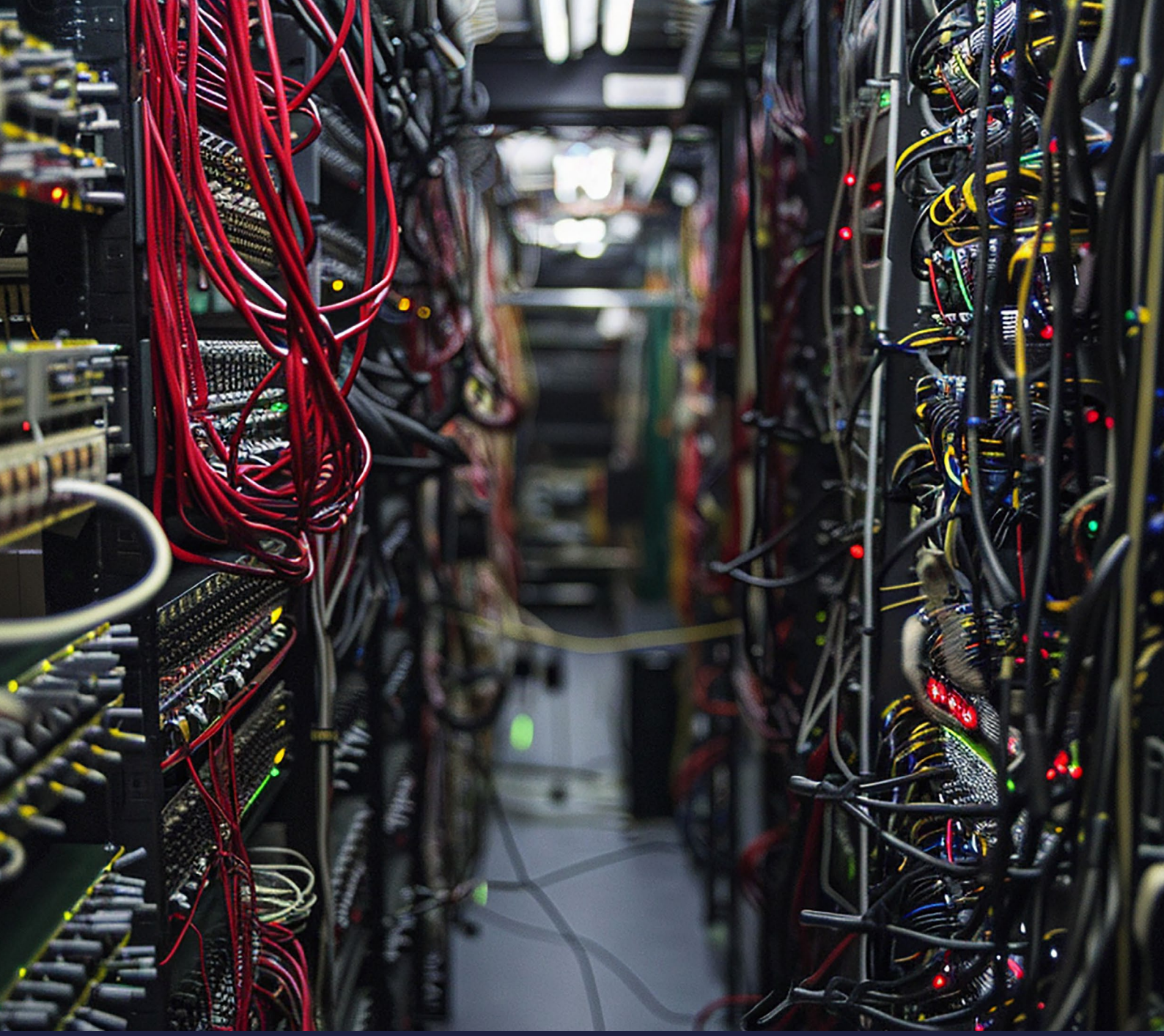


Update Critical

Counting the cost of cybersecurity risks from End-of-Life technology on Critical National Infrastructure

November 2025

WPI STRATEGY

CISCO

Contents

About WPI Strategy

WPI Strategy is a specialist public affairs consultancy, focused on combining economic research with political advocacy. We provide a range of private and charitable clients with research and advice to deliver better outcomes through improved public policy design and delivery.

wpi-strategy.com @wpi_strategy

Foreword

With unsettling regularity, global and regional headlines report on attackers successfully penetrating critical infrastructure systems that deliver essential services to the general public. The rapid pace of cybersecurity innovation, customer investments in technology and concerted efforts by industry and governments to encourage secure by design and secure by default approaches, has improved defences. However the frequency and impact of these attacks continues to grow and remains a significant concern.

