Enhancing Civil Nuclear Cyber Security

ONR and Accenture deliver board-level cyber security briefings to UK Dutyholders

By **Richard Piggin**, Accenture

SUMMARY

- The board-level briefings are key to delivering ONR's mission to protect society by securing safe nuclear operations.
- The briefings reinforce the importance of implementing effective cyber security strategies that cover the entire operating environment.
- The board and senior-level leadership are ultimately responsible for cyber risk and resilience, this accountability also carries individual liability.
- Accenture provided a cross-sector perspective to protecting critical national infrastructure (CNI).
- Human factors continue to be the principal cause of security breaches. A positive security culture will mitigate security risks where technology alone is insufficient.

1. INTRODUCTION

In May 2022, the Department for Energy Security & Net Zero published the 2022 Civil Nuclear Cyber Security Strategy [1]. It builds upon the developments made in the sector since the initial strategy was published in 2017, which focused upon ensuring that the civil nuclear sector could defend against, recover from, and be resilient to evolving cyber threats (Figures 1, 2).

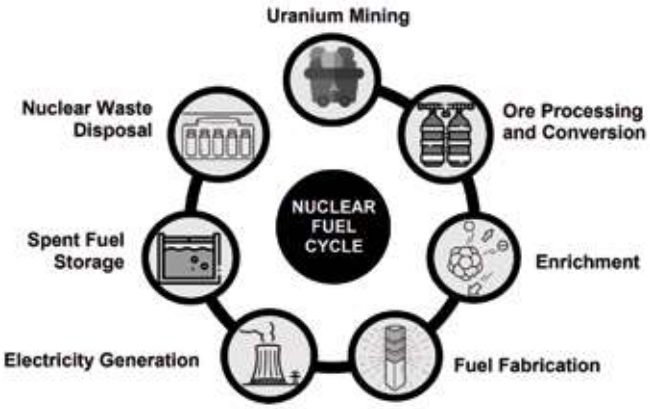

FIGURE 1: Overview of the Nuclear Fuel Cycle - Civil Nuclear Cyber Security Strategy 2022 [1]

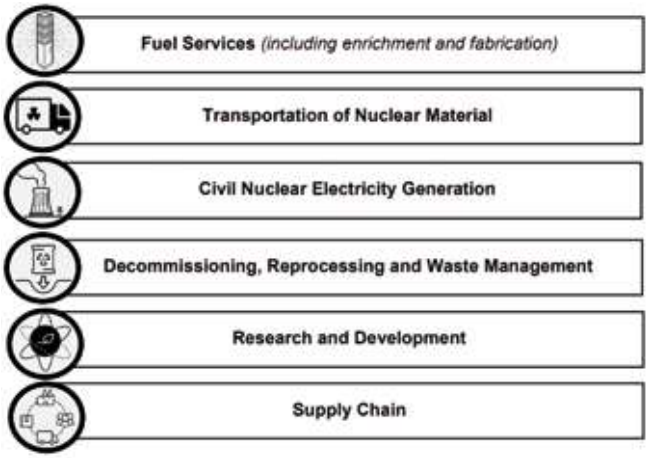

FIGURE 2: Civil Nuclear Sub-Sectors - Civil Nuclear Cyber Security Strategy 2022 [1]

This necessitates the protection of generating facilities, legacy facilities, new build projects and supply chains for civil nuclear from cyber attacks that could compromise Sensitive Nuclear Information, disrupt electricity supply, damage facilities, delay hazard and risk reduction, and risk radiological consequences to workers, the public or the environment. The World Economic Forum Global Risks Report 2023 highlights the immediacy, as "widespread cybercrime and cyber insecurity" is a new top 10 ranked risk for the next decade, with more aggressive and sophisticated attacks targeting greater widespread exposure [2].

