Exposure of the UK's critical national infrastructure to cyber attacks and ransom demands [1]

Dr R J Chapman[2]

Introduction

Those working on a day-to-day basis on critical national infrastructure (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 unsettled 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[3]. Walker[4] 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.

The requirement for this integration is articulated in an article published by Deloitte[5] which states components such as pumps and valves, may now have operational digital sensors or controls connected via computers to the internet. The article goes on to say :

> *Those digital devices at the edge (sensors, controllers, Internet of Things) are then often linked to the core IT networks (data storage, enterprise software) that may themselves be connected to the wider internet. This convergence of information and operational technology (IT and OT) can make every valve, switch, and pump in a critical infrastructure operation a computer potentially accessible to the internet, vastly increasing the challenge of securing them.*

Projects must also take account of adopting or connecting to legacy operational technology (OT) systems, such as electricity substations, transportation control rooms and their associated industrial control systems legacy systems. The Joint Committee on the National Security Strategy

[1] How to cite this paper: 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.
[2] R J Chapman (Dr Chapman and Associates Ltd)
[3] 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.
[4] Walker, A (1984) "Project Management in Construction", Published by Granada.
[5] Deloitte (2022), as footnote 3.

(JCNSS) within its November 2018 report[6] highlighted that "these bespoke and often legacy industrial control systems, which were not designed with cyber security in mind, are now increasingly networked and connected to the internet to enable more efficient control and real-time monitoring".

At a project level there may be no knowledge of the UK government's recent report issued by the JCNSS[7,8]. It describes the exposure of the country's critical national infrastructure (CNI) to ransomware attacks. Over the annals of time, the report may prove to be a landmark publication. 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"*[9]*.* 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. While the report highlights the country is currently ill prepared for a widespread attack, are current infrastructure projects exacerbating the problem? The purpose of this short paper is to question how well does the report draw attention to the need to ensure specifications (and selected components) of ongoing and planned CNI projects take cognisance of and respond to potential ransomware threats. Additionally, whether the subject warrants further scrutiny by a combination of project sponsors, cyber security specialists, designers and risk analysts.

Ransomware attack

A ransomware is a form of malicious software that enables cyber criminals to remotely lock down, steal, delete or encrypt files on a business's device. Criminals use ransomware to extort money from organisations or companies (a ransom) and will promise to restore access to a company's files or device once it has paid the ransom. Even when the ransom is paid the reinstatement is not always carried out.

Pervasiveness

The pervasiveness of the threat of ransomware attacks was highlighted at a CyberUK conference held in Belfast in April when Oliver Dowden, a Cabinet Office minister, advised attendees Russian

[6] JCNSS (2018) Cyber Security of the UK's Critical National Infrastructure, Section 2 "Protecting CNI against cyber attack: a 'wicked' problem". https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/170805.htm
[7] 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
[8] 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.
[9] Ditto

hackers were seeking "to disrupt or destroy" parts of the UK's critical national infrastructure[10]. In October the government placed a post on the internet[11], which drew attention to the UK being the third most targeted country in the world for cyber-attacks, after the US and Ukraine. 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 includes cyberattacks on critical infrastructure among the 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. The widespread acceptance of the threat and its potential impact is illustrated on the matrix in **Figure 1** below.

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. This belief 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[12]. In 2021 the US fuel pipeline operator Colonial Pipeline, which supplied almost half of the East Coast's fuel, shut down its network following a cyberattack[13]. 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[14]. Of significance is that on 15 November the FBI and the US Cybersecurity and Infrastructure Security Agency issued a joint statement[15] 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."

[10] 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

[11] 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/

[12] Financial Times (2019) "India confirms cyberattack on nuclear power plant" , October https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6

[13] 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/

[14] 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

[15] BBC (2023) "British Library: Employee data leaked in cyber attack". 21 November https://www.bbc.co.uk/news/entertainment-arts-67484639

