Integration of cyber resilience within energy projects forming the UK's critical national infrastructure [1]

Dr R J Chapman[2]

Introduction

This paper is a development of the themes described in the previous PM World Journal Featured Paper titled "Exposure of the UK's critical national infrastructure to cyber-attacks and ransom demands" published in February 2024[3]. Relevant aspects of the previous paper are drawn on and included here to aid establishing the background to the subject. Further research has shown that the spotlight needs to be kept on the integration of cyber resilience within new Critical National Infrastructure (CNI) projects. Projects need to be made aware of the scale, source and nature of cyber threats; the potential impact of cyber incidents; and hence the necessity to embed cyber resilience throughout each phase of the lifecycle of new CNI projects. However, navigating the literature, guidance and legislation is a very considerable challenge. The goal of this paper is to describe the cyber landscape; the requirements for embedding cyber security within energy projects; and an approach to resilience given their significance to society; and the economy.

The nature of the problem

According to the Cabinet Office, Cyber-attacks against the UK Government and CNI operators nationally have "grown in sophistication, complexity and severity"[4]. In addition, due to the limited success of current cyber resilience initiatives, efforts have "not yet fundamentally altered the risk calculus of attackers who continue to successfully target the UK and its interests[5]". Taking a broad perspective, malign actors have a range of motives for instigating cyber-attacks against the UK, such as the theft of intellectual property; criminal, commercial, financial and political gain; and sabotage and disruption through disinformation. Unfortunately, attackers have developed capabilities that evade mitigations and increasingly sophisticated cyber tools. Related enablers have been commoditised in a growing cyber 'industry', and the lowering of barriers to entry for all types of malicious actors. A further factor is that threat actors may well take an industry sector view when developing their attacks whilst CNI organisations will naturally be focussed on their own business scope, which may lead to a suboptimal approach to cyber security risk management. In addition, rewards are increasing as the ability of actors to steal and encrypt valuable data and extort ransomware payments continues to grow, disrupting businesses and key public services.

International perception of exposure to cyber attacks

There is evidence from around the world that critical infrastructure is subject to cybercrime. For instance, the World Economic Forum Global Risks Perception Survey 2022-2023 included

cyberattacks on critical infrastructure among their top risks for 2023 with the greatest potential impact on a global scale. The survey brought together insights from over 1,200 specialists from across the World Economic Forum's diverse network. In addition, the World Economic Forum's Insight Report entitled "Global Cybersecurity Outlook 2023" found that 91% of all respondents considered that a far-reaching, catastrophic cyber event is at least somewhat likely in the next two years.

The perception of exposure to cyber-attacks is no doubt due to the global reach of relentless media reports on cyberattacks. For instance, in 2019 the Nuclear Power Corporation of India Limited confirmed the Kudankulam nuclear power plant had been hacked using malware[6]. In May 2021, a ransomware attack against the Irish Health Service Executive (HSE) disrupted Irish healthcare IT networks and hospitals for over 10 days, causing significant consequences to patients and their families. Some stolen patient data was also published online. The HSE, which provides health and social care services in Ireland, shut down national and regional networks the same day to contain the incident. Malicious cyber activity was also detected on the Irish Department of Health's (DoH) network. In addition, the attack had an impact on Northern Ireland, affecting the ability to access data held by HSE for some cross-border patient services.

In the same year the US fuel pipeline operator Colonial Pipeline, which supplied almost half of the East Coast's fuel, shut down its network following a cyberattack[7]. On April 17, 2022, multiple institutions of the government of Costa Rica, (estimated to be over 30), were targeted by a ransomware attack. The government had to shut multiple computer systems used to declare taxes and for the control and management of imports and exports, causing enormous losses. It is reported that Costa Rica required technical assistance from the United States as well as Israel, Spain and Microsoft to deal with the cyberattack.

On 31 October 2023, the British Library confirmed that a cyberattack had led to a leak of employee data. The Rhysida ransomware group claimed responsibility for the attack, threatening to auction off the stolen data. The cyber gang set the ransom demand at 20 Bitcoin (£596,459). The library refused to pay the ransom. The Financial Times reported that the library would be forced to drain 40 per cent of its reserves to recover from the attack[8]. Of significance is that on 15 November the FBI and the US Cybersecurity and Infrastructure Security Agency issued a joint statement[9] saying "Threat actors leveraging Rhysida ransomware are known to impact 'targets of opportunity', including victims in the education, healthcare, manufacturing, information technology, and government sectors".

On 7th May 2024 a BBC News article reported that a ransomware group which had targeted the NHS Dumfries and Galloway health board earlier in the year, had now published a large volume of patient data on the dark web[10]. The health board's chief executive Julie White said the hack was unprecedented, advised the number of people affected could be in the thousands and described the data release as an "utterly abhorrent criminal act".

The global nature of the threat was reinforced by the press release issued by the Office of Public Affairs (within the U.S. Department of Justice) during January 2023. It announced the FBI had

infiltrated the Hive Network, preventing over $130 Million in ransom demands. It had been discovered that since June 2021 the Hive ransomware group had targeted more than 1,500 victims in over 80 countries, including critical infrastructure, hospitals, schools and financial firms. The U.S. Department of Justice acknowledged the support of the law enforcement authorities of eight countries including the United Kingdom's National Crime Agency.

The UK Government's informative and well written National Cyber Strategy succinctly articulates the international nature of the exposure to cyber-attacks and their multiple characteristics which are outside of the Government's control: "*Cyberspace also transcends national borders. Technology supply chains and critical dependencies are increasingly global, cyber criminals and state-based actors operate from around the world, powerful technology companies export products and set their standards, and the rules and norms governing cyberspace and the internet are decided in international fora. Cyberspace is also continually evolving as technology and the ways people use it change, requiring us to adopt an agile and responsive approach*"[11].

The importance of the UK's Critical National Infrastructure

The very fabric of our society is dependent on our CNI. It is by definition, the infrastructure that the country relies on most. It underpins our daily lives from the moment we wake up in the morning to the time we go to bed. The constituents of CNI are the most important systems in the UK today. They include providing safe drinking water, health services, transport, electricity and keeping the country connected to the internet. Disruptions to the power grid due to cyber-attacks could lead to widespread blackouts, affecting everything from hospitals to train services, Smart motorway signs[12], lighting, traffic lights and emergency services.

It is considered that large elements of the UK's critical national infrastructure (CNI) remain vulnerable to ransomware, particularly in sectors still relying on legacy IT systems. The scale of a major attack could potentially be enormous. The UK Government's Joint Committee for National Security (JCNSS) report referenced modelling undertaken by the Office for Budget Responsibility (OBR) which found that a major UK cyber-attack (which might take the form of a ransomware attack) "*could result in a shock to the economy of 1.6% of GDP, adding £29 billion to Government borrowing. It based its findings on a scenario in which a cyber-attack causes severe disruption to the electricity grid in the South-East of the UK, including London, causing 'rolling blackouts' for three weeks*".

What is Critical National Infrastructure

According to the UK Government's National Protective Security Authority (NPSA), the country's critical national infrastructure relates to those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. In the UK, the 13 national infrastructure sectors are listed in **Table 1** below.

Chemicals	Civil Nuclear	Communications	Defence	Emergency Services
Energy	Finance	Food	Government	Health
Space	Transport	Water		

Table 1: 13 national infrastructure sectors.

The UK's CNI has become increasingly interconnected and interdependent[13], making it harder for government departments to both comprehend and manage the threats faced by the UK. A joint initiative by the Cabinet Office, the National Cyber Security Centre (NCSC) and the National Protective Security Authority (NPSA) has developed a new methodology to collect data on this 'interconnectedness', called the *Criticalities Process* and is developing a new tool to visualise and interrogate the data produced called the *CNI Knowledge Base*. The UK Government's National Risk Register in particular highlights the connection between the UK's critical electricity system and other utilities, see **Box1** below. This 'interconnectedness' can also be international. An example is that German wind farm operation is dependent on satellites operated by the United States.

Box 1

UK Government's National Risk Register (NRR), Cyber-attack on electricity infrastructure
https://assets.publishing.service.gov.uk/media/64ca1dfe19f5622669f3c1b1/2023_NATIONAL_RISK_REGISTER_NRR.pdf

The interconnectedness is also described in the UK Government's National Risk Register (NRR) which is the external version of the National Security Risk Assessment (NSRA), the government's assessment of the most serious risks facing the UK. To ensure the UK is prepared for a broad range of scenarios, the NRR sets out a 'reasonable worst-case scenario' for each risk. These scenarios are not a prediction of what is most likely to happen, instead they represent the worst plausible manifestation of that particular risk (once highly unlikely variations have been discounted). The goal being to enable relevant bodies to undertake proportionate planning. The reasonable worst-case scenario for a malicious cyber-attack on a critical electricity system is where it leads to a total failure of the National Electricity Transmission System (NETS). The NRR states "a failure of this system has the potential to severely disrupt all other critical systems, resulting in greater consequences than typical utilities failures. All consumers without back-up generators would lose their mains electricity supply instantaneously and without warning. A nationwide loss of power would result in secondary impact across critical utilities networks (including mobile and internet telecommunications, water, sewage, fuel and gas). This would cause significant and widespread disruption to public services provisions, businesses and households, as well as loss of life".

UK Government awareness

The UK Government has reported it is evident there is a persistent and elevated threat to the cyber resilience of the country's CNI. As a consequence, it considers cyber security needs to be at the forefront of all decisions affecting both CNI and wider cyber-physical systems. This is reinforced by the NCSC's Annual Review 2023 which stated, "it is highly likely the cyber threat to UK CNI has heightened in the last year"[14]. In his Ministerial Foreword to the review, the Deputy Prime Minister, Oliver Dowden, stated "we live in a dangerous, volatile world. The new front line is online". In addition, he made the following three key points: the methods of cyber-attack are proliferating, the number of hostile state and non-state actors with the tools available to

implement an attack is growing and the ways in which these countries, organisations and individuals can inflict harm is increasing.