You might expect that these attacks are being mounted by advanced persistent threat actors using exquisitely designed tools that exploit novel "zero day" vulnerabilities. The reality is that even well-resourced adversaries often gain initial access through relatively simple means—such as unpatched network devices, mismanaged credentials, or IT equipment that is so obsolete that it cannot even be effectively updated or secured—rather than through highly sophisticated exploits.

Of particular concern is the ongoing challenge presented by the over-reliance on technology beyond its supported lifespan—meaning that the software can no longer be patched when new security flaws are discovered. Technology at the boundary edge of networks is particularly subject to attack because it is by its very nature exposed to a dynamic threat environment and must be regularly supported, maintained, and patched.

At Cisco, we are strongly focused on ensuring that the technology we develop is secure by design and as a default—so that exploitable vulnerabilities become rarer over time—and we are committed to clear communication when discovered bugs require patching or other mitigations. However, as WPI Strategy's report notes, the initial point of entry for attackers launching debilitating cyberattacks often involves IT that is unpatched or too old to patch. This is known as "technical debt"— the shadow liability from outdated technology that cannot be patched or operated securely.

And like any debt, the more you ignore it, the more it grows.

Our discussions with WPI Strategy began with the aim of helping shed light on the size and scope of technical debt faced by many operators of essential services. Early in the course of our discussions, we identified a gap in available economic data that could serve as a foundation for measuring the problem or developing metrics to support policy solutions. We believe this report offers a novel and important perspective on how to think about this problem.

The authors examine and compare how end-of-life risks vary across a series of key markets and critical sectors within those markets, which can guide other policymakers on where to focus their efforts most urgently. We hope WPI Strategy's work will be a catalyst for action—inspiring all stakeholders to continue working together to ensure that digital networks remain efficient, effective, and secure.

Jeff Campbell, SVP and Chief Government Strategy Officer, Cisco

Executive Summary

The growing digitisation of economies and the speed at which cybersecurity risks are evolving present a range of technology challenges for cybersecurity leaders. Given this context, tackling outdated technology and the vulnerabilities it offers would-be attackers is just as important as keeping up with new technology.

Those risks are even more acute when considering how technology impacts the running of critical national infrastructure (CNI), covering sectors as diverse and as crucial to the economy and society as financial services to the water sector. Cyberattacks in these sectors can have widespread impacts on national security, economic security, and public safety. In some sectors like energy or finance, the disruptions caused by a cyberattack are likely to be felt almost immediately, with the potential for the impact to be felt across a number of sectors. In other areas, like healthcare, a critical challenge will be the time needed to recover.

A key turning point is when old technology turns into obsolete technology which has reached an End-of-Life (EoL) state. Crucially, at this point its security is no longer being supported by vendors and any vulnerabilities no longer addressed.

The exact exposure of CNI systems to EoL technology is difficult to determine, however industry estimates in 2020 were that globally, across business network infrastructure, almost half (48%) of assets were ageing or obsolete.[1] Importantly, we know the technical debt (see glossary) associated with this obsolete technology is a growing and costly problem.

That growing cost and increasing risk alone should see countries seek to adopt a more active approach to tackling the presence of EoL technology in their systems. Tackling this technical debt would also move countries towards a more systematic and preventative approach to cybersecurity. 60% of EU cyber breaches in 2022-2023 exploited known vulnerabilities for which there were patches, but which had not been applied.

Governments and CNI operators around the world face increasing IT budgets, frequently aimed at maintaining aging systems, rather than remediating them. Current funding approaches to public sector IT projects in many countries end up encouraging underinvestment and de-prioritisation of remediation. This leaves governments servicing increasing technical debt, rather than investing in cybersecurity enhancements or innovations.

This research, produced by WPI Strategy and commissioned by Cisco, looks to understand the relative international exposure to EoL technology on key CNI sectors. We have modelled five key CNI sectors: Water, Healthcare, Manufacturing, Energy and Finance. Our work has also looked to assess what common lessons can be learned from the different national approaches in four key geographies: US, the EU (focusing our analysis on Germany and France), UK and Japan.