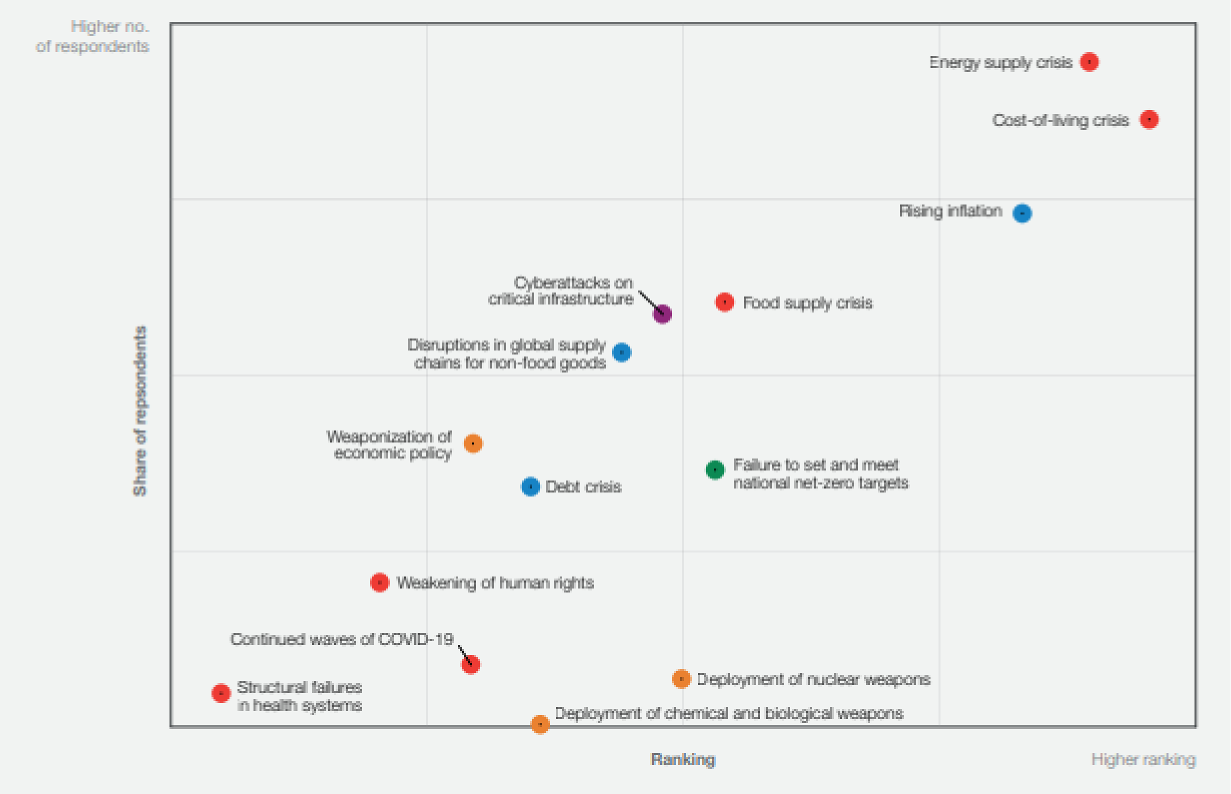


Figure 1: Source- Figure 1.1, World Economic Forum Global Risks, Perception Survey 2022-2023.

The global nature of the threat is reinforced by the press release issued by the Office of Public Affairs (within the U.S. Department of Justice) in 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 hospitals, schools, financial firms, and critical infrastructure. 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.

In April 2023 Dr Marsha Quallo-Wright, National Cyber Security Centre (NCSC), Deputy Director for Critical National Infrastructure, 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 critical national infrastructure, (including energy and telecommunications networks), prevent Chinese state-sponsored hackers from accessing and hiding on their systems[16]. 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

[16] 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

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.

Respondents to the World Forum's report said that artificial intelligence (AI) and machine learning, greater adoption of cloud technology, and advances in user identity and access management (**Figure 2**), will have the greatest influence on their cyber risk strategies over the next two years.