The 2017 strategy defined roles and responsibilities, along with commitments and expectations for HM Government, UK Civil Nuclear Duty holders (responsible persons on nuclear sites subject to security regulation), the civil nuclear supply chain, and

Regulators, including the Office for Nuclear Regulation and the Information Commissioner's Office. The 2022 strategy continues the cross-sector partnership, being developed with UK civil nuclear organisations, the Office for Nuclear Regulation and the National Cyber Security Centre. The strategy outlines how the sector will deliver four key objectives by 2026:

- Appropriately prioritise cyber security as part of a holistic risk management approach, underpinned by a common risk understanding, and outcome-focused regulation.
- Take proactive action to mitigate cyber risks in the face of evolving threats, legacy challenges and adoption of new technologies.
- Enhance resilience by preparing for, and responding collaboratively to cyber incidents, minimising impacts and recovery time.
- Collaborate to increase cyber maturity, developing cyber skills and promoting a positive security culture.

The Office for Nuclear Regulation (ONR) undertook a series of board-level briefings, in partnership with Accenture, across the UK civil nuclear sector in early 2023. The briefings covered the nuclear fuel cycle including fuel enrichment and manufacture, generation, and decommissioning. These briefings highlighted the importance of embedding an effective strategy, supported by strong leadership, governance, risk management and a positive security culture [3].

Paul Shanes CSyP FSyI FBCS, ONR's Head of Cyber Security Regulation, provided additional context to the author:

"The briefings demonstrate ONR's enabling approach to regulation. They provided an opportunity to communicate recent updates to the UK national and civil nuclear cyber security strategies whilst leveraging Accenture's knowledge of relevant good practice from other critical national infrastructure sectors. This work supports our role as the UK's independent nuclear regulator and is key to delivering our mission to protect society by securing safe nuclear operations." [4]

The paper highlights relevant good practice, relating it to the requirements of the civil nuclear sector and is based upon the materials produced to support executive briefings and has wide applicability to the leadership and governance of cyber security in other organisations.

ONR has since undertaken a series of inspections to assess the cyber security leadership and risk management arrangements. Initial findings suggest improvements are necessary from some dutyholder leadership teams; in defining their cyber security strategies and ensuring they have the skills to understand and manage specific cyber security risks [5].

2. AN UNCOMMON UNDERSTANDING OF CYBER SECURITY?

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 [6]. This is likely to be a problem for organisations, 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 [7].

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 who set the strategy are ultimately responsible and are increasingly being held accountable for cyber resilience [8].

3. 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 minimise 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.

3.1 Case study 1: 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. Maersk intends to use cyber security to create a competitive advantage and treat these attacks as business risks, not technology concerns.

Lessons identified included transparency, acknowledged as the principal lesson learnt, with support from clients and partners due to openness, and increased share value following the incident. Maersk recognised that most organisations are unlikely to be able to prevent

a nation-state attack, therefore the focus needs to be on recovery and prevention of extinction events. The extinction event approach uses consequence-driven impact analysis, assuming the worst-case incident. This contrasts with traditional probability methods, which seek to identify both specific scenarios and their likelihood of occurrence [9, 10].

4. NUCLEAR SAFETY AND CYBER SECURITY

Nuclear security is not a subset of nuclear safety, and so delivering effective nuclear safety will not necessarily also result in effective nuclear security. Both are interconnected, yet safety and security engineering disciplines are independent domains. It cannot be assumed that obscure, bespoke systems or air gaps can prevent attacks. Similar challenges have been observed in rail safety, with security guidance for safety engineers and managers published by the Centre for the Protection of National Infrastructure (now the National Protective Security Authority). Convergence has been driven through common technologies, platforms and networking, where safe operation of complex systems requires appropriate security. The two disciplines may also conflict, creating new functionality, vulnerabilities and hazards that may require additional mitigations to reduce safety and security risk in the provision of critical services [11, 12].