Our modelling provides a new perspective on how policymakers and infrastructure operators should think about the risks EoL technology poses, allowing them to compare their situation to other advanced economies.

1 NTT (2020), Global Network Insights Report, Lifecycle management infographic, https://services.global.ntt/-/media/ntt/global/insights/2020-global-network-insights-report/pdfs/lifecycle-management.pdf?rev=52283ff43bc0499c97e277f16f77bf6b

At a national level, our research indicates the following relative national risk scores for the countries we have assessed:

	Country	EoL Risk Score
	United Kingdom	92.0
	United States	88.0
EU	Germany	87.8
EU	France	83.0
	Japan	65.0

The UK has the highest relative risk score out of the countries we have assessed, with particularly high-risk scores for the UK's healthcare, energy and water sectors. This reflects the UK's relatively high exposure to EoL technology and that UK CNI sectors are relatively highly concentrated, which increases the impact of cyber incidents.

This contrasts with Japan's significantly lower score. This is due to their lower national exposure to EoL technology, their less centralised infrastructure base and a stronger, more consistent national focus on digital resilience.

Across the five countries we have assessed, the variation in risk scores between sectors points to areas of key vulnerabilities. For instance, healthcare stands out as a key area of vulnerability across all the countries assessed, reflecting both the real impact of cyberattacks on healthcare systems and the sector's exposure to EoL technology. As an illustration of this exposure, a 2022 industry survey found 60% of French hospitals still used Windows 7 systems, even though security updates for that system had ended in 2020.

Our work aims to provide policymakers with a picture of the reduction of cybersecurity risk that could be achieved if the problem of EoL technology was more actively managed. We have identified four lessons governments should focus on if they want to seriously tackle this critical challenge:

Lesson 1. **Without more active requirements on CNI operators to manage of EoL technology, governments risk growing hidden cyber risks.**

Lesson 2. **The funding model for dealing with obsolete technology needs to change, it is too often geared towards servicing technical debt, rather than its remediation.**

Lesson 3. **Guidance on managing technology lifecycles should be clearer and explicit about tackling the challenge of EoL technology.**

Lesson 4. **Governments should encourage more transparency and information sharing, to build more awareness and active handling of threats and vulnerabilities.**

To this end, we make the following recommendations -

1. **CNI operators should be responsible for maintaining live technology asset registers, alongside standardised lifecycle management and risk assessment requirements.**
   This would encourage operators to proactively identify technology assets reaching a near EoL state. Having identified these assets, an assessment can be made as to whether to invest to replace, or to put in place active risk management procedures.

2. **Governments should adopt a more active policy approach to managing EoL technology in critical national systems. This could be achieved through a range of approaches:**

   - **Procurement – Encouraging minimum cyber hygiene standards from vendors and IT partners.** This would encourage services like regular patching to be incorporated into procurement contracts.

   - **Procurement – Reforming approaches to IT investment to encourage innovative partnerships to enhance maintenance and servicing of systems.** This would support the rebalancing of IT budgets away from servicing technical debt, towards active patching and replacement.

   - **Funding – Explore opportunities to pilot and prioritise 'rip and replace' programmes for EoL technology.** Given the scale of the challenge within IT systems, there is an opportunity to both pilot programmes to specifically tackle EoL technology where they don't already exist and prioritise EoL in the programs that do exist. A focus on funding incentives to prioritise the highest-risk EoL technology would reduce risks significantly. Programmes could look at how to support both the direct replacement of assets and transitional support where feasible.

   - **Regulation - Ensuring that where policymakers have voluntary or mandatory incident reporting mechanisms in place, they collect data on the involvement of EoL technology and provide post-incident analysis on its impact on the severity of the incident.** Incident reporting requirements should be risk-based, proportional, and enable the use modern cybersecurity approaches including machine-generation and automation cyber tools. Ensuring greater transparency and cross-sector early warning related to technology beyond its supported lifespan would support operators.

   - **Visibility – Encourage industry-wide data sharing frameworks and standards.** Establishing greater data sharing between sectors would improve the visibility of threats and make early warning of known vulnerabilities easier.

   - **Developing industry requirements further – explore how new advances in AI can support more efficient approaches to update deployment.** Reducing Mean Time to Patch (MTTP) decreases risk by narrowing the window malicious actors have to exploit vulnerabilities. Automatic security updates, however, are not suitable for all operational environments, particularly for highly critical systems where deploying under-tested patches present unacceptable service disruption risks. As such, there should be further work to explore new advances in AI can support operators with that allow for real-time testing and deployment of patches, and for the isolation, segmentation, and protection of technologies that cannot be immediately patched or replaced if unpatchable.

