Cyber Security Strategy

Whitepaper for Executives in the Civil Nuclear Sector

accenture

context

Part of Accenture Security

Contents

1. Overview

The Office for Nuclear Regulation (ONR) requested that Accenture develop briefing materials to communicate the advantages of a good approach to cyber security strategy and resilience in the face of persistent and resourceful threats. This whitepaper covers strategy, leadership, governance, risk management and creating a positive security culture. We have also included case studies of strong, senior leadership delivering positive outcomes, and where poor leadership has led to capability gaps and cyber events impacting heavily on governance, reputation and the bottom line.

2. Audience

This whitepaper is targeted at board- and senior-level leadership within the dutyholders.

3. Purpose

This whitepaper provides an independent, cross-sector perspective to assist dutyholders to ensure they have a robust approach to cyber strategy and resilience. It provides additional information following earlier briefings, highlighting relevant good practice and it reflects Accenture's own experience.

4. Introduction

Cyber security has become an encompassing term, with a variety of definitions and intended meanings. This is noted by the Cyber Security Body of Knowledge (CyBOK) project, funded by the UK National Cyber Security Programme. The CyBOK introduction concludes that a succinct and broad definition remains elusive in this new and emerging knowledge area.[1] This is likely to be an issue for boards, where a common understanding is essential. The use of recognised cyber security frameworks can assist in communicating and managing cyber risk.

The CyBOK team highlight the almost exclusive focus upon information and related technical cyber security measures, often omitting the crucial areas of human behaviour and the impact of breaches from loss of information, safety or disruption of operations. They also consider networked control systems, where the imperative is to prevent unwanted physical actions.

Cyberspace is now being used to describe the operating environment, with virtual and real impacts. This topic has been introduced to a broader audience in the UK National Cyber Strategy 2022, from its original military use, describing the uniqueness of the cyber landscape and its physical impacts:

"The cyber domain is a human-made environment and is fundamentally shaped by human behaviour. It amplifies such behaviours for better or worse, the impacts of which are usually also felt in the physical world."

National Cyber Strategy 2022, pp 17-19.[2]

Organisations are now striving for cyber resilience, not just protection, with strategies that ensure durability and the opportunities it can provide as a business enabler. The World Economic Forum (WEF) distinguishes cyber resilience from cyber security, with a more strategic, long-term outlook, driven by leaders that recognise the importance of risk mitigation and proactive risk management. Organisational leaders that set the strategy are ultimately responsible and are increasingly being held accountable for cyber resilience. [3]

5. Cyber resilience and strategy

The cyber-resilient organisation brings together the capabilities of cyber security, business continuity and enterprise resilience. It embeds security across the business ecosystem and applies fluid security strategies to respond quickly to threats, so it can minimize the damage and continue to operate under attack. As a result, the cyber resilient organisation can introduce innovation and operating models securely across the entire value chain, strengthening trust and instilling confidence.

The cyber security strategy provides objectives for an organisation's desired future security state, and is integrated with the business strategy. This necessitates an understanding of the current state, with the strategy setting the course for achieving the desired future state within a defined period.

A cyber resilience strategy requires:

- An 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.

1. Cyber Security Body Of Knowledge (CyBOK): https://www.cybok.org/media/downloads/Introduction_v1.1.0.pdf
2. National Cyber Strategy 2022: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022
3. World Economic Forum Principles for Board Governance of Cyber Risk : https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk

6. The role and importance of cyber security strategy

Organisations pursuing cyber resilience require their senior stakeholders to proactively manage cyber risk, alongside other enterprise risks. Leaders set the organisational intent and describe outcomes to be delivered in the strategy. The strategy documents decisions and is used to control implementation and progress, whilst ensuring it aligns with the need of the organisation's business strategy.

A resilience focused strategy enables organisations to take advantage of digitisation and technological change, with an approach that enables the business and provides a source of competitive advantage, whilst maintaining value.