Figure 2: Integration of Artificial Intelligence into CNI

Geopolitical attacks on critical infrastructure

Russia has attracted considerable adverse media coverage for its alleged actions, specifically with regard to Ukraine but also across the globe. Ukraine's independence from Russia has never sat well with Russia's leadership. In December 2015 the Russian digital 'army' made their way into the computers that controlled Ukraine's power grid with the result that hundreds of thousands of Ukrainians were without power for many hours. To complicate things further, the hackers shut down the emergency phone lines. However, this attack was to become overshadowed by what has been described as the most destructive and costly cyberattack in world history[17]. On June 27, 2017, Ukranians woke up to black screens everywhere. They could not get paid, take money from ATMs, buy petrol at petrol stations, pay for a train ticket or buy groceries. Most significantly, they could not monitor radiation levels at Chernobyl. Yet the attack could have been worse. Ukraine was not fully internet connected. Hospitals, chemical plants, oil refineries, gas and oil pipelines, factories, and traffic lights for instance were not 'web-enabled'. In March 2022 the UK issued a press release[18] accusing Russia's Federal Security Service (FSB-the KGB's successor agency) of being behind a historic global campaign targeting critical national infrastructure, including the UK's energy sector. Specifically, it accused the Russian defence ministry subsidiary, the Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM), for an incident involving safety override controls in a Saudi petro-chemicals plant in 2017.

[17] Nicole Perloth (2021), "This is how they tell me the world ends", published by Bloomsbury. Compelling reading!

[18] UK government press release.(2022) "UK exposes Russian spy agency behind cyber incidents. The UK, together with the US and other allies, has exposed historic malign cyber activity of Russia's Federal Security Service (FSB)". 24 March. https://www.gov.uk/government/news/uk-exposes-russian-spy-agency-behind-cyber-incidents.

The malware used against the petro-chemical plant was designed specifically to target the plant's safety override for the Industrial Control System (resulting in 2 emergency shutdowns of the plant) and give the actors complete control of infected systems. The malware had the capability to cause significant impact, possibly including the release of toxic gas or an explosion - either of which could have resulted in loss of life and physical damage to the facility.

Structure of the JCNSS report

The JCNSS report, it could be argued, is broken down into six primary subjects which follow a logical sequence. These are illustrated in **Figure 3** below.

- **The nature of the problem** has been known for some time. However, as the report explains, 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 identified targets and deployed this readymade malicious software to attack victims and then earned a percentage of each successful ransom payment. Typically, after a victim pays, affiliates and administrators split the ransom 80/20. The Hive group mentioned above used this model.

- **The perpetrators.** As highlighted in the JCNSS report, the UK government considers that the majority of ransomware attacks against the UK are from Russian-speaking perpetrators. The FBI confirmed that DarkSide, a group residing within Russia's borders, was responsible for the compromise of the Colonial Pipeline networks[19]. The Conti ransomware cartel thought to run from Russia were reported by the BBC to be behind the Costa Rica attack[20]. As reported in the Financial Times[21], cyber specialists considered the attack on the India nuclear power station was the work of the Lazarus Group, known to have ties to two North Korean backed groups.

- **Where are we now.** 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 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

[19] CNN (2021) "What we know about the pipeline ransomware attack: How it happened, who is responsible and more". https://edition.cnn.com/2021/05/10/politics/colonial-ransomware-attack-explainer/index.html

[20] BBC Technology (2022) "President Rodrigo Chaves says Costa Rica is at war with Conti hackers", 18 May. https://www.bbc.co.uk/news/technology-61323402

[21] Financial Times (2019) "India confirms cyberattack on nuclear power plant" , October https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6.

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*"

Of particular concern are the resource constrained sectors such as health and local government. Supply chains are also thought to particularly vulnerable and have been described by the NCA as *the 'soft underbelly'* of CNI. Projects now have to collaborate with even more manufacturers, suppliers and contractors to maintain cyber resilience.

While not addressed by the report, of significance is the Product Security and Telecommunications Infrastructure Act 2022 (PSTIA), which the government declares is a "government bill to make provision about the security of internet-connectable products and products capable of connecting to such products; to make provision about electronic communications infrastructure; and for connected purposes". In simple terms relevant connectable products are those that are internet-connectable or network-connectable (and hence ultimately connectable to the internet).