These recommendations are aimed at supporting governments and CNI operators tackle this important but underappreciated area of cyber risk. Adopting measures like these would both provide a better picture of where those risks exist but also focus operators' attention on managing their assets.

Crucially, actively tackling EoL technology offers governments a clear route to raising cyber resilience across critical sectors of the economy by tackling vulnerabilities before they can be exploited.

CHAPTER 1

Introduction

The growing digitisation of economies and the speed at which cybersecurity risks are evolving present a range of technology challenges for cybersecurity leaders. Given this context, tackling outdated technology and the vulnerabilities it offers would-be attackers are just as important as keeping up with new technology.

The risk of cyberattacks on critical national infrastructure (CNI), covering sectors as diverse and crucial to life as financial services to the water sector, should be of critical concern. Cyberattacks in these sectors can and do cause significant and longstanding harm to national security, economic security, and public safety.

The threat actors launching these attacks are able to do so by simply looking for exploitable vulnerabilities in systems, wherever they can find them. So, the clear strategy should be to minimise and harden the 'threat surface', e.g. all the potential points of vulnerability that attacks can use to gain entry, disrupt or damage systems.

A key turning point is when old technology turns into obsolete technology which has reached an End-of-Life (EoL) state. The challenge the presence of obsolete technology in systems presents is that it gives threat actors an ongoing avenue for attacks and can lead to greater damage since the technology is harder for system operators to manage and therefore detect, respond and recover from attacks.

That is why technology companies are continuously updating their products and producing 'patches', fixes that are intended to eliminate vulnerabilities.

This is something that most of us now experience in our everyday lives. Most consumers have learnt the value of regularly updating their personal technology devices and the software that runs on them, whether proactively or just through the sheer weight of prompting. In many cases, this process is automatic and requires little personal effort.

The challenge for system operators is much harder, requiring significantly more effort. IT teams actively need to prioritise, test and deploy updates throughout their systems. The effect of this challenge is that countries and their critical national infrastructure are seeing an enormous cost build up in maintaining and living with 'legacy systems'.

The end-of-life problem

Calling this technology by the commonly used term 'legacy' technology can be deceptive. At this point, the technology can still be functioning and used within systems as intended.[1]

A bigger problem is when technology has become so old and obsolete that it can no longer be supported against security risks. It has reached the end of its life. Technology naturally has a lifespan, so once legacy technology reaches its 'end-of-life' state, the risks to the overall cyber resilience of the system multiply.

1 Art 3 of the EU's Digital Operations Resilience Act 2022 defines 'legacy ICT system' in this way, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=FR, as does the UK government's 2019 'Managing legacy technology' guidance, https://www.gov.uk/guidance/managing-legacy-technology#defining-legacy-technology.

End-of-Life technology is technology, hardware or software, commonly understood to be:

- **Out of support from the supplier** – meaning that it is unsuitable for, or that IT suppliers no longer provide, security patches, fixes or technical support, or
- **Impossible to update** – meaning that IT suppliers or third parties are no longer able to extend the life of obsolete technology.

This technology therefore presents higher risk within systems – above the acceptable risk thresholds for cybersecurity.

It is the increased risk presented by EoL technology that should catapult this from being a managed IT systems architecture issue to a cybersecurity issue with national ramifications. In 2023, hackers were able to exploit widely used productivity tool that had reached an EoL state to gain access to at least two US federal agencies.[2]

2 CISA (2023), Cybersecurity advisory, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-339

Critical national infrastructure (CNI)

A key area for this concern should be CNI sectors. These are sectors within a country whose infrastructure is so vital to national wellbeing that a cyberattack on them could have a significant effect across national security, economic security, and public safety.

Every country designates sectors it considers critical. These typically include sectors as broad as water, energy, government services, public health, transportation, financial services, food and communications. Alongside governments, these sectors involve thousands of public and private organisations responsible for delivering both the infrastructure itself and the services that surround it.