Cyber security strategy alignment with business priorities ensures the resulting outcomes are proportionate to the risk faced by the business. The strategy quantifies organisational cyber risk appetite and tolerance. It will also identify threats to the organisation. Using recognised cyber frameworks will assist in the application of relevant good practice and meeting sector baselines. As such, it is also a regulatory requirement for dutyholders, being critical to effective implementation (Figure 1).

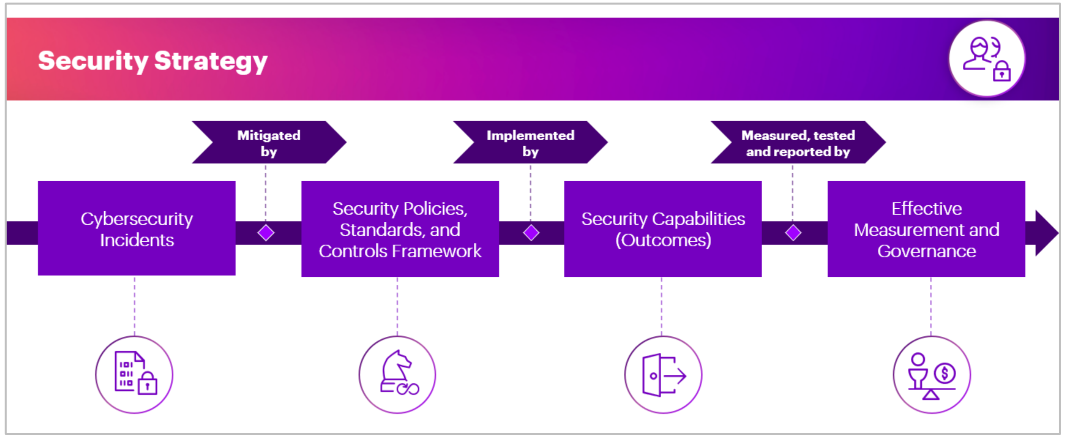

Security Strategy
Mitigated by
Implemented by
Measured, tested and reported by
Cybersecurity Incidents
Security Policies, Standards, and Controls Framework
Security Capabilities (Outcomes)
Effective Measurement and Governance

Figure 1. Cyber security strategy implementation

7. Security strategy principles

When we assist organisations in the implementation of their cyber resilience programmes, our approach uses the following guiding principles:

- **Business-centric.** Ensure cyber resilience is driven by business and organisational priorities. Our research showed this was a key differentiator of cyber resilient organisations, with significant financial advantages.
- **Enterprise-wide.** Cyber is an enterprise level issue, to be treated in a similar manner to other organisational risks. It isn't just an IT, Operational Technology (OT) or a technology issue. It is an operating environment with risk, in the same way we operate in a physical environment, where physical risks manifest.
- **Exposure focused.** We must focus beyond compliance requirements to address actual exposure to be cyber resilient.
- **Extended ecosystem coverage.** Be responsible for your extended eco-system, not just the immediate supply-chain. Recent events have demonstrated systemic risks flow from the complex nature of digital systems and the interconnectivity with other systems and organisations. The Colonial Pipeline, Solarwinds and NotPetya incidents illustrate systemic risks.[4,5,6]
- **Agile.** We seek to build cyber security organisations that can evolve and grow along with the business.
- **Technology enabled.** Create a cyber resilient organisation that is technology enabled, not just full of technology. Your strategy should be technology agnostic, focusing on the desired outcomes, whilst providing flexibility to keep pace with technological change.

Nation state destructive malware disrupts shipping operations - 2017

The NotPetya malware infected almost 50,000 end-user devices and thousands of servers at the international shipping company Maersk, and affected many other organisations. Maersk managed to rebuild all devices and applications within 2 weeks. The company reported approximately $300 million in losses, despite maintaining 95% of regular shipments. The Maersk Chairman, Jim Hagemann Snabe told the World Economic Forum in Davos they faced a company extinction event, and being average at cyber security is not enough, you have to be good at it. Maersk intends to use cyber security to create competitive advantage and treat these attacks as business risks, not technology concerns.