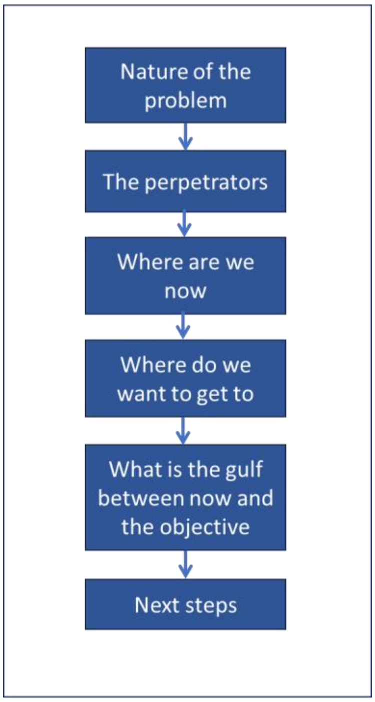

Nature of the problem
The perpetrators
Where are we now
Where do we want to get to
What is the gulf between now and the objective
Next steps

Figure 3: Structure of the report-
A hostage to fortune: ransomware and UK national security

- **Where do we want to get to.** It is suggested here that considerations of future ransomware attacks should influence the design and specification of current ongoing and future CNI projects so that vulnerability is not exacerbated.

- **Possible next steps.** The JCNSS has identified a number of options for the government to pursue. Some of the suggestions are as follows. Reform the Computer Misuse Act 1990 (CMA). Establish crypto-asset trace and seizure, to reduce the incentives for criminals and to claw back some of the financial losses experienced by ransomware victims. Creation of a partnership between the intelligence agencies and the NCA to deploy a full-spectrum response to the ransomware threat. Explore the possibility of imposing legal sanctions through international cooperation to deter state-linked ransomware crime. Increase resilience. It is suggested here that over and above the numerous suggestions of the JCNSS, the scope of CNI projects and particularly their components will dictate the vulnerabilities of the future and hence must feature in any vulnerability assessments.

What is Critical National Infrastructure

According to the UK government's National Protective Security Authority (NPSA), the countries 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 as:

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

Table 1: 13 national infrastructure sectors.

The UK's Critical National Infrastructure (CNI) has become increasingly interconnected and interdependent[22], 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 NCSC and the 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*. This interconnectedness can be international. An example is that German wind farm operation is dependent on satellites operated by the United States.

Initiatives

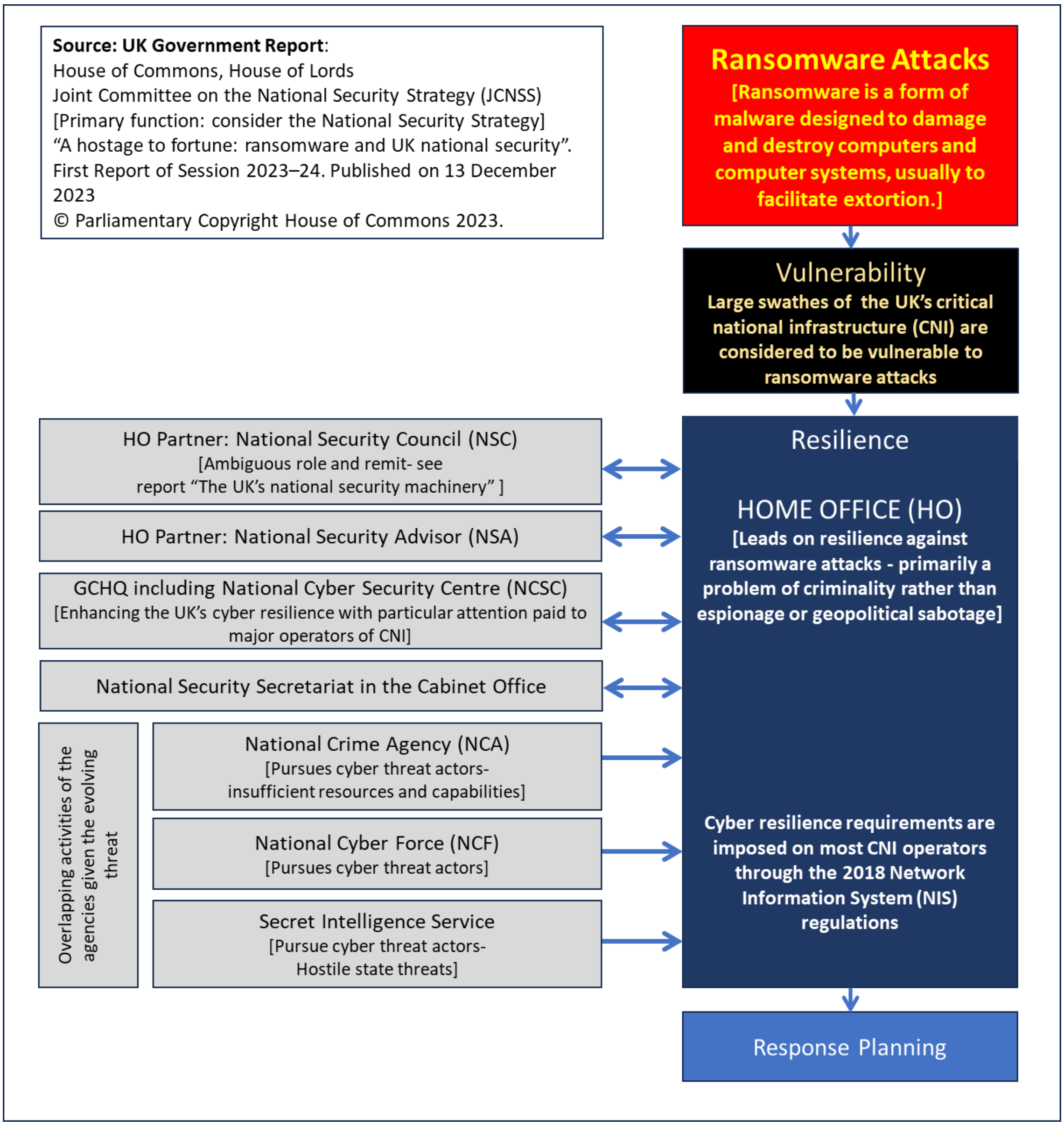
The JCNSS report follows on the heels of alerts issued by the NCSC including the alert titled: "Heightened threat of state-aligned groups against western critical national infrastructure" issued in April 2023 and referred to above. The alert sought to highlight the emerging risk posed by state-aligned 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[23]. 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