Widely published incidents across industrial sectors have demonstrated siloed approaches, focused on IT security, and omitting Operational Technology (OT) in particular, which expose potentially vulnerable systems. The IET Code of Practice: Cyber Security and Safety addresses this convergence and the necessity to integrate safety assurance and cyber security [13]. The publication also considers where there may be tensions between safety and security requirements, such as creating security-induced safety hazards (e.g. inability to logon and access a safety system using shared accounts), and issues with estimating static safety risks, whilst considering the rapidly changing security environment, with dynamic threats and emerging vulnerabilities.

4.1 Case study 2: 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 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.

Lessons identified included the segmentation/isolation of critical systems, network monitoring and the necessity to protect engineering workstations used to make program and configuration changes. Clearly defined accountability/responsibility for specific domains or environments to ensure control measure implementation and validation was also identified [14-19].

5. 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 needs 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 help to 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 3).

6. SECURITY STRATEGY PRINCIPLES

When assisting organisations in the implementation of their cyber resilience programmes, the Accenture approach uses the following guiding principles:

- **Business-centric.** Ensure cyber resilience is driven by business and organisational priorities. Accenture 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 or a technology issue. It is an operating environment with risk, in the same way operations occur in a physical environment, where physical risks manifest.
- **Exposure focused.** The need to focus beyond compliance requirements to address actual exposure to be cyber resilient.
- **Extended ecosystem coverage.** Be responsible for the extended ecosystem, 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 [20-22].
- **Agile.** 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. The security strategy should be technology agnostic, focusing on the desired outcomes, whilst providing flexibility to keep pace with technological change.

The cyber resilience strategy needs to align with the business strategy and its timeframe. Shorter than 2-3 years is fundamentally operational planning, which is not strategic.

7. GOVERNANCE AND LEADERSHIP

The board and senior-level leadership are ultimately responsible for an organisation's cyber risk and resilience, a notion that is front and centre in ONR's outcome-focused regulatory approach. 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