The UK government's report issued by the JCNSS[15,16] on 13 December 2023 made it abundantly apparent that the government is very aware of potential cyber threats. It describes the exposure of the country's CNI to ransomware attacks. It makes for a sobering read. Its key message is stark: "*There is a high risk that the Government will face a catastrophic ransomware attack at any moment, and that its planning will be found lacking. If the UK is to avoid being held hostage to fortune, it is vital that ransomware becomes a more pressing political priority, and that more resources are devoted to tackling this pernicious threat to the UK's national security".* Ransomware is considered the number one cyber threat to the nation with the ability to "*bring the UK to a standstill" [17].* Given events that have occurred in Germany and the U.S., an attack could potentially affect a large section of the population all at once. It is especially relevant to all those engaged in new critical infrastructure projects.

Cyber-attacks on the UK's CNI

The pervasiveness of the threat of ransomware attacks was highlighted at a CyberUK conference held in Belfast in April when Oliver Dowden advised attendees Russian hackers were seeking "to disrupt or destroy" parts of the UK's critical national infrastructure[18]. In October 2023 the government placed a post on the internet[19], which drew attention to the UK being the third most targeted country in the world for cyber-attacks, after the US and Ukraine.

In April 2023 Dr Marsha Quallo-Wright, National Cyber Security Centre (NCSC) Deputy Director for CNI, said: "It has become clear that certain state-aligned groups have the intent to cause damage to CNI organisations, and it is important that the sector is aware of this". In May 2023 Paul Chichester, director of operations at the NCSC stressed that it was vital that operators of UK CNI, (including energy and telecommunications networks), prevent Chinese state-sponsored hackers from accessing and hiding on their systems[20]. The warning came after it emerged that a Chinese hacking group known as Volt Typhoon had targeted a US military outpost in the Pacific Ocean. The intelligence group labelled "Five Eyes" composed of the US, the UK, Australia, Canada and New Zealand issued a joint notice describing the nature of the Volt Typhoon threat and how to deal with it. Of particular significance to energy supply is the nuclear sector. In 2023 the UK's Office for Nuclear Regulation (ONR) singled out the French energy company EDF, a provider of CNI, and placed it under significantly enhanced regulatory attention for cyber security[21]. This arose after the operator failed to comply with commitments it had made in March 2023 to enhance its cyber security provision and provide the ONR with a comprehensive and fully resourced cyber security improvement plan. EDF operates a significant component of the UK's nuclear power infrastructure, including facilities in County Durham, Lancashire, Suffolk and Torness.

New CNI projects

As highlighted in the previous paper, those working on a day-to-day basis on CNI projects may be unaware of the likelihood and potential impact of cyber-attacks on the nation's CNI or how critical it would be to UK citizens, the economy and national security. In addition, they may be unfamiliar with how UK foreign policy has been received overseas and whether it has aggravated foreign powers to the point where they have threatened or are currently sponsoring attacks on elements of our CNI. Clearly the coming together of evolving international relations and improvements in digital technology is both a global problem but also a potentially more dangerous one[22]. Walker[23] highlighted that given the complexity of projects, more and more specialist disciplines have emerged (and continue to do so) which produces a high level of differentiation. Hence for successful projects, strong integration of these specialisms is required. This is true for the integration of information, technology and cyber security with project design and how completed infrastructure will interface with the internet.

A moving picture

As highlighted by the World Energy Council (WEC) the transforming energy sector requires new, agile risk management approaches to match its evolving risk profile and ensure it continues to be effective and reliable given the critical role it plays in every country's infrastructure[24]. However, as the energy sector becomes more sophisticated and interconnected it also becomes more vulnerable to disruption from cyber-attacks. The WEC has drawn attention to the fact that each connected pathway to a nation's electric, oil and natural gas infrastructure (as well as each connected devise on an energy system) presents a new route for maligned cyber actors to cause damage to or destruction of CNI. "The global expansion of cyberspace is changing the way we live, work and communicate, and transforming the critical systems we rely on in areas such as finance, energy, food distribution, healthcare and transport. In short, cyberspace is now integral to our future security and prosperity"[25].

The JCNSS report mentioned above explains that the nature of cyberattacks has been evolving. For instance, the evidence submitted to the Joint Committee by BAE systems described a rise in criminal actors adopting the Ransomware-as-a-Service (RaaS) model, featuring administrators (sometimes called developers), and affiliates where various elements of ransomware operations are increasingly outsourced. In essence RaaS is a subscription-based model where the developers or administrators develop a ransomware strain and create an easy-to-use interface with which to operate it and then recruit affiliates to deploy the ransomware against victims. Affiliates who have identified targets and deployed this readymade malicious software attacking victims have subsequently earned a percentage of each successful ransom payment. Typically, after a victim pays, affiliates and administrators split the ransom 80/20.

The changing scale of the problem is illustrated by the data collected by the AV-Test institute, an independent IT security research institute based in Magdeburg, Germany (see **Figure 1**). The institute declares that it registers over 450,000 new malicious programs (Malware) and

potentially unwanted applications (PUA) every day. They are examined and classified according to their characteristics and saved. The graph below shows the numbers accumulated since 1984. Malware is an umbrella term for a range of online threats, including viruses, spyware, adware, ransomware, and other types of harmful software. A computer virus is simply one type of malware.

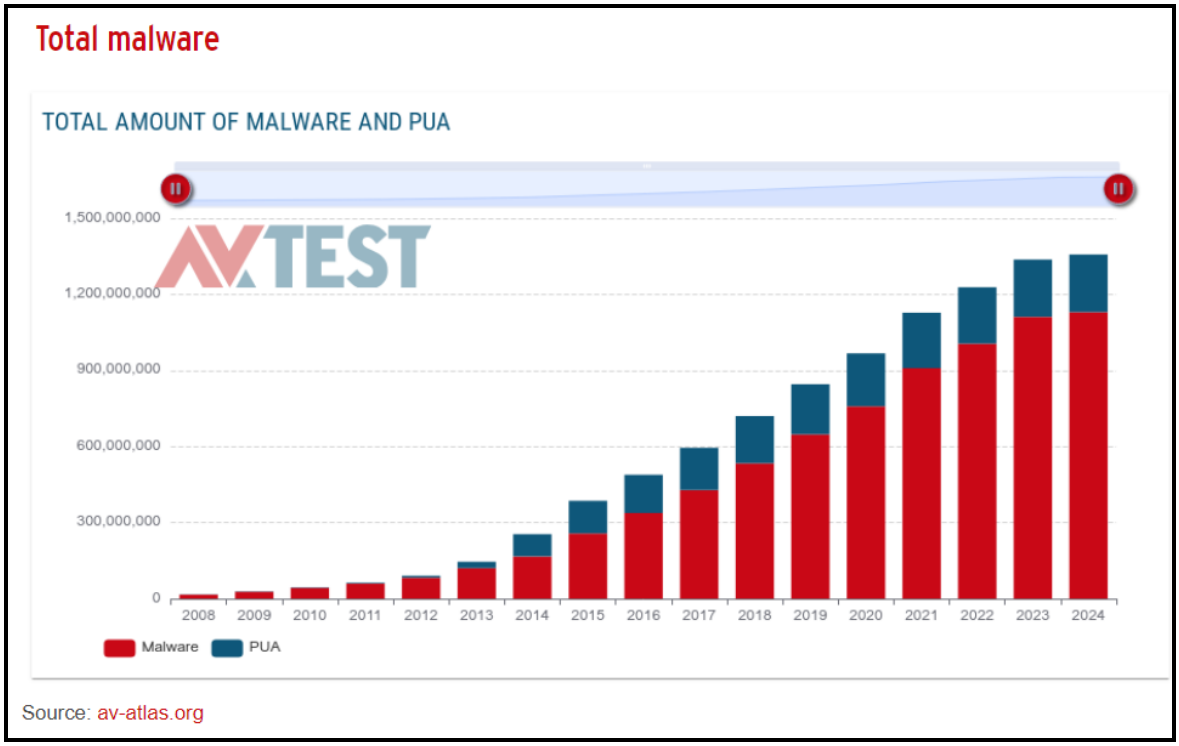

Figure 1: Emerging new malicious programs

Included in **Box 2** below are the most common ways in which malware is spread. It illustrates that malware can be spread by company personnel being deceived by both email and websites that appear legitimate, vulnerabilities within software and operating systems and networks.

Box 2

The spread of Malware

Kaspersky, a well-known privately-owned cybersecurity company has described the most common ways in which malware threats can spread:

- **Email:** If your email has been hacked, malware can force your computer to send emails with infected attachments or links to malicious websites. When a recipient opens the attachment or clicks the link, the malware is installed on their computer, and the cycle repeats.
- **Physical media:** Hackers can load malware onto USB flash drives and wait for unsuspecting victims to plug them into their computers. This technique is often used in corporate espionage.
- **Pop-up alerts:** This includes fake security alerts which trick you into downloading bogus security software, which in some cases can be additional malware.
- **Vulnerabilities:** A security defect in software can allow malware to gain unauthorized access to the computer, hardware, or network.
- **Backdoors:** An intended or unintended opening in software, hardware, networks, or system security.
- **Drive-by downloads:** Unintended download of software with or without knowledge of the end-user.

- **Privilege escalation:** A situation where an attacker obtains escalated access to a computer or network and then uses it to launch an attack.
- **Homogeneity:** If all systems are running the same operating system and connected to the same network, the risk of a successful worm spreading to other computers is increased.
- **Blended threats:** Malware packages that combine characteristics from multiple types of malware, making them harder to detect and stop because they can exploit different vulnerabilities.

UK government initiatives

UK Government alerts

The JCNSS report follows on the heels of alerts issued by the NCSC including the alert titled: "Heightened threat of state-aligned groups against western critical national infrastructure" issued in April 2023 and referred to above. The alert sought to highlight the emerging risk posed by state-aligned adversaries following the Russian invasion of Ukraine. This alert builds on other initiatives such as advise given to the construction industry in August 2022 in the form of the new Information Security Best Practice guide[26]. The NCSC advises the aim of the guide is to help construction firms keep sensitive data safe from attackers by offering tailored advice on how to securely handle the data they create, store it and share it in joint venture projects. It states the guide is a unique collaboration between experts from industry and the National Cyber Security Centre (NCSC), the Department for Business, Energy and Industrial Strategy (BEIS) and the Centre for the Protection of National Infrastructure (CPNI).