[22] https://www.ncsc.gov.uk/files/Criticalities-and-CNI-Knowledge-Base-Industry-Flyer.pdf
[23] NCSC, BEIS & CPNI (2022) "Joint Ventures in the Construction Sector: Information Security Best Practice Guidance", August

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).

Contributing parties to resilience within UK government

The report describes the contributing parties to supporting resilience against cyber attacks however it is difficult to absorb who the parties are, their role, their capabilities-and how they coordinate their efforts. **Figure 4** below attempts to describe the UK government organisations (which are providing state protection against ransomware) and their relationship to the Home Office which currently occupies the lead role. However, the relationships in particular are difficult to quickly decipher from the report.



Source: UK Government Report:
House of Commons, House of Lords
Joint Committee on the National Security Strategy (JCNSS)
[Primary function: consider the National Security Strategy]
"A hostage to fortune: ransomware and UK national security".
First Report of Session 2023–24. Published on 13 December 2023
© Parliamentary Copyright House of Commons 2023.

Ransomware Attacks
[Ransomware is a form of malware designed to damage and destroy computers and computer systems, usually to facilitate extortion.]
Vulnerability
Large swathes of the UK's critical national infrastructure (CNI) are considered to be vulnerable to ransomware attacks
Resilience
HOME OFFICE (HO)
[Leads on resilience against ransomware attacks - primarily a problem of criminality rather than espionage or geopolitical sabotage]
Cyber resilience requirements are imposed on most CNI operators through the 2018 Network Information System (NIS) regulations
Response Planning
HO Partner: National Security Council (NSC) [Ambiguous role and remit- see report "The UK's national security machinery"]
HO Partner: National Security Advisor (NSA)
GCHQ including National Cyber Security Centre (NCSC) [Enhancing the UK's cyber resilience with particular attention paid to major operators of CNI]
National Security Secretariat in the Cabinet Office
Overlapping activities of the agencies given the evolving threat
National Crime Agency (NCA) [Pursues cyber threat actors- insufficient resources and capabilities]
National Cyber Force (NCF) [Pursues cyber threat actors]
Secret Intelligence Service [Pursue cyber threat actors- Hostile state threats]

Figure 4: Participating UK government organisations supporting resilience

Clarity required by PLC boards

CNI is largely provided by the private sector. Existing infrastructure as expected is composed of new and legacy systems. Preserving the security of CNI may be exacerbated by board member's comprehension of accountabilities and responsibilities of the organisations' departments and how a cyber attack may unfold. There is a perception that decision making within boards may compromised due to a lack of understanding of who within their organisation is responsible for the security of their organisations' operational technology (OT) [24]. This may be result from a lack of knowledge about the ways in which informational technology (IT) and OT policies are coordinated and how these teams interface with each other. As highlighted by the ABS Group[25], it is common for the roles of IT and OT professionals involved in security, to differ. While IT teams focus on data control based on information security policies (reliability, integrity, and availability) and the prevention of data breaches, OT teams are responsible for the security of the physical controls in installations (ensuring that operations remain active and uncompromised). Any breach of an OT network can impact critical infrastructure, put human lives at risk, disrupt public services and affect the national economy.