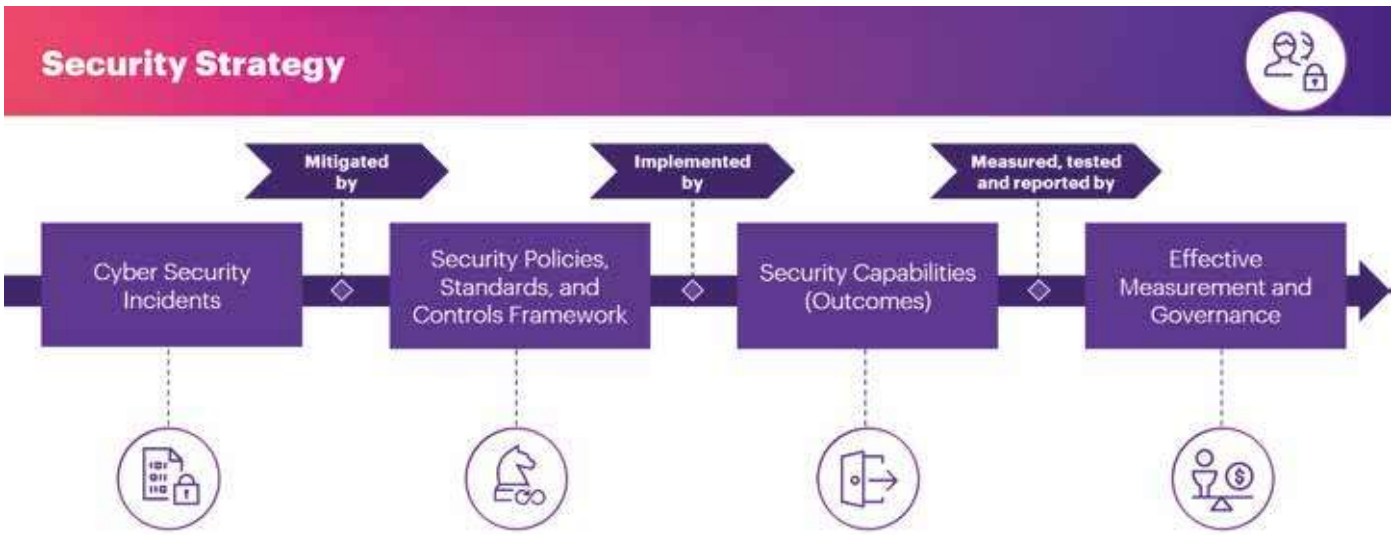

FIGURE 3: Cyber security strategy implementation

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. Accenture research revealed cyber security stimulates enterprise reinvention, driving business resilience, with a stronger alignment between cyber security practices and the business strategy achieving better outcomes (Figure 3) [23, 24].

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 (CAF) 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 [25, 26].

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.

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.

Accenture research identified four levels of cyber resilience (Figure 4). 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 [23].

8. 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

FIGURE 4: Four levels of cyber resilience - Accenture State of Cybersecurity Resilience 2021 [23]

MITRE ATT&CK® ENTERPRISE IMPACT
Account Access Removal
Data Destruction
Data Encryption for Impact
Data Manipulation
Defacement
Disk Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Resource Hijacking
Service Stop
System Shutdown/Reboot

TABLE 1: MITRE ATT&CK® Enterprise Impact
Source: https://attack.mitre.org/matrices/enterprise/

MITRE ATT&CK® ICS IMPACT
Damage to Property
Denial of Control
Denial of View
Loss of Availability
Loss of Control
Loss of Productivity and Revenue
Loss of Protection
Loss of Safety
Loss of View
Manipulation of Control
Manipulation of View
Theft of Operational Information

TABLE 2: MITRE ATT&CK® ICS Impact
Source: https://attack.mitre.org/matrices/ics/

should regularly ensure organisational risk tolerance is consistent with the organisational risk appetite. An example of risk identification and assessment is shown in Figure 5.

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 The differing impacts are illustrated in Tables 1 and 2. The recently revised NIST SP 800-82r3 Guide to Operational Technology Security provides comprehensive guidance, whilst introducing readers to OT's unique characteristics [27, 28].

Organisations then need to put measures in place to specifically defend against theses 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 a number of roles relative to a 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 the security strategy and business objectives together and is used to operationalise the governance programme to monitor and support cybersecurity initiatives. The implementation should provide end-to-end traceability of cyber security, business risk and threat management through defined governance, policy and control monitoring.

FIGURE 5: Risk management - likelihood and impact examples

9. CYBER 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, is 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 6 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 permit 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 [29, 30].

Fundamental Security Principle 7 (FSyP7) within ONR's SyAPs, states that 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 [20].

The National Cyber Security Centre (NCSC) guidance, known as the Cyber Assessment Framework (CAF) has deliberate similarities with the NIST CSF. 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).

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. The NIST framework developments currently in the CSF 2.0 draft are especially relevant, including the addition of the Govern function, establish, and monitor cybersecurity risk management, strategy and policy. There is also increased emphasis upon supply chain management and secure software development. Final publication is anticipated in early 2024 [31].

9.1 Case study 3: Colonial Pipeline disruption - 2021

The DarkSide ransomware attack impacted IT systems, however, OT systems controlling the pipeline were shut down 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. Most of the $5 million ransom was recovered by the FBI ($2.4m after bitcoin fluctuation) from the gang's affiliate which led to the collapse of the DarkSide brand. The incident led to operational disruption with an international impact upon aviation, with panic buying of petroleum and lawsuits.

Lessons identified included account management governance failings, where a vulnerable virtual private network profile was not intended to be in use, facilitated initial the gang access. OT network protection, (including IT & OT segmentation) can atrophy over time creating hyper-connectivity due to cloud resources, system integrators, original equipment vendors, personnel and enterprise IT. However, some organisations' IT and OT systems have tightly coupled dependencies, where segregation can be difficult to implement. Protection of the crown jewels is paramount, along with gaining visibility into OT networks with traffic monitoring and addressing insecure connectivity. Ensuring critical OT systems backups (known as lifeboats to protect against ransomware encryption) and incident response plans are in place and exercised is essential given the increasing threat of ransomware.