[4] US Department of Energy, Colonial Pipeline Cyber Incident : https://www.energy.gov/ceser/colonial-pipeline-cyber-incident
[5] Foreign, Commonwealth & Development Office, Russia: UK exposes Russian involvement in SolarWinds cyber compromise: https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise
[6] Wired, The Untold Story of NotPetya, the Most Devastating Cyberattack in History: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

8. Governance and leadership

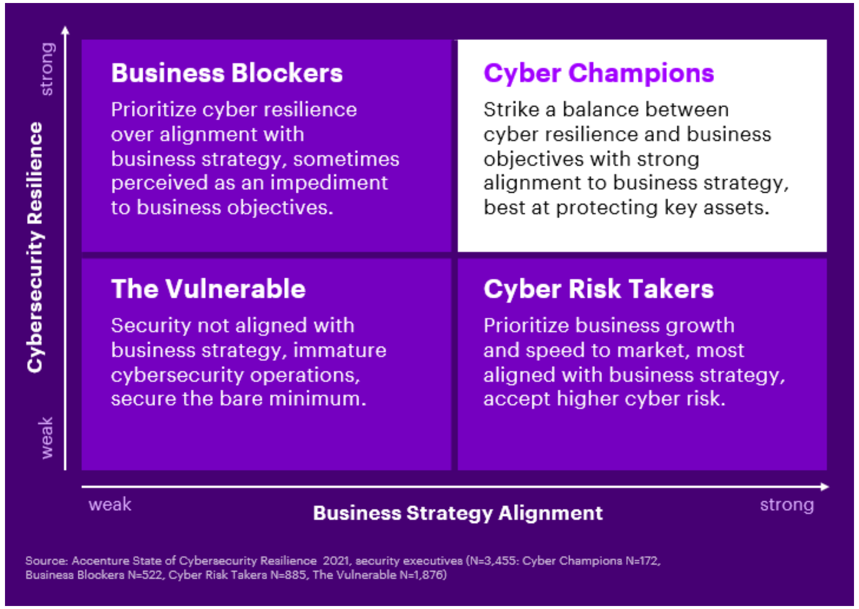
The board and senior-level leadership are ultimately responsible for your organisation's cyber risk and resilience. The leadership holds primary accountability for discharging legal, regulatory and mandatory requirements. As such, governance shortcomings may impact the individual too. Especially where OT cyber risks could lead to physical harm. The leadership team must be aware of their role and responsibilities.

All staff must understand their responsibilities for security and cyber resilience. It is essential that the leadership sets the tone for fostering and maintaining the organisational security culture, including managing cyber risk with safety.

The governance function establishes and maintains the organisational framework, with supporting process to ensure the security programme aligns with organisational goals and objectives. Our research has shown a stronger alignment between cyber security practices and the business strategy achieves better outcomes (Figure 1). [7]

An outcome-based approach, such as the Office for Nuclear Regulation's Security Assessment Principles and the National Cyber Security Centre's Cyber Assessment Framework places the onus upon boards to manage risk and apply suitable judgement to achieve specified outcomes. Combining an outcome focus with risk management and the application of recognised cyber security frameworks provides greater business resilience and benefits over just chasing compliance. Implementation experiences demonstrate improved risk understanding, identifying strengths and areas for improvement, informed risk tolerance and prioritising security remediation, facilitating resource allocation and security budget setting.

Good governance should ensure accountability for decisions, their implementation and the measurement of progress with key performance indicators. These will enable course corrections and the provision of feedback to senior stakeholders. An organisational wide governance structure and cyber security strategy will support the delivery of cyber resilience and demonstrate due care and diligence.



Business Blockers

Prioritize cyber resilience over alignment with business strategy, sometimes perceived as an impediment to business objectives.

Cyber Champions

Strike a balance between cyber resilience and business objectives with strong alignment to business strategy, best at protecting key assets.

The Vulnerable

Security not aligned with business strategy, immature cybersecurity operations, secure the bare minimum.

Cyber Risk Takers

Prioritize business growth and speed to market, most aligned with business strategy, accept higher cyber risk.

