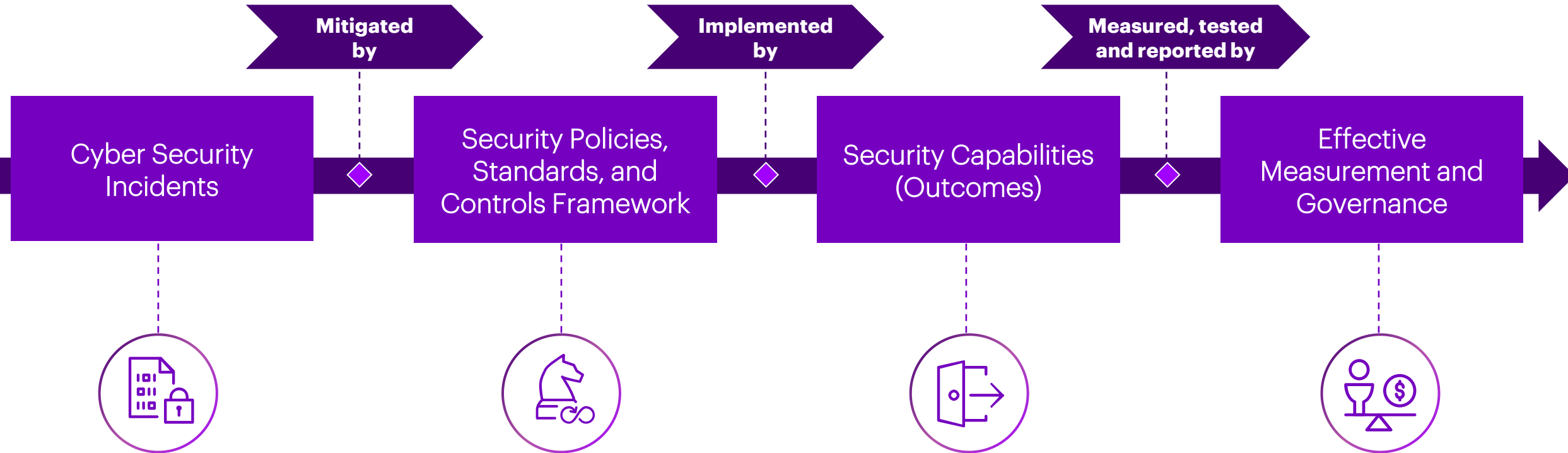


Frameworks can be used to define fundamental outcomes which the strategy seeks to achieve.

Security management framework - example

Our Security Strategy will provide end to end traceability of cyber and information security, business risk and threat management through defined governance, policy and control monitoring

Security Strategy



Positive security culture

Leadership defines and demonstrates a positive security culture

The security culture is the foundation of daily life in the organisation, where poor security behaviours are simply not acceptable.



01

Is there an open approach to assess security in a no-blame manner?



02

What level of training and awareness do employees have?



03

How could employees or an insider cause an incident, intentionally or by accident?



04

Does the culture enable cyber resilience to be used as a justification?

What about your strategy?

- Do you have a cyber resilience strategy that aligns with the business strategy?
- Is your vision and mission for cyber security clear and understood?
- Have the organisational critical assets or “crown jewels” been identified and do you understand their place in the value creation chain?
- Does the strategy scope cover the entire cyber environment; including, information systems, control systems, safety systems, security systems, building management systems?
- Do you demonstrate and lead a positive security culture?
- Does the organisation participate in sector and industry information sharing forums?
- What is the timeframe for your cyber resilience strategy? Does it align with business strategy timeframe? Shorter than 2-3 years is really operational planning.



Author

Richard Piggin

richard.piggin@accenture.com

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security.

Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services – all powered by the world's largest network of Advanced Technology and Intelligent Operations centres. Our 700,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities.

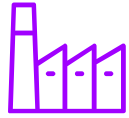
Visit us at www.accenture.com

Further information

- Accenture State of Cybersecurity Resilience 2021: <https://www.accenture.com/gb-en/insights/security/invest-cyber-resilience>
- Cyber Security Body Of Knowledge (CyBOK): <https://cybok.org/>
- ENISA Definition of Cybersecurity - Gaps and overlaps in standardisation: <https://www.enisa.europa.eu/publications/definition-of-cybersecurity>
- IET Code of Practice: Cyber Security and Safety: <https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/>
- MITRE ATT&CK® for Industrial Control Systems: https://collaborate.mitre.org/attackics/index.php?title=Main_Page&oldid=9504
- Ministry of Defence Cyber Primer: <https://www.gov.uk/government/publications/cyber-primer>
- National Cyber Strategy 2022: <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022>
- NCSC Board Toolkit: <https://www.ncsc.gov.uk/collection/board-toolkit/>
- NCSC Cyber Assessment Framework (CAF): <https://www.ncsc.gov.uk/collection/caf>
- NCSC Questions for boards to ask about Cybersecurity (NCSC Board Toolkit): <https://www.ncsc.gov.uk/files/Board-toolkit-QAs.pdf>
- NIST Cybersecurity Framework (CSF): <https://www.nist.gov/cyberframework>
- ONR Security Assessment Principles (SyAPs): <https://www.onr.org.uk/syaps/>
- PAS 555:2013 Cybersecurity risk. Governance and management: <https://shop.bsigroup.com/products/cyber-security-risk-governance-and-management-specification/standard>
- World Economic Forum Cyber Resilience Principles Tools: https://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf
- World Economic Forum Principles for Board Governance of Cyber Risk: <https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk>