DarkSide, the Organised Criminal Group responsible for the ransomware, offered a menu of services to their affiliates: Triple or quadruple extortion, in addition to file encryption, including data leaks and distributed denial-of-service (DDoS) attacks. Services also offered the collection of senior executive information for blackmail. More recently, criminal groups have preferred data theft and extortion, purporting to follow a moral code, and not sought to encrypt CNI [20, 32-37].

10. SECURITY CULTURE

Convergence has increased the need to manage cyber security and develop a security-informed approach to safety, where security considerations are integrated into the management of safety risks. Security threats that impact safety must be considered to ensure a security-minded engineering approach, which addresses security threats and vulnerabilities throughout the lifecycle.

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 factors remain 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 across disciplines [38].

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.

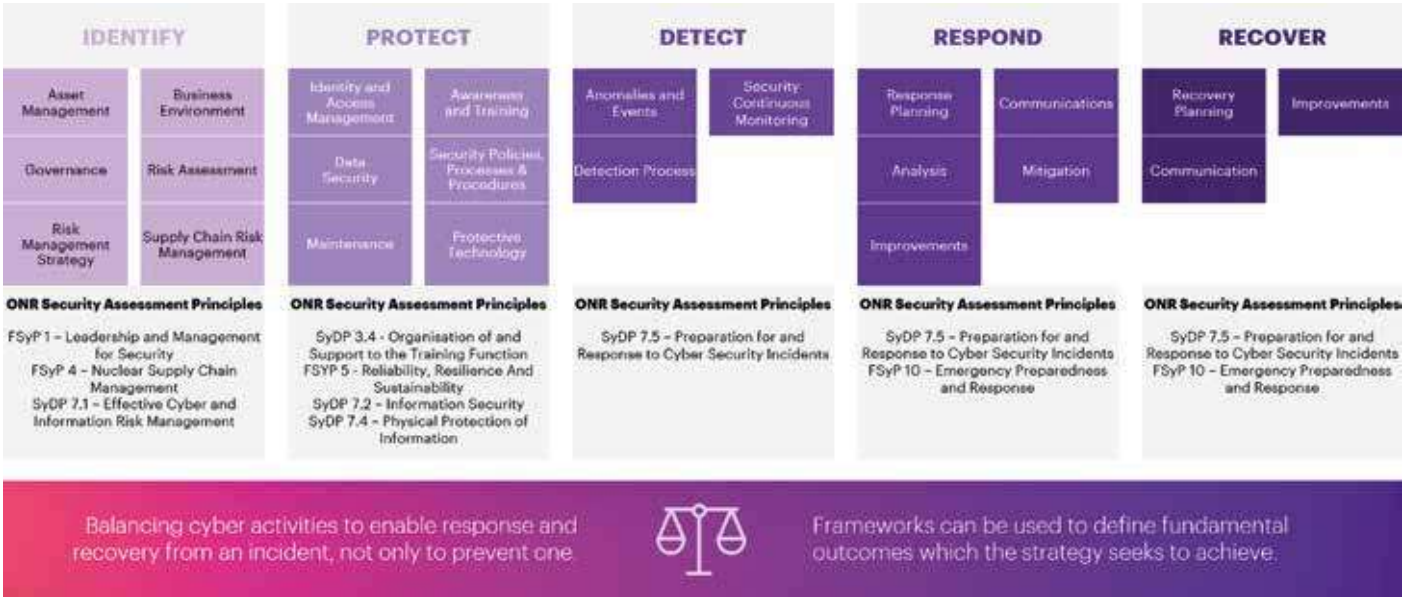

FIGURE 6: Relevant good practice: NIST CSF mapped to ONR's SyAPs

- 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 a 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?
- Do key stakeholders have a thorough understanding of the insider threat programme and the risks faced by the organisation [39]?
- Does the culture enable cyber resilience to be used as a justification?