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)

Figure 2. Four levels of cyber resilience

Nation state targeted attack on petrochemical safety system - 2017

Dubbed Triton, Trisis or Hatman, the malware specifically targeted Schneider Electric's Triconex Safety Instrumented System with the intent to manipulate industrial control systems in a Middle Eastern petrochemical plant. Safety systems are used to protect systems and provide emergency shutdown. Industrial safety systems run independently from the main control system 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 failure that would lead to a dangerous physical incident.

Cyber resilience and effective cyber risk management are critical challenges for many organisations. The consequences of poor security strategy can lead to reputational damage, loss in shareholder value, safety incidents and governance issues. Boards often say they lack both tools and competencies to manage cyber risks in the same way they approach other risks. Cyber security vocabulary is frequently a challenge in developing mutual understanding between boards and specialists. Ensuring a common frame of reference, with case studies or stories can help. Raising cyber security competency, with access to specialist expertise, will help to develop senior stakeholder's knowledge, ensuring effective oversight.

Our research identified four levels of cyber resilience (Figure 2). The Cyber Champions—organisations that strike a balance, not only excelling at cyber resilience, but also aligning with the business strategy to achieve better business outcomes. They are successful in at least three out of four cyber resilience performance criteria— better at stopping attacks, finding and fixing breaches faster and reducing their impact.

[7] Accenture State of Cybersecurity Resilience 2021: https://www.accenture.com/gb-en/insights/security/invest-cyber-resilience

9. Risk management

Senior stakeholders set the desired priorities, goals and outcomes by managing risk and determining the level of acceptable risk or risk tolerance. The acceptable risk is the level of risk the organisation will bear after risk measures have been put in place. Expressing risk appetite in financial terms will inform decision making. Risk tolerance is more granular, focused on specific risks, and how the organisation would cope if they deviated from the risk appetite. Stakeholders should regularly ensure organisational risk tolerance is consistent with the organisational risk appetite. An example of risk identification and assessment is shown in Figure 3.

When undertaking risk assessments, an organisation will identify, assess, and seek to understand security risks to critical systems, both in IT and OT. It is important to assess the methods that might be used by attackers. The MITRE ATT&CK® knowledgebase illustrates adversary tactics and techniques, from initial access through to impact in IT and OT environments.[8] Organisations then need to put measures in place to specifically defend against them, and monitor progress with suitable key performance indicators (KPIs) to measure risk reduction. An example would be privileged account management, and relevant KPIs, including the number of users, the number of newly created users, and number of roles relative to number of departments.

The risk management topic also includes the organisational approach to risk, including governance, and management accountability for reporting cyber risk to the board. This forms the foundation to the governance operating model, which brings your security strategy and business objectives together and is used to operationalise the governance programme to monitor and support your cyber security initiatives. The implementation should provide end to end traceability of cyber security, business risk and threat management through defined governance, policy and control monitoring.