Legislation

The UK NIS Regulations: The regulations came into force in 2018 to improve the cyber security of companies providing critical infrastructure and digital services from cyber attacks. The NIS Regulations provide legal measures to boost the overall level of security (both cyber and physical resilience) of network and information systems that are critical for the provision of digital services (online marketplaces, online search engines, cloud computing services) and essential services (transport, energy, water, health, and digital infrastructure services). Organisations which fail to report breaches and network outages within 72 hours face fines up to £17 million[27]. The NIS Directive was declared by the UK Government as being an important part of its five-year £1.9 billion National Cyber Security Strategy to protect the nation from cyber threats[28]. Subsequent changes made to the NIS regulations include requiring essential and digital services to improve cyber incident reporting to regulators such as Ofgem, Ofcom and the ICO[29]. This includes notifying regulators of a wider range of incidents that disrupt service or which could have a high risk or impact to their service, even if they don't immediately cause disruption.

National Cyber Strategy 2022

The National Cyber Strategy[30] describes UK government's **vision** is that the UK in 2030 will continue to be a leading responsible and democratic cyber power, able to protect and promote the country's interests in and through cyberspace in support of national goals. To realise this vision, the UK government intends to pursue five strategic goals. The aim of each is to bolster the nation's strength in one of the five dimensions of cyber power, and collectively enhance the country's ability to uphold a cyberspace that reflects the country's values and interests.

These five goals, labelled as pillars, are intended to form a strategic framework to guide government activity. The pillar of specific interest is Pillars 2 which is described in more detail in **Box3**.

- Pillar 1: Strengthening the UK cyber ecosystem, investing in our people and skills and deepening the partnership between government, academia and industry.
- Pillar 2: Building a resilient and prosperous digital UK, reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are secure online and confident that their data is protected.
- Pillar 3: Taking the lead in the technologies vital to cyber power, building our industrial capability and developing frameworks to secure future technologies.
- Pillar 4: Advancing UK global leadership and influence for a more secure, prosperous and open international order, working with government and industry partners and sharing the expertise that underpins UK cyber power.
- Pillar 5: Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace, making more integrated, creative and routine use of the UK's full spectrum of levers.

Box3

The second of the strategic goals (referred to as Pillars) of the UK Government's National Cyber Strategy 2022
Pillar 2: Cyber Resilience

Overall, the government requires regulated operators of critical national infrastructure (CNI), to raise their standards and manage their risk more proactively. It expects large businesses and organisations, to be more accountable for protecting their systems, services and customers as a core part of running their business. The intention of the Strategy is for the government to :

- increase the adoption of the Cyber Assessment Framework (CAF) or equivalents across CNI sectors, and improve comparability with other cyber security assessment and reporting frameworks in use.
- complete criticality reviews and map dependencies within CNI and its supply chains.
- build stronger partnerships with CNI owners and operators to improve access to threat and risk information, and agree risk posture.
- work to understand new risks or where new CNI is emerging as a consequence of digitalisation and new technologies, including as part of broader priorities such as the transition to Net Zero.
- Cyber risks to UK critical national infrastructure are more effectively managed. Such services are by definition those that the country relies on most.

Operational Technology

Organisations engaged in new CNI projects need to integrate cyber resilience into each project life cycle, including design, procurement and construction, to enable their operations to be safe, reliable and free of interruption. The operation of the UK's CNI is now heavily reliant on Operational Technology (OT), so disruption to the services that they control is of significant concern. Operational Technology (OT) makes all these things happen and pervades our lives in both readily discernible and unseen ways, automatically monitoring and controlling processes

and equipment that are too dangerous, too demanding or too monotonous for manual operation[31]. OT is defined as technology that interfaces with the physical world and includes Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS)[32]. Many businesses strive for improved OT process efficiency and reliability, which often results in increased connectivity to business software and the Internet. This convergence has the potential to increase system vulnerabilities. While cyber security for Information Technology has traditionally been concerned with information confidentiality, integrity and availability, it is worth emphasising that OT priorities are safety first followed by reliability and availability, as there are clearly physical dangers associated with OT failure or malfunction.

Cyber Security Design Principles

The NCSC has published *cyber security design principles*[33]. The principles are intended to help designers produce secure and resilient systems. In particular, the principles are aimed at ensuring that when a project is completed and enters operations, compromise and disruption by cyber incidents is minimised. The design principles are discussed in **Box4.**

Box4

NCSC cyber security design principles

Five principles for the design of cyber secure systems. A system is defined by the NCSC as "a collection of digital components that are connected using communication technologies to perform a business function".

1. Establish the context before designing a system.
   Before you can create a secure system design, you need to have a good understanding of the fundamentals and take action to address any identified short-comings.
2. Make compromise difficult
   Designing with security in mind means applying concepts and using techniques which make it harder for attackers to compromise your data or systems.
3. Make disruption difficult
   When high-value or critical services rely on technology for delivery, it becomes essential that the technology is always available. In these cases the acceptable percentage of 'down time' can be effectively zero
4. Make compromise detection easier.
   Even if you take all available precautions, there's still a chance your system will be compromised by a new or unknown attack. To give yourself the best chance of spotting these attacks, you should be well positioned to detect compromise.
5. Reduce the impact of compromise
   Design to naturally minimise the severity of any compromise.

Ofgem risk management guidance

Ofgem has provided comprehensive and lucid guidance for Operators of Essential Services (OES) based on the Network and Information Systems Regulations 2018 (NIS Regulations)[34]. The NIS Regulations

provide legal measures to maintain and improve the level of security (both cyber and physical resilience) of network and information systems relied upon or used for the provision of essential services. Accountability for compliance with the NIS Regulations lies with the OES. Both operators of Essential Services (OESs) and Relevant Digital Service Providers (RDSPs) must comply with the requirements of the NIS Regulations. Ofgem describes the actions that an OES must follow to accord with the NIS Regulations, these are set out in **Box5** below.

Box5

Under the heading of 'Approach' Ofgem describes the actions that an OES must follow to accord with the NIS Regulations.

"To achieve the aims of the NIS Regulations (i.e. securing those network and information systems that are critical to the delivery of essential services), OES are required to actively manage the security and resilience of their network and information systems whilst also demonstrating compliance with the NIS Regulations to Ofgem through reporting and engagement". The guidance calls for each OES to consider the various steps required to achieve and maintain compliance with the NIS Regulations. In general, these relate to the implementation of a management system for security and resilience which:

1. Employs appropriate processes for identifying and managing the scope of the network and information systems that are relied upon or used for the provision of the essential service. This may include considering, but not limited to: sites, assets, systems, components, interfaces, services, processes, people, and third party suppliers.
2. Employs appropriate processes for managing risks posed to the security of network and information systems on which an essential service relies, or which are used for the provision of the essential service, including those risks that originate from outside of the organisational boundary of an OES as a result of third party dependencies.
3. Actively manages security and resilience during system design and throughout the engineering lifecycle, including by ensuring requirements are considered in the procurement process for products and services.
4. Delivers essential services in a resilient manner, having the capability to detect, respond and recover from network and information system incidents, ensures levels of essential service continuity during an incident, and conducts timely and accurate incident reporting.

Ofgem: Scope examples

Network and information systems: Ofgem has identified examples of the types of network and information systems that are likely to support the provision of an essential service as follows. Ofgem emphasises it is not an exhaustive list, but indicates the types of systems an OES may consider a part of the NIS Scope: operations management systems; supervisory control and data acquisition systems (SCADA); distributed control system (DCS); local controllers (e.g. programmable and electronic controllers); safety instrumented systems (SIS) and safety-related systems; protection systems; intelligent electronic devices; remote terminal units (RTUs); physical plant and sensing equipment; data centre and cloud systems (e.g. cloud SCADA); demand management and balancing systems; real time operation systems; critical communications including wireless networks; and IT Systems deemed critical by the business for the delivery of essential services.

Ancillary systems: Ofgem has identified examples of ancillary systems that may be in scope include: Utility systems (e.g. Heating, Ventilation, and Air Conditioning (HVAC); Power supply; chilled water, Instrumentation air, etc.); trading systems and interfaces; backup control centres; backup systems; remote access solutions; OT configuration management; change management systems; OT asset management systems; cloud/on premise-based monitoring or management systems; building management systems; and physical and cyber security systems.

Ofgem: Risk Management

The NIS reporting requirements cover risk management. Ofgem comments that effective risk management supports decision makers in the response to identified risk exposure.

Methodology: Ofgem does not mandate the use of any specific methodology for risk management. However, it stipulates an OES must explain its risk management methodology (ideally aligned to industry good practice and risk management standards) and apply it consistently to the entirety of its NIS scope. Ofgem provides examples of risk management standards such as ISA 62443-3-2 Security Risk Assessment and System Design standard[35], National Institute of Standards and Technology's (NIST) Risk Management Framework[36], ISO27005[37] and Information Security Forum's IRAM2 methodology[38].

Identification and assessment: Ofgem considers that identifying, assessing and prioritising risk is fundamental to an OES's ability to make risk-based decisions regarding security and resilience. It is expected an OES will ensure security risks to specific network and information systems on which essential services relies are identified and described in terms of threat, vulnerability and consequence; assessed in terms of likelihood and impact and considered in terms of worst-case scenarios. Ofgem provides guidance on threat identification, description, prioritisation and risk response decisions.

Ofgem: NCSC Cyber Assessment Framework

The NCSC have developed the CAF guidance collection[39] which is composed of 14 security and resilience principles, associated guidance, and the assessment framework itself. Distributed across four overarching objectives, the CAF's 14 security and resilience principles are broken down into 39 contributing outcomes. The contributing outcomes are further explained by associated indicators of good practice (IGPs).

Within Part C of the NIS Reporting Requirements, OES are expected to conduct and maintain an accurate positional report against the CAF. OES must have regard to the guidance issued by NCSC when conducting these assessments. OES must also consider relevant NCSC guidance to inform which security and resilience changes to make, and how to make them. When conducting an assessment against the CAF, an OES must assess the 39 contributing outcomes and assign one of the following statuses: Achieved; Partially Achieved; Not achieved; Not relevant, or; Not yet assessed. OES must be able to provide rationale and evidence for the assessed status of each CAF contributing outcome. For CAF outcomes assessed as either 'Achieved', 'Partially Achieved', or 'Not Achieved', an OES must provide rationale as to how their existing security and resilience capability is deemed to meet any of those statuses. For CAF outcomes assessed as 'Not required'

or 'Not yet assessed', an OES must provide rationale as to why these are exceptions and/or when they are due for assessment.