Summary

This report has recorded the prevalence of ransomware attacks and their impact should they materialize. Following the UK government's release of its report on the exposure of country's critical national infrastructure (CNI) to ransomware attacks, this paper questions how well does the report draw attention to the need for information and technology to be integrated with project design to ensure specifications (and selected components) of ongoing and planned CNI projects take cognisance of and respond to potential ransomware threats. In addition, it poses the question whether the subject warrants further scrutiny by a combination of project sponsors, cyber security specialists, designers and risk analysts.

For readers of the JCNSS report it is difficult to clearly understand the government departments involved in providing resilience, their specific role and how their efforts are coordinated across government.

Previous research by the lead author

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

- "The SME business guide to fraud risk management" published by Routledge in 2022 (see Appendix 1 below)

[24] Forbes (2023) "Critical Infrastructure: Why It's The New Target For Cybercriminals A Discussion With Ian Bramson" 10 January. https://www.forbes.com/sites/forbesbooksauthors/2023/01/10/critical-infrastructure-why-its-the-new-target-for-cybercriminals-a-discussion-with-ian-bramson/

[25] The ABS Group declares it "provides data-driven risk and reliability solutions and technical services that help our clients confirm the safety, integrity, quality and environmental efficiency of their critical assets and operations".

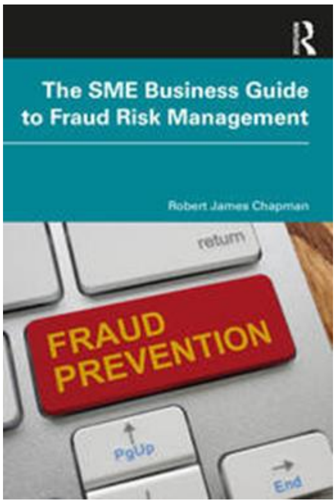
- Chapman, R. J. (2022). Update: the exposure of small UK project management organisations to fraud; PM World Journal, Vol. XI, Issue IX, September. https://pmworldlibrary.net/wp-content/uploads/2022/09/pmwj121-Sep2022-Chapman-exposure-of-small-uk-pm-organisations-to-fraud-update.pdf

- 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

Appendix 1: The SME business guide to fraud risk management



Publisher: Routledge; 1st edition (27 April 2022)

Language: English

ISBN 9781032055466

Author: Robert James Chapman

Primary Reviewer: Matthew Collantine

Formats: Paperback (and also Hardback)

Available from: Amazon

Currently available from numerous booksellers in England, America, France and Germany

Book Description

All organisations are affected by fraud, but disproportionately so for SMEs, given their size and vulnerability. Some small businesses that have failed to manage business fraud effectively have not only suffered financially but also have not survived. This book provides a guide for SMEs to understand the current sources of business fraud and the specific risk response actions that can be taken to limit exposure, through the structured discipline of enterprise risk management.

The book provides:

- A single-source reference: a description of all of the common fraud types that SMEs are currently facing - in one location.
- An overview of enterprise risk management: a tool to tackle fraud, as recommended by the Metropolitan Police Service and many other government-sponsored organisations.
- Illustrations of fraud events: figures (where appropriate) of how frauds are carried out.
- Case studies: brief case studies of the fraud types described, (to bring the subject to life and illustrate fraud events and their perpetrators), enabling readers to be more knowledgeable about the threats.
- Sources of support and information: a description of the relationship between the government agencies and departments.
- What to do: 'specific actions' to be implemented as opposed to just recommending the preparation of policies and processes that may just gather dust on a shelf.

The book gives SMEs a much better understanding of the risks they face and hence informs any discussion about the fraud prevention services required, what should be addressed first, in what order should remaining needs be addressed and what will give the best value for money.

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. 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.