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

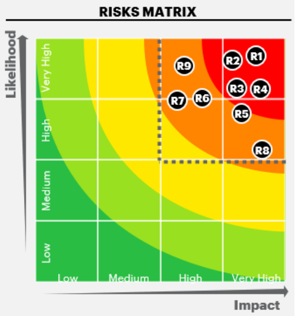
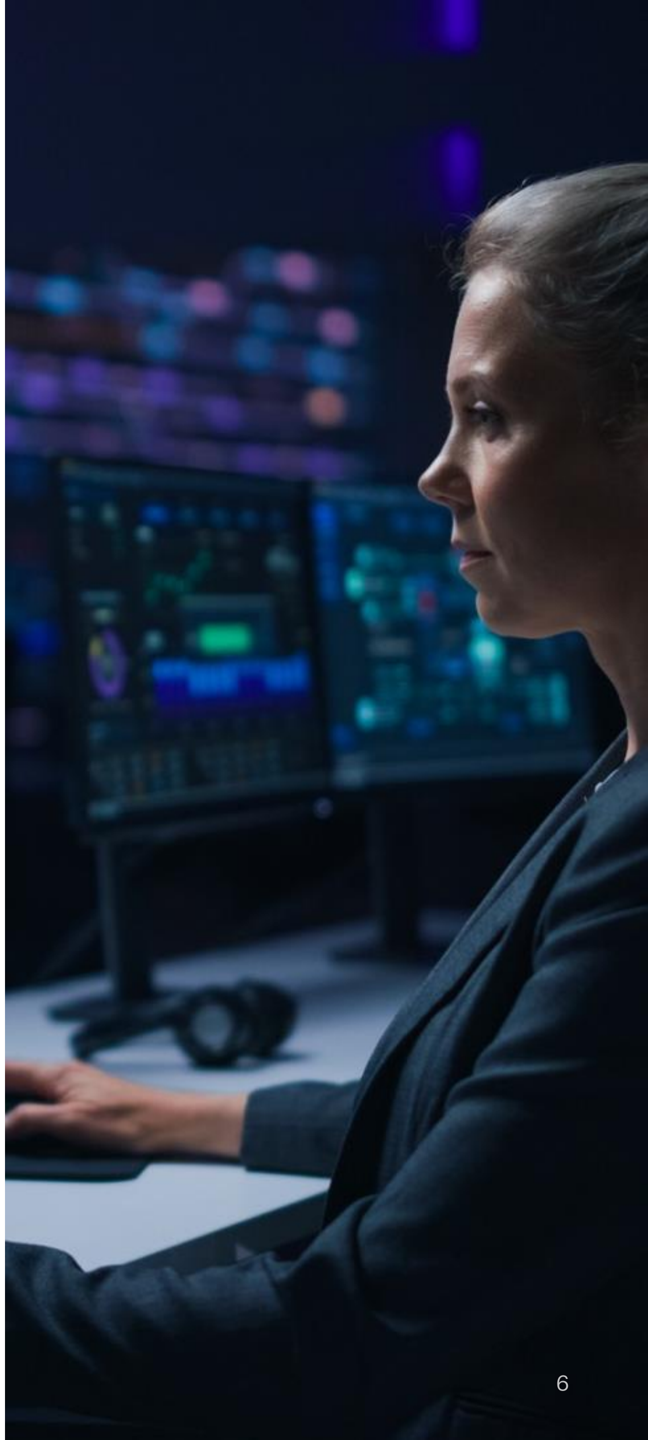


Figure 3. Risk management - likelihood and impact examples

Colonial Pipeline disruption - 2022

Darkside ransomware attack impacted IT systems, however OT systems controlling the pipeline were shutdown as a precautionary measure. This interrupted the supply of 2.5 million barrels of aviation fuel, diesel, and petroleum daily across the entire US East Coast. The ransomware gang used remote access account credentials which were available on the dark web. The majority of the $5 million ransom was recovered by the FBI ($2.4m after bitcoin fluctuation). The incident led to operational disruption with an international impact upon aviation, with panic buying of petroleum and lawsuits. Account management failings facilitated the initial access of the gang.

[8] MITRE ATT&CK® for Industrial Control Systems: https://collaborate.mitre.org/attackics/index.php?title=Main_Page&oldid=9504



10. Cybers security strategy components

Outlining the purpose, vision and mission are the starting points for the cyber security strategy. These capture how security will be an enabler to the organisation, unpinning strategic business objectives. An end-to-end understanding of how the organisation delivers value is an important lens when considering the risk and threats faced. This process will identify how various functions support activities in the value chain, and shape the security strategy, and the plan to address risks and threats.

The security concerns, such as Confidentiality, Integrity, Availability or Safety will drive security and their emphasis will differ across the value chain and their environments. OT requires different security approaches due to control systems and their physical interaction . An understanding of the degree of risk/consequence across the value chain is necessary to make informed decisions regarding security investments and strategic next steps. Thus, planning to protect what is important, often referred to as 'identifying the crown jewels.'

Cyber security frameworks can be used as a systematic approach to managing cyber risk. The functions shown in Figure are regarded as the essential pillars of a holistic cyber security programme:

Identify – understanding and managing risk to systems, people, assets, data, and capabilities.