11. CONCLUDING REMARKS

11.1 A security-minded approach for the whole cyber environment

The strategy scope needs to cover the entire cyber environment, including information systems, control systems, safety systems, security systems, building management systems and the Internet of Things (IoT Sensors/Actuators). An integrated approach must incorporate security into safety cases to address security issues, technology convergence and deal with the potential tensions between safety and security that may arise. This necessitates creating a common understanding across safety and security disciplines, emphasising the importance of leadership and a positive security culture. Leadership teams have a legal responsibility to manage safety and security risks, and shortcomings will have inevitable consequences for accountable individuals.

ACKNOWLEDGEMENTS

It is acknowledged that the briefing materials this article is based upon were commissioned by the Office for Nuclear Regulation in support of the 2022 Civil Nuclear Cyber Security Strategy.

ACRONYMS

BEIS	Department for Business, Energy & Industrial Strategy
CAF	Cyber Assessment Framework
CISA	Cybersecurity & Infrastructure Security Agency
CNI	Critical National Infrastructure
CPNI	Centre for the Protection of National Infrastructure (responsibilities now with NPSA)
CSF	Cybersecurity Framework
CyBOK	Cyber Security Body of Knowledge
DESNZ	Department for Energy Security & Net Zero
DOE	US Department of Energy
FBI	US Federal Bureau of Investigations
FCDO	Foreign, Commonwealth & Development Office
FSyP	Fundamental Security Principle
HMG	His Majesty's Government
ICS	Industrial Control Systems
IET	Institution of Engineering Technology
IoT	Internet of Things
IT	Information Technology
KPI	Key Performance Indicators
NCSC	National Cyber Security Centre
NPSA	National Protective Security Authority
NIST	US National Institute of Standards and Technology
ONR	Office for Nuclear Regulation
OT	Operational Technology
WEF	World Economic Forum
SyAPs	Security and Assessment Principles

REFERENCES

[1] DESNZ (formerly BEIS), Civil Nuclear Cyber Security Strategy 2022, 2022 https://www.gov.uk/government/publications/civil-nuclear-cyber-security-strategy-2022

[2] WEF, Global Risks Report 2023, 2023, p. 42 https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

[3] ONR, Chief Nuclear Inspector's Annual Report on Great Britain's Nuclear Industry 2022/23, 2023, p. 12 https://www.onr.org.uk/documents/2023/cni-annual-report-2023.pdf

[4] Piggin, R. Leading cyber security in the UK civil nuclear sector, ITNOW, Volume 65, Issue 4, Winter 2023 https://doi.org/10.1093/itnow/bwad129

[5] ONR, Chief Nuclear Inspector's Annual Report on Great Britain's Nuclear Industry 2022/23, 2023, pp 12-13 https://www.onr.org.uk/documents/2023/cni-annual-report-2023.pdf

[6] NCSC, Cyber Security Body Of Knowledge (CyBOK), 2021 https://www.cybok.org/media/downloads/Introduction_v1.1.0.pdf

[7] HMG, National Cyber Strategy 2022, 2022 https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

[8] WEF, Principles for Board Governance of Cyber Risk, 2021 https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk

[9] The Register, IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation blitz, 2018 https://www.theregister.com/2018/01/25/after_notpetya_maersk_replaced_everything/

[10] CSO, Rebuilding after NotPetya: How Maersk moved forward, 2019 https://www.csoonline.com/article/567845/rebuilding-after-notpetya-how-maersk-moved-forward.html

[11] CPNI, Rail Code of Practice For Security-Informed Safety, 2022 https://www.npsa.gov.uk/system/files/documents/rail-code-practice-security-informed-safety.pdf