Many OT environments form part of the UK's CNI, so disruption to services that they control is potentially of concern. The NCSC published guidance to help regulators and operators of essential services adhere to the requirements of the Network and Information Security (NIS) Regulations. This guidance can help OT managers ensure that any connectivity between their OT environments and their wider enterprise networks or the Internet is managed securely.

Integration of cyber security within energy projects

Risk Process: A readily understood structure for describing, communicating and embedding cyber risk management within projects is the international standard ISO 31000:2018 - Risk management, a practical guide. It is not a ruled based document and has wide applicability. It has enjoyed international popularity and adoption since the publication of the first edition in 2009 by both its architects and advocates. The risk process described within the standard is included in **Figure 2** below. The standard ISO/IEC 27005:2022(en) "Information security, cybersecurity and privacy protection-Guidance on managing information security risks" is tailored to managing information risks. Many of the terms included in ISO 27005:2022 are drawn from ISO 31000:2018 (or ISO Guide 73:2009 Risk management-vocabulary, common to many ISOs). The risk process described within this standard is shown alongside ISO 31000 in **Figure 3** below to show the similarities.

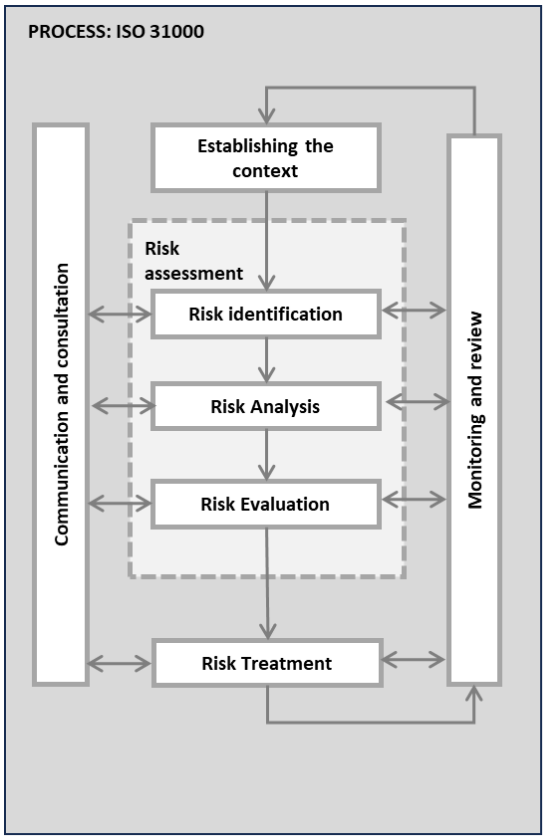

Figure 2: Risk management process, ISO31000

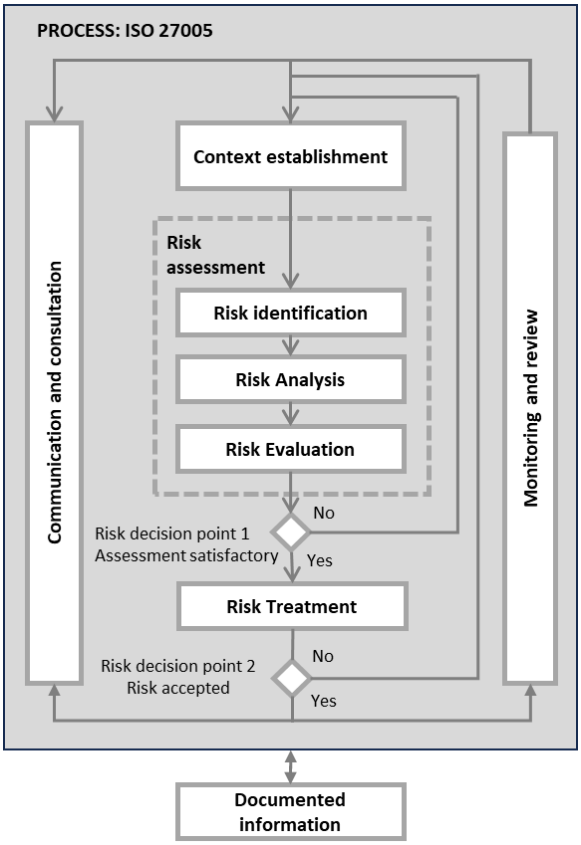

Figure 3: Risk management process ISO27005

STEP 1: Cyber risk context for projects

The context of the management of cyber risk is multi-faceted and complex. It consists of a significant series of interrelated features. Context can be segregated into **internal** and **external** context.

External: The external context includes the nature of the internet, the presence and behaviour of malign actors, the NIS regulations, international standards as well as legal, statutory and regulatory (Ofgem) compliance. A component of the external context is the heavy reliance society, the economy and individuals place on the efficient operation of the county's CNI 365 days a year. Examples of the actions of malign actors in the external environment are included in **Box6**.

Box 6

Threat exposure. The actions of individuals or organisations.

Disruption and destruction: Interference with CNI operational technology by state-aligned groups, hacktivists and groups partnering with capable nation states who have a desire to achieve a disruptive and destructive impact
Living off the land: Described by the NCSC as compromised CNI where Chinese and Russian state sponsored actors are among attackers "operating discreetly, with malicious activity blending in with legitimate system and network behaviour making it difficult to differentiate,". The NCSC has urged operators of CNI to follow the recommended actions to help detect compromises and mitigate vulnerabilities.
Espionage: In May 2023, the NCSC issued a joint advisory revealing details of 'Snake', a sophisticated espionage malware used by Russian cyber actors against their targets. These targets included CNI operators, and the targets were in more than 50 countries across the world.
Ransomware: Denial of service. Ransomware attacks remain one of the greatest cyber threats to UK CNI sectors.

Cyber technologies company MITRE within their Cyber Resiliency Engineering Framework (CREF) Navigator™, a visualization tool which is aimed at aiding "organizations to customize their cyber resiliency goals, objectives, and techniques", recommends maintaining an up-to-date view of the external cyber landscape, as illustrated by an extract of their Navigator below (**Figure 4**). See the component headed "Contextual Awareness". [40]

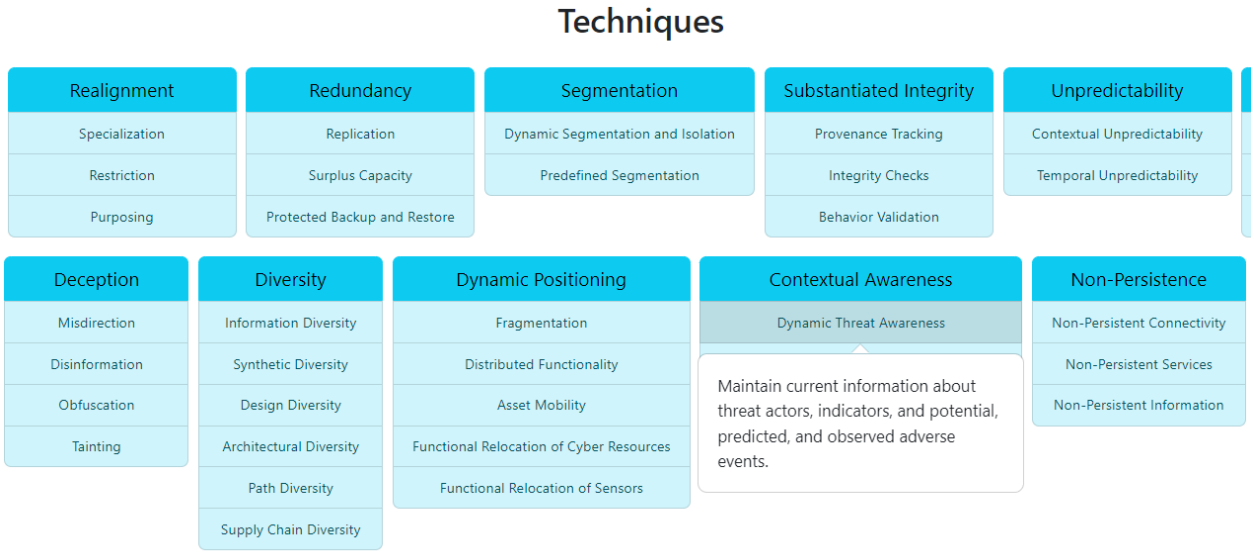

Figure 4: MITRE Cyber Resiliency Engineering Framework (CREF) Navigator™

Internal: The internal context includes an organisation's own goals, risk appetite, processes, procedures, priorities and assurance practices. It includes the norms around procurement, contract strategy, choice of contract and contract conditions. It also includes the adopted project management methodology including project phases and stage gates and governance. Cyber resilience needs to be embedded throughout a project's life cycle including all phases and gates (go/no go decision points), see **Figure 5** below.