Protect – implementation of safeguards and limiting the impact of cyber security incidents.

Detect – activities to identify a cyber security event and permitting timely discovery of an incident.

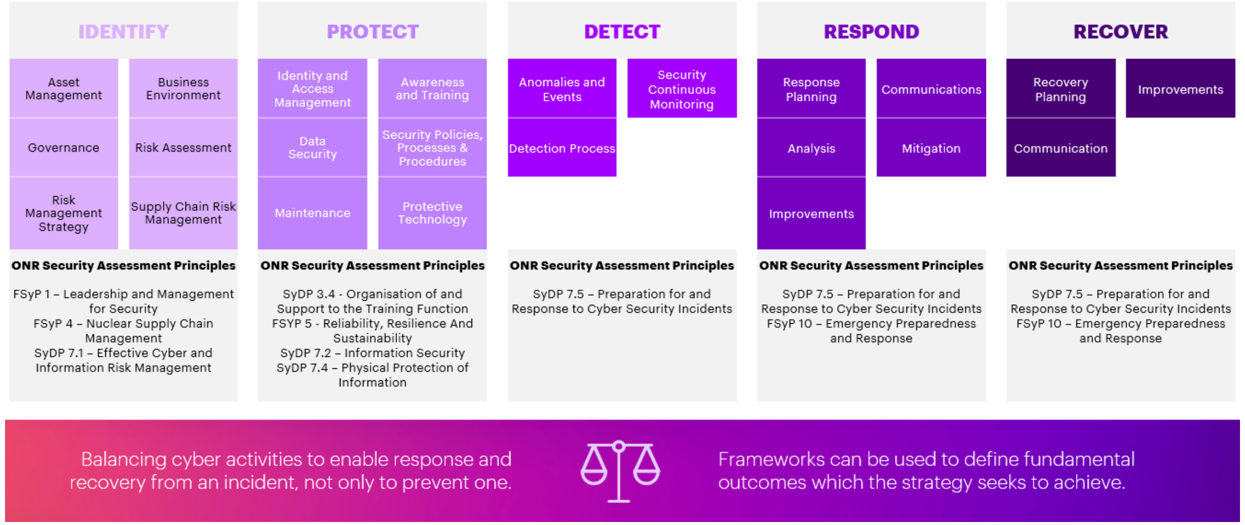
Respond – actions taken when a cyber security incident is detected, to contain the impact of the event.

Recover – resilience and restoration planning and activities for the timely recovery of capabilities or services impaired following a cyber security incident.

Frameworks can be used to define cyber resilience functions, with a collection of lower-level contributing cyber security and resilience outcomes. These are illustrated using the US National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), which is mapped to the ONR Security and Assessment Principles (SyAPs) in Figure 4. [9]

The ONR Fundamental Security Principle 7 (FSyP7), states dutyholders must implement and maintain effective cyber security and information assurance arrangements to protect Sensitive Nuclear Information (SNI) and technology. SyAPs are also outcome focused and used by ONR to assess dutyholder's security arrangements. [10]

The National Cyber Security Centre (NCSC) guidance, known as the Cyber Assessment Framework (CAF) has deliberate similarities with the NIST CSF. [11] Both the NIST CSF and NCSC CAF refer to relevant good practice, including ISO/IEC 27001/27002 standard series and IEC 62443 series for control systems or Operational Technology (OT).



IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management	Identity and Access Management Awareness and Training Data Security Security Policies, Processes & Procedures Maintenance Protective Technology	Anomalies and Events Security Continuous Monitoring Detection Process	Response Planning Communications Analysis Mitigation Improvements	Recovery Planning Improvements Communication
ONR Security Assessment Principles FSyP 1 – Leadership and Management for Security FSyP 4 – Nuclear Supply Chain Management SyDP 7.1 – Effective Cyber and Information Risk Management	**ONR Security Assessment Principles** SyDP 3.4 - Organisation of and Support to the Training Function FSYP 5 - Reliability, Resilience And Sustainability SyDP 7.2 – Information Security SyDP 7.4 – Physical Protection of Information	**ONR Security Assessment Principles** SyDP 7.5 – Preparation for and Response to Cyber Security Incidents	**ONR Security Assessment Principles** SyDP 7.5 – Preparation for and Response to Cyber Security Incidents FSyP 10 – Emergency Preparedness and Response	**ONR Security Assessment Principles** SyDP 7.5 – Preparation for and Response to Cyber Security Incidents FSyP 10 – Emergency Preparedness and Response

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.