[12] P. Litherland ; R. Orr ; R. Piggin, Cyber security of operational technology: understanding differences and achieving balance between nuclear safety and nuclear security, 11th International Conference on System Safety and Cyber-Security, 2016 https://digital-library.theiet.org/content/conferences/10.1049/cp.2016.0856

[13] IET, Code of Practice: Cyber Security and Safety, 2021 https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/

[14] Wired, Unprecedented Malware Targets Industrial Safety Systems in the Middle East, 2017 https://www.wired.com/story/triton-malware-targets-industrial-safety-systems-in-the-middle-east/

[15] Dragos, TRISIS Malware: Analysis of Safety System Targeted Malware, 2017 https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

[16] Wired, Menacing Malware Shows the Dangers of Industrial System Sabotage, 2018 https://www.wired.com/story/triton-malware-dangers-industrial-system-sabotage/

[17] Darkreading, Triton/Trisis Attack Was More Widespread Than Publicly Known, 2019 https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known

[18] US Department of Justice, United States v. Gladkikh, 1:21-cr-00442 (D.D.C. June 29, 2021) https://www.justice.gov/d9/press-releases/attachments/2022/03/24/dc_gladkikh_0.pdf

[19] US Department of Justice, Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide, 2022 https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical

[20] US DOE, Colonial Pipeline Cyber Incident, 2021 https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

[21] FCDO, Russia: UK exposes Russian involvement in SolarWinds cyber compromise, 2021 https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise

[22] Wired, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, 2018 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

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

[24] Accenture, The Cyber-Resilient CEO, 2003 https://www.accenture.com/content/dam/accenture/final/accenture-com/document-2/Accenture-The-Cyber-Resilient-CEO-Final.pdf

[25] ONR, Security Assessment Principles (SyAPs) Version 1, 2022 https://www.onr.org.uk/syaps/

[26] NCSC, CAF guidance version 3.1, 2022 https://www.ncsc.gov.uk/collection/caf

[27] MITRE, ATT&CK® Matrix for ICS, 2023 https://attack.mitre.org/matrices/ics/

[28] NIST, NIST SP 800-82r3 Guide to Operational Technology (OT) Security, 2023 https://doi.org/10.6028/NIST.SP.800-82r3

[29] NIST, Cybersecurity Framework, 2023 https://www.nist.gov/cyberframework

[30] NIST, Public Draft: The NIST Cybersecurity Framework 2.0, 2023 https://doi.org/10.6028/NIST.CSWP.29.ipd

[31] ONR, Security Assessment Principles for the Civil Nuclear Industry. 2022 Edition Version 1, 2022, p. 22 https://www.onr.org.uk/syaps/security-assessment-principles.pdf

[32] Accenture, Securing the T&D network of the future - The path forward: operational security in utility transmission & distribution, 2022, pp. 12-13

[33] WEF, Global Risks Report 2022, 2022, pp. 47-48 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

[34] Dragos, Recommendations Following the Colonial Pipeline Cyber Attack, 2021 https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/

[35] Blount, J., Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline Company. Senate Committee on Homeland Security & Governmental Affairs, 8 June 2021, p. 4 https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Blount-2021-06-08.pdf

[36] NCSC, NCA, Ransomware, extortion and the cyber crime ecosystem, 2023 p. 8 https://www.ncsc.gov.uk/pdfs/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem.pdf

[37] CISA, #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability, 2023 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

[38] WEF, Global Risks Report 2022, 2022, p. 52 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

[39] NPSA, Reducing Insider Risk, 2023 https://www.npsa.gov.uk/reducing-insider-risk

DR RICHARD PIGGIN, ENGD CENG MIET MBCS

Richard has an EngD from the University of Warwick, and a Cyberspace Operations PgDip from Cranfield University. He was a co-instigator/contributor to the IET Code of Practice: Cyber Security and Safety. Linkedin.com/in/richardpiggin/