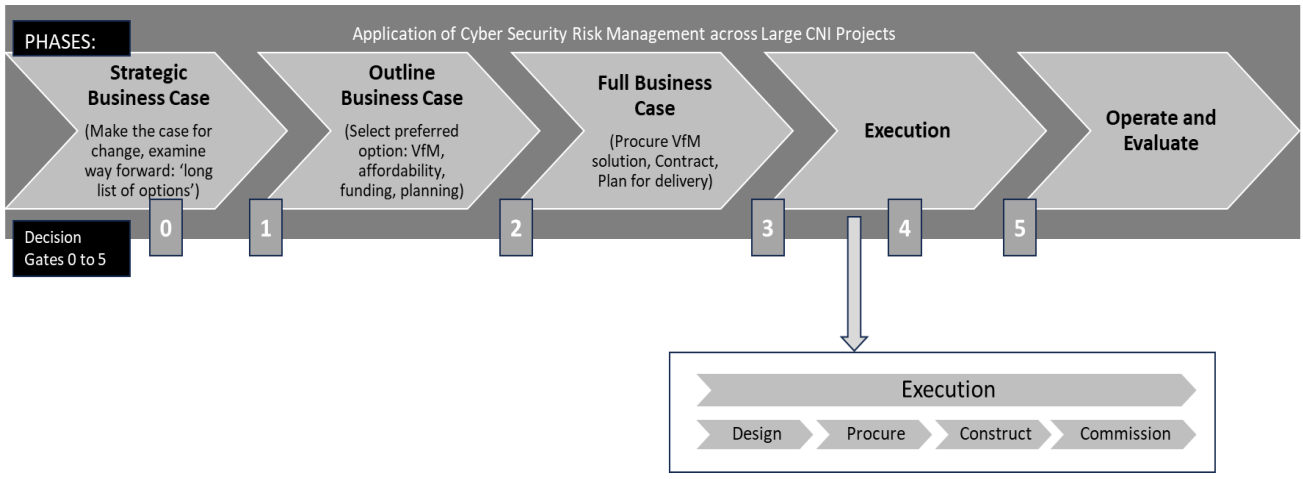

Figure 5: Project life cycle phases and gates

Gate 3: In the Project Life Cycle (PLC) illustrated in the figure, Gate 3 is a critical decision gate in that typically the Information Technology (IT) / Operational Technology (OT), [together with the cyber security design and risk verification and validation plans], have been developed, documented and agreed with the business as a whole or a specific business unit, together with IT/OT and Cyber Risk and Information Security.

Execution: Again, in the PLC illustrated, 'Execution' is carried out by an appointed contractor, (commonly, by not exclusively engaged by way of an NEC contract). The 'Procure' element of Execution relates to the appointed contractor engaging subcontractors and suppliers.

STEP 2: Risk identification

Source: OES organisations are guided to consider a broad landscape of threats including what they describe as un-targeted and targeted attacks by actors employing commodity and bespoke capabilities across all stages of a cyber-attack[41]. The terms referred to are explained in the **Box 7** below.

Box 7

The following terms are described in the National Cyber Security Center's highly informative publication "Common Cyber Attacks: Reducing the Impact guidance".

Untargeted: In un-targeted attacks, attackers indiscriminately target as many devices, services or users as possible. They do not care about who the victim is as there will be a number of machines or services with vulnerabilities. To do this, they use techniques that take advantage of the openness of the Internet, which include: phishing, water holing, ransomware and scanning.

Targeted: In targeted attacks an organisation is singled out because the attacker has a specific interest in that organisation, or has been paid to target it. The groundwork for the attack could take months so that they can find the best route to deliver their exploit

directly to the organisation's systems (or users). A targeted attack is often more damaging than an un-targeted one because it has been specifically tailored to attack the organisation's systems, processes or personnel, in the office and sometimes at home. Targeted

attacks may include: spear-phishing, deploying a botnet, or subverting the supply chain.
Commodity capabilities: involves tools and techniques that are openly available on the Internet (off-the-shelf) that are relatively simple to use. This includes tools designed for security specialists (such as system penetration testers) that can also be used by attackers as they are specifically designed to scan for publicly known vulnerabilities in operating systems and applications.
Bespoke capabilities: involves tools and techniques that are developed and used for specific purposes, and as a consequence require more specialist knowledge. This could include malicious code ('exploits') that take advantage of software vulnerabilities (or bugs) that are not yet known to vendors or anti-malware companies, often known as 'zero-day' exploits. It could also include undocumented software features, or poorly designed applications. Bespoke capabilities usually become commodity capabilities once their use has been discovered, sometimes within a few days.

Threats: Are required to be described in terms of **threat**, **vulnerability** and **impact**. The NCSC describes these terms in a particular way, see **Box 8**. Threat has a different meaning in the context of cyber security as opposed to say infrastructure projects. For cyber security a threat commonly refers to an individual or organisation whereas for infrastructure projects, a threat is an adverse event from a plethora of sources such as the weather, commodity prices, inflation, supplier capacity or ground conditions.

Box 8

NCSC's risk management guidance
https://www.ncsc.gov.uk/collection/risk-management/the-fundamentals-and-basics-of-cyber-risk

Threat: Threats are individuals or organisations that could cause something adverse to happen. Commonly referred to as threat actors.
Vulnerability: This is any weakness in a system that can be exploited by a threat actor. These vulnerabilities do not have to be technical in nature (such as software, hardware and firmware). They can also be weaknesses in procedures, in physical and environmental security, and in personnel security.
Impact: The consequences of a threat being realised such as a cyber system becoming unusable, unreliable, or unsafe, or a cyber event leading to a loss of: money, a contract, or reputation or even a business failing.
Asset: Network and information systems on which the essential service relies, or which are used for the provision of an essential service.
Security Controls (Treatment): Security Controls are technical and non-technical measures that are put in place to mitigate identified risks. They broadly fall into four categories: procedural, physical, personnel and technical control (sometimes known as P3T). Most security mitigation approaches will include a mix of all four types of control.

Threats: From **Box 8** threats are individuals or organisations that could cause adverse events and are commonly referred to as threat actors. These actors may include nation states, terrorists, criminal organisations, malicious insiders, competitors, hacktivists, careless employees, contractors or a third-party supplier. These adverse events may be intentional or unintentional such as careless employees.

Vulnerabilities: Organisations need to scan for vulnerabilities in their systems and hosted software applications on a regular basis. This activity can be supported by employing scanning tools and techniques that examine interoperability between tools [that is the ability of software

packages from different vendors to exchange information between them]. The scanning tools should include the capacity to readily update the vulnerabilities to be scanned. In addition scanning should include analysis of vulnerability scan reports and the communication of findings with other operators, application support teams and security analysists, with the view to securing reciprocal arrangements.

Risk Breakdown Structure (RBS): An RBS may be defined as a hierarchical decomposition of the project environment assembled to provide a comprehensive illustration of the potential sources of risk. Each descending level represents an increasingly detailed definition of the sources of risk[42]. It is used as a prompt to strive to ensure that identification is as comprehensive as possible, for unidentified vulnerabilities will not be managed.

Description: In line with common good practice, Ofgem require that risks are sufficiently detailed to allow them to be assessed and for risk response actions to be defined.

Database: The efficient management of threats and opportunities requires a risk management database as a secure, readily accessible, 'one source of the truth' of risk data which records threat exposure, assessment and treatment.

STEP 3: Analysis
Analysis examines the potential impact of a vulnerability in terms of likelihood and impact.
Likelihood: Likelihood can be assessed using a table similar one to the one below **(Table 2)** for qualitative assessments to rank vulnerabilities and prioritise action.

Ref	Traffic Light	Probability	Explanation
E	Very High	70% or greater	Event is **expected** to occur in most circumstances. Frequently occurs among energy providers.
D	High	Between 50% and 69%	Event is **likely** to occur in most circumstances. Regularly occurs among energy providers.
C	Medium	Between 30% and 49%	It is **Possible** the event will occur at some time. Has occurred within the industry.
B	Low	Between 10 and 29%	**Unlikely** although the event has occurred previously within the industry
A	Very Low	Less than or equal to 9%	**Rare**, may occur in exceptional circumstances.

Table 2: Range of likelihood from A to E

The reference is used to cross refer with the Qualitative risk impact matrix illustrated in **Table 3.**
Impact: Is typically measured in terms of financial impact and delay but can be expanded to include a number of other parameters such as reputation, health and safety and break in service.

Impact measure						
	6-Catastrophic	Portfolio Management	Portfolio Management	Group Risk Committee	Group Risk Committee	Group Risk Committee
	5-Severe	Programme Management	Portfolio Management	Portfolio Management	Group Risk Committee	Group Risk Committee
	4-Major	Programme Management	Programme Management	Portfolio Management	Portfolio Management	Group Risk Committee
	3-Serious	Business Unit Manager	Programme Management	Programme Management	Portfolio Management	Portfolio Management
	2-Minor	Business Unit Manager	Business Unit Manager	Programme Management	Programme Management	Portfolio Management
	1-Incidental	Business Unit Manager	Business Unit Manager	Business Unit Manager	Programme Management	Programme Management
		E-Rare	D-Unlikely	C-Possible	B-Likely	A-Expected
Frequency or likelihood						

Table 3: Qualitative risk impact matrix based on frequency and impact

The colour coding provides the ability to provide one of four subjective risk ratings to a vulnerability aided by a colour coding of the cells of the matrix, where red = very high, orange = high, yellow = medium and green = low. In addition, it provides the ability to record the reporting regime for vulnerability ratings from say the Group Risk Committee down to Business Unit Managers. It is typical for a description of the impact ratings to be recorded such as what are the implications of a catastrophic or severe impact for instance.

STEP 4: Evaluation

This includes an assessment of the aggregate exposure of weighted impacts to understand the potential impact on a project. In addition, sensitivity assessments can be carried out to discern the impact of a single threat under examination on the aggregate exposure. The aggregate exposure can be compared with an organisaition's risk appetite to support go/no go decisions at project gates (See **CaseStudy1** and **Box9**).

Company Risk Appetite: The UK Government's publication "The Orange Book – Management of Risk, Principles and Concepts, 2020" (and referred to in the UK Government's "Risk Appetite Guidance Note 2021") provides a helpful overview of risk appetite: "the Board should determine and continuously assess the nature and extent of the principal risks that the organisation is exposed to and is willing to take to achieve its objectives – its risk appetite – and ensure that planning and decision-making reflects this assessment. Effective risk management should support informed decision-making in line with this risk appetite, ensure confidence in the response to risks, transparency over the principal risks faced and how these are managed".

CASE STUDY1: SSE plc (Source: Annual Report 2023, page 70)

Risk Appetite Statement:

The Group risk appetite remains aligned to the achievement of SSE's strategic objectives. SSE will however only accept risk where it is consistent with its core purpose, strategy and values; is well understood; can be effectively managed; is in line with stakeholder expectations and offers commensurate reward.

SSE has no appetite for risks brought on by insecure actions including those relating to cyber security. In areas where SSE is exposed to risks for which it has little or no appetite, even though it has implemented high standards of control and mitigation, the nature of these risks mean that they cannot be eliminated completely.