Case Studies

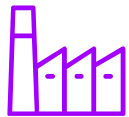
Incidents do happen



Norwegian Aluminium giant Norsk Hydro estimates impact of 2019 cyber attack that **impacted its smelting operations between \$65M to \$75M.**



The impact of the Colonial Pipeline ransomware attack is still unfurling. Class action **lawsuits are being filed** for supply chain/ ecosystem impacts.



TRITON malware was designed to **compromise the safety system of a petrochemical plant**, to override the safety system and cause a failure that would lead to a dangerous physical incident.



The transport and logistics company Maersk **declared losses exceeding \$300m** due to the NotPetya attack in 2017



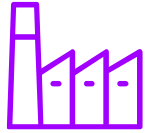
The Heathrow airport **was fined £120,000** for failed data protection on sensitive information in 2017



British Airways data loss in 2018 infringed GDPR – the initial penalty was **£183 million** which was reduced to £20m.

Case Studies

Norsk Hydro



Overview

- Ransomware impacted production in Europe and the US
- Reverted to manual operations
- Announced ransom would not be paid



Key points

- Initial access obtained with phishing email
- IT/OT convergence – impact on operations / unplanned downtime
- Leadership - Transparency after event. Norsk Hydro response was acknowledged an exemplar of good practice
- Norsk Hydro were fully open about the breach which included regular press conferences.
- Estimated financial impact \$65m – \$75m

Case Studies

Colonial Pipeline



Overview

- Ransomware attack impacted IT systems
- Network shutdown as a precautionary measure
- Interrupted the supply of 2.5 million barrels of aviation fuel, diesel, and petroleum daily across the entire US East Coast
- 100 gigabytes of data exfiltrated
- Exploited VPN remote access account with leaked password available on dark web
- CP paid \$5 million ransom – recovered a majority of bitcoin by the FBI (\$2.4m after bitcoin fluctuation)

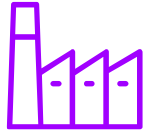


Key points

- Led to operational disruption and legal consequences
- Class action lawsuits are being filed for supply chain / ecosystem impacts
- Poor identity and access management permitted unused account without multi-factor authentication
- The supply chain impact to CNI and the US government, also affected European flights

Case Studies

Petrochemical facility
in the Middle East



Overview

- Triconex safety controller targeted with malware designed to manipulate industrial control systems
- Safety systems are used to protect systems and provide emergency shutdown

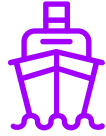


Key points

- Dubbed TRITON or TRISIS and HATMAN, the malware specifically targeted Schneider Electric's Triconex Safety Instrumented System
- Industrial safety systems run independently from main control system operating a facility, in order to monitor and prevent potentially dangerous conditions.
- The malware was designed to compromise the system and manipulate the controller to override the safety system and cause a safety-related failure that would lead to a dangerous physical incident.

Case Studies

Maersk



Overview

- NotPetya malware infected almost 50,000 end-user devices and thousands of servers
- Rebuilt all devices and applications within 2 weeks
- Reported around \$300 million in losses, despite maintaining 95% of regular shipments



Key points

- Led to potential reputational damage/prospect of organisational collapse – “company extinction event”
- Chairman: “average is not good enough, be good at it”, we will use cyber security to create competitive advantage
- Common security measures no longer robust enough against evolving threats
- Treating attacks as business risks, not technology concerns

Case Studies

Heathrow Airport



Overview

- USB containing unencrypted sensitive information was lost
- Data breach of personal data and airport security measures



Key points

- Data breach of personal information violated General Data Protection Regulation (GDPR)
- Information Commissioner's Office (ICO) imposed £120,000 fine
- Exposed sensitive information concerning security measures which could threatened airport security
- Absence of suitable policies and procedures for data security
- Incident exposed culture and awareness issues in data security

Case Studies

British Airways



Overview

- Breached the personal data of nearly 500,000 individuals
- Contravened the General Data Protection Regulation (GDPR)
- Compromised website and app which exfiltrated data to attacker
- Possibly malicious embedded code from third party – supply chain attack
- ICO initially filed a Notice of Intent to fine £183 million – subsequently reduced to £20 million



Key points

- Confidentiality/reputational damage – personnel and customer data
- There was an issue with culture and employees not following policies and procedures
- Managing supply chain risk and third party suppliers/partners