Figure 4. Relevant good practice NIST CSF – cyber security frameworks can be used to define cyber resilience functions

The NIST CSF and NCSC CAF both provide a common language and mechanism to describe an organisation's current state and future target states. They also help to identify and prioritise improvements, measure progress and communicate cyber security risks.

[9] NIST Cybersecurity Framework: https://www.nist.gov/cyberframework
[10] ONR Cyber Security and Information Assurance: https://www.onr.org.uk/operational/tech_insp_guides/cns-insp-gd-7.1.pdf
[11] NCSC CAF guidance: https://www.ncsc.gov.uk/collection/caf

11. Security culture

Convergence has increased the need to manage cyber security. Embedding a proactive cyber security culture and mindset is essential to enabling the digital enterprise. A positive security culture will mitigate security risks where technology alone is insufficient. Human error remains the principal source of cyber security breaches, due to lack of awareness and suitable training. The senior leadership needs to define, demonstrate, and inspire a positive security culture and encourage collaboration.

Organisations should focus on the following areas to build a proactive cyber security culture:

- Strategic executive alignment is critical to build a cohesive ownership of cyber security across IT and OT and address potentially incompatible approaches to addressing cyber risk.
- Upskilling of IT & OT cyber security “joint taskforce” professionals with the right skills to enable and sustain cyber security across the organisation.
- Establishing incentives and disincentive policies to promote and enforce cyber resilient behaviours across the organisation.
- Implement continuous, interactive and human centred awareness and learning programme to build user alertness including new joiners and third parties
- Driven by data analytics, predictive models as opposed to traditional approaches to measure behavioural change against vulnerabilities.
- Leaders to lead by example and inspire their teams to demonstrate cyber resilient behaviours.

Clear expectations should be set for staff behaviour, and an acceptance that incidents will arise, with staff encouraged to report issues so they can be rectified swiftly, without threat of blame or criticism.

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

- Is there an open approach to assess security in no-blame manner?
- What level of training and awareness do employees have?
- How could employees or an insider cause an incident, intentionally or by accident?
- Does the culture enable cyber resilience to be used as a justification?

Heathrow Airport security data breach - 2017

An unencrypted USB memory stick was found by a member of the public on the pavement in West London and handed to the Mirror newspaper. Sensitive information included employee personal data and airport security measures that were protectively marked. The Information Commissioner’s Office imposed a £120,000 fine and stated "Data protection is a boardroom issue and it is imperative that businesses have the policies, procedures and training in place to minimise any vulnerabilities of the personal information that has been entrusted to them.” The ICO reported an absence of suitable policies and procedures for data security, with the incident exposing security culture and awareness issues. At the time, only two percent of the 6,500-strong workforce had received data protection training.

British Airways data breach - 2018

A compromise of the BA website and mobile app enabled the attacker to exfiltrated personal data of nearly 500,000 individuals. This exposed supply chain management and security culture issues with an employee not following appropriate policies and procedures. The ICO initially filed a Notice of Intent to fine £183 million under GDPR. This was reduced to £20 million having taken the economic impact of Covid-19 into account. However, it is still the largest penalty issued by the ICO.

12. What about your strategy?

Consider the following questions:

- 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; information systems, control systems, safety systems, security systems, building management systems etc.?
- 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 and does it align with the 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 then 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 out 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 cyber security (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 Cyber security 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

Copyright 2022 Accenture. All rights reserved. Accenture and its logo are registered trademarks of Accenture.