Project Risk Appetite: UK government security guidance provides advice for individual projects in setting their cyber security risk appetite. The benefit of describing risk appetite is described as assisting a project in achieving "the outcomes included in the Secure by Design principles to adopt a risk-driven approach and embed continuous assurance"[43]. The guidance advises that creating a project risk appetite statement will allow a project to: determine acceptable and unacceptable risks; create a risk culture and set risk expectations to be shared across the delivery team; and make informed, timely and effective risk management decisions. The guidance recommends that projects adopt the following five steps in defining a project cyber risk appetite:

Step 1: Summarise your project scope
Step 2: Align with the organisation's risk appetite
Step 3: Determine relevant security threats
Step 4: Determine the required constraints
Step 5: Communicate the security risk appetite

Once compiled it needs to be signed off by the appropriate personnel such as the project and programme managers, the Project Director together with the individuals responsible for assessing cyber security risks and implementing relevant controls, such as technical subject matter experts and cyber security specialists.

Box 9

The red lines of risk exposure which organisations are not willing to cross.

Risk appetites are how organisations define the risk red lines associated with business or operational opportunities. This could include for example, what an organisation, programme, project, operation or system owner is unwilling to accept risk exposure on, such as fulfilling its legal / regulatory obligations to the protection of personal information, or continued plant operations. These risk red lines must be communicated to those who need to work with them, in a way that is accessible and understood.

STEP 5: Treatment

A window onto how leading OES organisations are responding to potential vulnerabilities, is to examine their annual reports. Three case studies are included below. The quality of the description of the approach to response planning varies considerably. When reporting, organisations typically seek a judicious balance between providing confidence to shareholders, regulators, joint venture partners and employees, while at the same time as not sharing information that may be helpful to a competitor. In addition, the organisations within the case studies vary substantially in size (see **Figure 6**) and in all probability have very different cyber security arrangements. Taken together these factors may explain the difference in approach. The case studies are recorded in order based on their turnover.

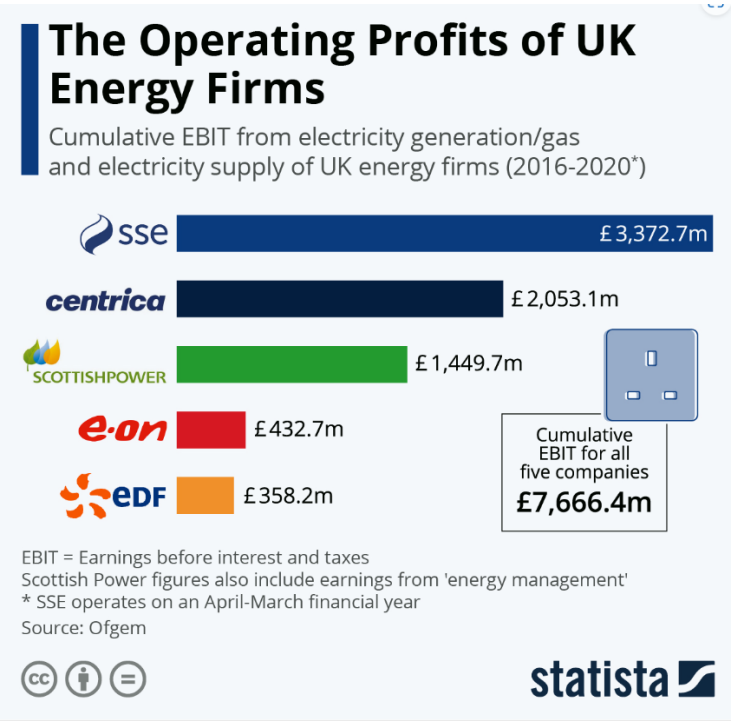

Figure 6: The operating profits of UK Energy Firms

CASE STUDY 2:

SSE plc Risk Response Implementation (Source Annual Report 2023)

Approach to response planning:

- Publication of an SSE Cyber Security **Policy** and SSE Data and Information Management Policy.
- Key technology and infrastructure risks are incorporated into the **design of systems** and are regularly appraised with risk mitigation plans recommended.
- SSE conducts regular internal and **third-party testing of the security of its information and operational technology networks and systems**.
- Continued strengthening and embedding of the cyber risks and controls framework to continue to
- identify threats and reduce exposures through, for example, improved use of data analytics and further
- migration from unsupported systems.
- Significant longer term **Security Programme investment and planning** which seeks to strengthen
- the resilience of the systems on which SSE relies.
- **IT Service Assurance** works with individual Business Units to form and agree appropriate service level
- agreements for business-critical IT services.
- **Business continuity plans** are reviewed in response to changes in the threat to the Group and regularly tested.
- Over the course of the year an updated **Cyber Security Culture Strategy** was launched. This has been designed to continue to improve the cyber security maturity across the Group and build positively on the existing, strong cyber culture. The implementation of this strategy will be assessed and monitored to measure its impact on the levels of cyber security awareness and culture across the Group

CASE STUDY 3:

CENTRICA plc (Source: Annual Report and Accounts 2023)

Approach to response planning:

- Ongoing **threat intelligence gathering**, collaboration and information sharing with industry peers and National Cyber Security Centre.
- The **Cyber Security Change Programme** builds security capabilities and improvements in controls that increase the difficulty of targeting Centrica and being able to exploit weaknesses without detection.
- The **Ransomware Programme** has delivered improvements to enhance Centrica's ability to co-ordinate and recover from a ransomware attack.
- Enhanced **cyber controls** dedicated to protecting operational technology (control systems used to manage domestic, commercial and industrial processes) have been implemented.
- **Training and awareness** campaigns delivered to all employees in 2023 and focused training has been developed for key groups to raise awareness and highlight responsibilities in protecting data.
- Cyber-attack **simulations** to identify and remediate control gaps.

CASE STUDY 4:

E.ON Operational and IT Risk Management (Source: Annual Report 2023)

Approach to response planning:

- Cybersecurity and the continuous protection of IT and OT systems against cyberattacks constitute a focus area of E.ON's risk management. Examples include the analysis of attacks on the systems of the network business (which could affect the operation of E.ON's critical infrastructure), on the sales business (which could result in the loss of customer data), and on internal systems (which E.ON uses to control commercial processes in all its business units).
- Operating units and the Cybersecurity and Enterprise Risk Management divisions jointly and proactively evaluate and manage risks for E.ON.
- Technologically complex production facilities are used in the distribution of energy, resulting in major risks from procurement and logistics, construction, the operation and maintenance of assets, as well as general project risks.

Cyber Security Assurance: Cybersecurity Capability Model C2M2

Assistance in developing mature practices is available online. As reported in "The Rules of Project Risk Management, Implementation Guidelines for Major projects" published in 2014[44], following a U.S. White House initiative focused on assessing the security of the electricity industry, in 2012 the US Department of Energy (DOE) developed the C2M2 Cybersecurity Capability Maturity Model[45]. It was the product of a collaboration between cybersecurity and energy industry experts. Model updates have been supported by hundreds of energy sector stakeholders. Numerous revisions have been made and version 2.1 was released in June 2022. C2M2 is a free tool to help organisations evaluate their cybersecurity capabilities and make the most of their security investments. It uses a set of industry-vetted cybersecurity practices focussed on both information technology (IT) and operations technology (OT) assets and environments.

Summary

If the operation of the nation's critical infrastructure is to be resilient to cyber attacks from malign actors, predominantly located overseas, cyber security needs to be embedded within CNI projects from inception through to completion. This entails ensuring that the design, together with engagement with the supply chain, builds in cyber reliance. This design must reflect and keep abreast of the moving risk landscape recognised to be growing in sophistication, complexity and severity. International risk management standards support the development and implementation of a structured approach to risk management. Over and above the daily challenge of maintaining resilience is the need to meet the needs of Ofgem and satisfy the requirements of the NIS legislation. The potential implications on not being successful and CNI being disrupted or damaged on a major scale, would be harmful to our way of life, our economy and in some instances our very safety.

Previous research by the lead author

This paper develops the research conducted by the lead author for the following:

- Chapman, R. J., (2024). Exposure of the UK's critical national infrastructure to ransomware attacks and ransom demands; PM World Journal, Vol. XIII, Issue II, February. https://pmworldlibrary.net/wp-content/uploads/2024/02/pmwj138-Feb2024-Chapman-exposure-to-Uks-critical-national-infrastructure-to-cyber-attacks.pdf

- Robert Chapman (2024) "How to protect your critical national infrastructure project from cyberattacks". Association for Project Management Blog, Published on 21 Mar 2024.

- "The SME business guide to fraud risk management" published by Routledge in 2022

- Chapman, R. J. (2022). Update: the exposure of small UK project management organisations to fraud; PM World Journal, Vol. XI, Issue IX, September. https://pmworldlibrary.net/wp-content/uploads/2022/09/pmwj121-Sep2022-Chapman-exposure-of-small-uk-pm-organisations-to-fraud-update.pdf

- Chapman, R. J. (2022). The exposure of small UK project management organisations to fraud; PM World Journal, Vol. XI, Issue V, May. https://pmworldlibrary.net/wp-content/uploads/2022/05/pmwj117-May2022-Chapman-exposure-of-small-uk-pm-organisations-to-fraud.pdf

- Appendix K Cybersecurity Capability Maturity Model within "The Rules of Project Risk Management, Implementation guidelines for major projects, Second Edition" published in 2020 by Routledge

- Chapman, R. J. (2015) "United States Cyber Security for the armed forces" Institute of Risk Management, Risk Management Professional Magazine, winter edition

Annex A: Glossary

Drawn from: UK Government Policy paper, National Cyber Strategy 2022 (HTML), Updated 15 December 2022
https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

Action Fraud	the reporting centre for fraud and cyber-crime where citizens and organisations should report fraud if they have been scammed, defrauded or experienced cyber-crime in England, Wales and Northern Ireland. In Scotland, reports go to Police Scotland.
Active Cyber Defence (ACD)	helps organisations to find and fix vulnerabilities, manage incidents or automate disruption of cyber-attacks. Some services are designed primarily for the public sector, whereas others are made available more broadly to private sector or citizens, depending on their applicability and viability.
Artificial Intelligence	a technology in which a computing system is coded to ''think for itself', adapting and operating autonomously. AI is increasingly used in more complex tasks, such as medical diagnosis, drug discovery, and predictive maintenance.
Authentication	the process of verifying the identity, or other attributes of a user, process or device.
Autonomous System	a collection of IP networks for which the routing is under the control of a specific entity or domain.
Blockchain Technology	a particular way of storing data. A blockchain is an example of a distributed ledger – a type of append-only, tamper-proof storage technology.
COBR	Cabinet Office Briefing Rooms. The UK central government response to emergencies is underpinned through use of COBR; the physical location, usually in Westminster, from which the central response is activated, monitored and co-ordinated and which provides a focal point for the government's response and an authoritative source of advice for local responders.
Competent Authorities	regulatory bodies as described in the Network and Information Systems (NIS) Regulations 2018. There are multiple competent authorities responsible for different sectors covered by NIS.
Connected Places	a community that integrates information and communication technologies and IoT devices to collect and analyse data to deliver new services to the built environment, and enhance the quality of living for citizens.
Critical National Infrastructure	Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:
	a. major detrimental impact on the availability, integrity or delivery of essential services including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or
	b. significant impact on national security, national defence, or the functioning of the state.
Crypt-Key (CK)	the term used to describe the UK's use of cryptography to protect the critical information and services on which the UK government, military and national security community rely, including from attack by our most capable adversaries.
Cryptocurrency	a digital currency and payment system, e.g. Bitcoin.
Cryptography	the science or study of analysing and deciphering codes and ciphers; cryptanalysis.
Cyber Assessment Framework (CAF).	provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible
Cyber Attack	deliberate exploitation of computer systems, digitally-dependent enterprises and networks to cause harm.

Cyber crime	cyber-dependent crime (crimes that can only be committed through the use of ICT devices, where the devices are both the tool for committing the crime and the target of the crime); or cyber–enabled crime (crimes that may be committed without ICT devices, like financial fraud, but are changed significantly by use of ICT in terms of scale and reach).
Cyber ecosystem	the totality of interconnected infrastructure, persons, processes, data, information and communications technologies, along with the environment and conditions that influence those interactions.
Cyber Incident	an occurrence that actually or potentially poses a threat to a computer, internet-connected device, or network – or data processed, stored, or transmitted on those systems – which may require a response action to mitigate the consequences.
Cyber power	Cyber power is the ability to protect and promote national interests in and through cyberspace. Building cutting-edge cyber security and operational capabilities and a leading cyber security sector.
Cyber Resilience	The overall ability of systems, organisations and citizens to withstand cyber events and, where harm is caused, recover from them.
Cyber Risk	The potential that a given cyber threat will exploit the vulnerabilities of an information system and cause harm.
Cyber Security	The protection of internet-connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.
Cyber Security Body of Knowledge (CyBOK)	A unique resource, providing for the first time an underpinning body of knowledge encompassing the breadth and depth of cyber security, showing that cyber security encompasses a wide range of disciplines.
Cyber Power	Cyber power is a concept which the UK government defines as the ability of a state to protect and promote its interests in and through cyberspace. The government identifies five broad dimensions of cyber power as: • The foundation of the UK's cyber power is seen as the people, knowledge, skills, structures and partnerships that underpin all the other components and integrate them into a national approach. • The ability to protect the UK's assets through cyber security and resilience, in order to realise the full benefits that cyberspace offers to our citizens and economy. • The technical and industrial capabilities to maintain a stake in the evolution of key cyber technologies and deploy new advances in the interests of society. • The global influence, relationships and ethical standards to shape rules and norms in cyberspace in line with our values and interests and promote international security and stability. • The ability to take action in and through cyberspace to support national security, economic wellbeing and crime prevention. It is considered that given the pace of technological change cyber power it can be gained and lost more quickly, as previously cutting-edge capabilities are rendered obsolete by new advances. The strategy aims to be pro-active rather than reactive.
Cyberspace	What is cyberspace? To many of us, cyberspace is the virtual world we experience when we go online to communicate, work and conduct everyday tasks. In technical terms, cyberspace is the interdependent network of information technology that includes the internet, telecommunications networks, computer systems and internet-connected devices. For the military, and when considering our efforts to counter threats in cyberspace, it is an operational domain, along with land, sea, air and space.

	Cyberspace can be described in terms of three layers: Virtual: It consists of representations of people and organisations through a virtual identity in a shared virtual space. Virtual representations can be an email address, user identification, or a social media account. Logical: The part of cyberspace made up of code or data, such as operating systems, protocols, applications and other software. Physical: The logical layer cannot function without the physical layer and information flows through wired networks or the electromagnetic spectrum. The physical layer of cyberspace includes all the hardware on which data is transmitted, - large complex telecommunications systems operated by big tech companies.
Cyber Threat	anything capable of compromising the security of, or causing harm to, information systems and internet connected devices (to include hardware, software and associated infrastructure), the data on them and the services they provide, primarily by cyber means.
Data Breach	the unauthorised movement or disclosure of information on a network to a party who is not authorised to have access to, or see, the information.
Domain	a domain name locates an organisation or other entity on the internet and corresponds to an Internet Protocol (IP) address.
Devolved government or devolved administration –	responsible for many domestic policy issues with the power to make laws for these areas. The separate legislatures and executives in Scotland, Wales and Northern Ireland following devolution,
Digital Twin	a virtual replica or representation of assets, processes, systems, or institutions in the built, societal, or natural environments that provides insight into how complex physical assets and citizens behave, helping organisations improve decision-making and optimise processes. Changes in the real world are reflected in the twin, and changes in the twin can be replicated automatically in the real world.
Five Eyes	Five Eyes is the name of the intelligence alliance between the USA, UK, Canada, Australia and New Zealand which helps share information to keep its citizens as safe as possible from threats.
GCHQ	Government Communications Headquarters; the centre for the government's signals intelligence activities and Cyber National Technical Authority (NTA).
GFCE	Global Forum on Cyber Expertise.
Government Cyber Coordination Centre (GCCC)	Proposed joint venture between GSG, CDDO and NCSC bringing together their respective functions and areas of expertise to better coordinate operational cyber security efforts across government, transform how cyber security data and threat intelligence is used across government and truly enhance government's ability to 'defend as one'.
Horizon-scanning.	a systematic examination of information to identify potential threats, risks, emerging issues and opportunities allowing for better preparedness and the incorporation of mitigation and exploitation into the policy-making process
ICANN	Internet Corporation for Assigned Names and Numbers. It coordinates website names and IP addresses.
Incident Management	the management and coordination of activities to investigate, and remediate, an actual or potential occurrence of an adverse cyber event that may compromise or cause harm to a system or network.
Incident Response	the activities that address the short-term, direct effects of an incident, and may also support short-term recovery.
Industrial Control System (ICS).	an information system used to control industrial processes, such as manufacturing, product handling, production and distribution, or to control infrastructure assets

Integrated Review	'Global Britain in a Competitive Age, the Integrated Review of Security, Defence, Development and Foreign Policy', describes the government's vision for the UK's role in the world over the next decade and the action government will take to 2025.
Integrity	in information security, integrity means that information has not been changed accidentally, or deliberately, and is accurate and complete.
Internet	a global computer network, providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols.
Internet of Things	the totality of devices, vehicles, buildings and other items embedded with electronics, software and sensors that communicate and exchange data over the internet.
Legacy IT	Legacy IT refers to systems and their component software and hardware that are outside of vendor support, on extended support and/or on bespoke support arrangements
Managed Service Providers	third parties that provide a set of defined services to a customer and assume the responsibility of running, maintaining, and securing those services.
Microgeneration	the small-scale generation of energy by households, small businesses and communities.
NATO	North Atlantic Treaty Organisation.
NCA	National Crime Agency.
National Cyber Security Centre (NCSC)	the UK's technical authority for cyber threats, providing a unified national response to cyber incidents to minimise harm, helping with recovery and learning lessons for the future.
Network and Information Systems (NIS) Regulations 2018.	UK regulations that provide legal measures to boost the level of security (both cyber & physical resilience) of network and information systems for the provision of essential services and digital services
OECD	The Organisation for Economic Co-operation and Development, an intergovernmental economic organisation.
Offensive Cyber	adding, deleting or manipulating data on systems or networks to deliver a physical, virtual or cognitive effect. Offensive cyber operations often exploit technical vulnerabilities, use systems or networks in ways that their owners and operators would not intend or condone, and may rely on deception or misrepresentation.
Operational Technologies (OT)	combine hardware and software to monitor, control and automate physical processes, particularly in industrial sectors such as energy, manufacturing, water, and transport.
Operators of Essential Services	organisations within vital sectors which rely heavily on information networks, for example utilities, healthcare, transport, and digital infrastructure sectors as identified by the criteria in the Network and Information Systems (NIS) Regulations 2018.
Plan for Digital Regulation	sets out the government's overall approach for governing digital technologies in order to drive growth and innovation.
Quantum Technologies	Quantum technology relies on the principles of quantum physics. The advancing understanding and control of what are known as 'quantum effects' such as superposition and entanglement will lead to a new wave of advances that will underpin our economy and society: sensing, data transmission and encryption, timing and computing.
Ransomware	malicious software that denies the user access to their files, computer or device until a ransom is paid.
Secure by Design	software, hardware and systems that have been designed from the ground up to be secure.
Vulnerability	bugs in software programs that have the potential to be exploited by attackers.
Vulnerability Reporting Service	A mechanism through which an organisation can be alerted to security flaws before they are exploited by attackers

Annex B: UK government authorities supporting cyber resilience

There are a number of UK government organisations supporting the defence of the UK against cyber attacks with both disparate and overlapping roles. Some of the primary parties are included below.

Cabinet Office: is responsible for the National Cyber Strategy, which comprises the NIS National Strategy. The Cabinet Office also has overall responsibility for improving the security and resilience of critical national infrastructure.

Department for Digital, Culture, Media and Sport: (DCMS) is responsible for the overall implementation of the NIS Regulations, including co-ordinating the relevant authorities and NCSC. DCMS issues guidance for competent authorities to support wider NIS implementation across the UK.

National Cyber Security Centre: set up by the government in October 2016 as part of GCHQ, has multiple functions. It is described by government as embodying "world class cyber threat detection and analysis capabilities". It is the national single point of contact (SPOC) for engagement with international [EU] partners on NIS, coordinating requests for action or information and submitting annual incident statistics. The NCSC works with partners across the public and private sector, at home and overseas, to detect and respond to threats and incidents. It is also the UK's Computer Security Incident Response Team (CSIRT). It is responsible for monitoring cyber security incidents at a national level; providing real-time threat analysis, defence against national cyber-attacks, technical advice, and response to major cyber incidents to help minimise harm. In April 2023 the NCSC issued an alert to CNI organisations warning of an emerging threat from state-aligned groups, particularly those sympathetic to Russia's invasion of Ukraine[46]. The alert warned that some groups had declared an intent to launch 'destructive and disruptive attacks' and that CNI organisations should ensure they have taken steps outlined in the NCSC's heightened threat guidance to strengthen their defenses. In 2023, the NCSC also released a joint advisory with CISA (the US's Cybersecurity and Infrastructure Security Agency), highlighting the risks posed by China against UK CNI. The NCSC maintains the outcome-based Cyber Assessment Framework (CAF) and provides extensive guidance on cyber security matters as the National Technical Authority.

National Cyber Force (NCF): created 2021 implements the National Offensive Cyber Programme has invested in offensive cyber capabilities.

National Crime Agency (NCA): is the national law enforcement response which seeks to disrupt and raise the cost of hostile and criminal activity in cyberspace.

National Crime Agency's (NCA) **National Cyber Crime Unit** (NCCU): provides national leadership and coordination of the response, supported by a network of dedicated **Regional Cyber Crime Units** (RCCUs) in each of England and Wales' nine police regions, in partnership with their counterparts in Police Scotland and Police Service of Northern Ireland, as well as the Metropolitan Police Service's Cyber Crime Unit.

About the Author

Robert J. Chapman, PhD, MSc.

United Kingdom

Dr Robert J Chapman is an international risk management specialist. He has provided risk management services in the UK, the Republic of Ireland, Holland, UAE, South Africa, Malaysia and Qatar on multi-billion programmes and projects across 14 different industries. He is author of the texts: 'The SME business guide to fraud risk management' published by Routledge, 'Simple tools and techniques for enterprise risk management' 2nd edition, published by John Wiley and Sons Limited, 'The Rules of Project Risk Management, implementation guidelines for major projects' 2nd edition published by Routledge Publishing and 'Retaining design team members, a risk management approach' published by RIBA Enterprises. He holds a PhD in risk management from Reading University and has been elected a fellow of the IRM, CIHT, APM and ICM and is a former member of the RIBA. In 2007 Andrew Bragg (APM Chief Executive at the time) formally confirmed he has exceptional risk management skills. Robert has passed the M_o_R, APM and PMI risk examinations. In addition, he has provided project and risk management training in Scotland, England, Singapore and Malaysia. Robert has been an external PhD examiner.

References

[1] How to cite this work: Chapman, R. J. (2024). Integration of cyber resilience within energy projects forming the UK's critical national infrastructure, *PM World Journal*, Vol. XIII, Issue VI, June.
[2] R J Chapman (Dr Chapman and Associates Ltd-registered in the UK)
[3] Chapman, R. J., (2024). Exposure of the UK's critical national infrastructure to ransomware attacks and ransom demands; PM World Journal, Vol. XIII, Issue II, February.
[4] UK Government (2022) Policy paper, National Cyber Strategy 2022, Updated 15 December 2022, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#pillar-5-countering-threats.
[5] Ditto
6 Financial Times (2019) "India confirms cyberattack on nuclear power plant" , October https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6
[7] World Economic Forum (2021) "What the cyber-attack on the US oil and gas pipeline means and how to increase security". https://www.weforum.org/agenda/2021/05/cyber-attack-on-the-us-major-oil-and-gas-pipeline-what-it-means-for-cybersecurity/
[8] Financial Times (2024) "British Library to burn through reserves to recover from cyber attack.5 January. https://www.ft.com/content/4be5d468-0cc3-4881-a5fb-b5d0163de93e
[9] BBC (2023) "British Library: Employee data leaked in cyber attack". 21 November https://www.bbc.co.uk/news/entertainment-arts-67484639
[10] BBC (2024) "Hackers threaten to publish huge cache of NHS data". https://www.bbc.co.uk/news/articles/c3g5r9g45n4o
[11] UK Government (2022) Policy paper, National Cyber Strategy 2022, Updated 15 December 2022, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022?trk=article-ssr-frontend-pulse_x-social-details_comments-action_comment-text
[12] BBC (2024) "Claims that smart motorways tech leaves drivers at risk", 22 April. https://www.bbc.co.uk/news/uk-68848418
[13] https://www.ncsc.gov.uk/files/Criticalities-and-CNI-Knowledge-Base-Industry-Flyer.pdf
[14] NCSC (2023) "Annual Review 2023". https://www.ncsc.gov.uk/files/Annual_Review_2023.pdf
[15] House of Commons, House of Lords Joint Committee on the National Security Strategy, A hostage to fortune: ransomware and UK national security, First Report of Session 2023–24, Published on 13 December 2023
[16] The Joint Committee on the National Security Strategy scrutinizes the structures for Government decision-making on national security, particularly the role of the National Security Council and the National Security Adviser.
[17] Ditto
[18] Guardian (2023) "Russian hackers want to 'disrupt or destroy' UK infrastructure, minister warns", Dan Sabbagh Defence and security editor, Wed 19 Apr . https://www.theguardian.com/technology/2023/apr/19/russian-hackers-want-to-disrupt-or-destroy-uk-infrastructure-minister-warns
[19] UK Parliament Committees (2023) How resilient is UK Critical National Infrastructure to cyber-attack? 24 October 2023. https://committees.parliament.uk/committee/135/science-innovation-and-technology-committee/news/198084/how-resilient-is-uk-critical-national-infrastructure-to-cyberattack/
[20] The Guardian (2023) "GCHQ warns of fresh threat from Chinese state-sponsored hackers, National Cyber Security Centre urges operators of critical national infrastructure to prevent hacks". Dan Milmo, Global technology editor. 25 May. https://www.theguardian.com/technology/2023/may/25/experts-warn-against-china-sponsored-cyber-attacks-on-uk-networks
[21] ComputerWeekly.com (2023) "Nuclear regulator raps EDF over cyber compliance, The Office for Nuclear Regulation says EDF has come up short on needed measures to improve cyber security standards at several critical UK nuclear facilities" Alex Scroxton, published 19 Oct 2023 https://www.computerweekly.com/news/366556335/Nuclear-regulator-raps-EDF-over-cyber-compliancey
[22] Deloitte (2022), "Incentives are key to breaking the cycle of cyberattacks on critical infrastructure. The path to protecting critical infrastructure from cyberattack may lie not through new technology, but through a better understanding and shaping of incentives". Deloitte Insights Magazine, Issue 30, Summer 2022, Featured Article.

[23] Walker, A (1984) "Project Management in Construction", Published by Granada.
[24] World Energy Council (2019) "Cyber challenges to the energy transition", published by the World Energy Council.
[25] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022
[26] NCSC, BEIS & CPNI (2022) "Joint Ventures in the Construction Sector: Information Security Best Practice Guidance", August
[27] DfDCM&S and NCSC (2018) "Tough new rules to protect UK's critical infrastructure come into force" published 10 May 2018.
[28] Ditto
[29] DfDCM&S (2022) "Cyber laws updated to boost UK's resilience against online attacks", published 30 November 2022
[30] UK government (2022) "National Cyber Strategy 2022 Pioneering a cyber future with the whole of the UK", https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf
[31] NCSC (2024) "Operational Technology, Making sense of cyber security in OT environments". Published 18 March 2024. https://www.ncsc.gov.uk/collection/operational-technology
[32] Ditto
[33] NCSC (2019) Secure design principles, Guides for the design of cyber secure systems. Published 21 May 2019. https://www.ncsc.gov.uk/collection/cyber-security-design-principles
[34] Ofgem is the Office of Gas and Electricity Markets. Ofgem is a non-ministerial government department governed by GEMA. GEMA is the body referenced in the NIS Regulations. The terms "Ofgem" and the "Gas and Electricity Markets Authority" are used interchangeably in the guidance.
[35] IEC 62443 Series: Security for Industrial Automation and Control Systems, https://webstore.iec.ch/searchform&q=62443
[36] NIST Risk Management Framework, https://csrc.nist.gov/Projects/risk-management https://www.securityforum.org/solutions-and-insights/information-risk-assessment, methodology-iram2/
[37] ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management, https://www.iso.org/standard/75281.html
[38] Information Security Forum Information Risk Assessment Methodology 2 (IRAM2),
[39] NCSC CAF Guidance, https://www.ncsc.gov.uk/collection/caf.
[40] MITRE (2023), "MITRE Launches Cyber Resiliency Engineering Framework Navigator". https://www.mitre.org/news-insights/news-release/mitre-launches-cyber-resiliency-engineering-framework-navigator
[41] NCSC (2016) Common Cyber Attacks: Reducing the Impact guidance, https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact# download
[42] Definition based on the description provided within Chapman, R. J. (2011) "Single tools and techniques for enterprise risk management", John Wiley and Sons Limited.
[43] UK Government (2024) "Working out the project's security risk appetite". Update: 31 January 2024 https://www.security.gov.uk/guidance/secure-by-design/activities/working-out-the-projects-security-risk-appetite
[44] Chapman, R.J. (2014) "The Rules of Project Risk Management, Implementation Guidelines for Major Projects", Gower Publishing Limited, UK and Ashgate Publishing Limited, USA
[45] Office of Cybersecurity, Energy Security, and Emergency Response "Cybersecurity Capability Maturity Model C2M2", https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2. Downloaded May 2024
[46] NCSC (2023) "NCSC warns of emerging threat to critical national infrastructure. Alert issued warns of the emerging threat from state-aligned groups and the different forms of activity". Published 19 April 2023, https://www.ncsc.gov.uk/news/ncsc-warns-of-emerging-threat-to-critical-national-infrastructure