Digital systems increasingly underpin this infrastructure, underlining the importance of protecting it against cyber threats. The European Union Agency for Cybersecurity (ENISA) has defined the 'criticality' of sectors based the socio-economic impact of a significant incident in the sector, the potential to cause disruptions in other sectors, the reliance on information and communication technology (ICT) and a measure of how long it would take for the impact of an attack to be felt, described as 'time-criticality'. Their scoring of different EU sectors illustrates how important ICT is for these sectors.

Sector	Socio-economic impact	Dependency on ICT	Time-Criticality	Score average
Electricity	**10**	**8**	**10**	**9.3**
Banking	**7**	**9**	**9**	**8.3**
Drinking water	**3**	**4**	**6**	**4.3**
Telecoms	**9**	**10**	**10**	**9.7**
Health	**8**	**10**	**8**	**8.7**

Source: ENISA's Cybersecurity Maturity and Criticality Assessment of NIS2 sectors - 2025

These are not just potential risks. Since 2000, the European Repository for Cyber Incidents has recorded 1499 cyberattacks on critical infrastructure worldwide; however, it notes that this is just the "visible tip of the iceberg" since these are just publicly reported incidents.[3] 90% of EU entities in critical sectors expect an increase in cyberattacks in 2025.[4]

3 EUREPOC, Critical Infrastructure Tracker, https://cit.eurepoc.eu

4 ENISA (2024), NIS Investments report 2024, https://www.enisa.europa.eu/sites/default/files/2024-11/CSPA%20-%20NIS%20Investments%20-%202024_0.pdf

Cyberattacks on CNI sectors have real consequences to the health, security and economy of nations. The economic and human cost of cyberattacks on critical national infrastructure can be extensive and severe. Last year, an attack on a provider of UK health services, Synnovis, affected more than 11,000 patients and had a total cost of £32.7 million.[5]

Cyber threats to CNI are real-world national threats

High-profile incidents, alongside growing global tensions and coordinated threats, reflect a real risk that countries are choosing to live with 'known holes in fences' throughout their CNI networks.

The UK's National Cyber Security Centre has highlighted "a widening gap between the increasingly complex threats and our collective defensive capabilities in the UK, particularly around our critical national infrastructure".[6]

For example, a 2022 industry survey found 60% of French hospitals still used Windows 7 systems, even though security updates for that system had ended in 2020. [7]

These are vulnerabilities that are being exploited. In February 2024, the multilateral Joint Cybersecurity Advisory released advice that the Chinese state-sponsored cyber group called Volt Typhoon had compromised multiple critical national infrastructure sectors in the US, including communications, energy, transportation and water.

The four immediate actions highlighted in that advice both started with 'Apply patches for internet-facing systems' and ended with 'Plan "end of life" for technology beyond manufacturer's supported lifecycle'.[8]

"There has been far too little public focus on the fact that PRC-hackers are targeting our critical infrastructure, our water treatment plants, our electrical grid, our natural gas pipelines, our transportation systems, and the risk that poses to every American poses our attention …now.

Just this morning we announced an operation where we and our partners identified hundreds of routers that had been taken over by the PRC state-sponsored hacking group known as Volt Typhoon.

Let us be clear. Cyber threats to our critical national infrastructure represent real world threats to our physical safety."

Then FBI Director, Christopher Wray, in evidence to US Congress, House Select Committee on China, January 2024

5 NHS England (2024), Update on cyber incident: Clinical impact in south east London , https://www.england.nhs.uk/london/2024/09/26/update-on-cyber-incident-clinical-impact-in-south-east-london-thursday-26-september-2024/

6 NCSC (2024), NCSC Annual Review, https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024/chapter-01/staying-in-the-race

7 BPI France (2025), Cybersecurity in health: Where are we? [in French], https://bigmedia.bpifrance.fr/nos-dossiers/cybersecurite-en-sante-ou-en-sommes-nous

8 CISA (2024), PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

EU experts have placed 'human error and exploited legacy systems' and 'exploitation of unpatched and out-of-date systems within overwhelmed cross-sector tech ecosystems' as the third and fourth most important cybersecurity threat through to 2030.[9] It ranked above other threats including 'abuse of AI' (no. 9) and 'targeted attacks' (no.12).

In addition, 60% of EU cyber-attack breaches in 2022-2023 exploited known vulnerabilities for which there were patches, but which had not been applied. [10] This underlines the need for a greater focus on asset management and cyber hygiene by system operators, as discussed below.

Understanding the EoL challenge

Whilst legacy technology has been much discussed and is a well understood problem, practical approaches to dealing with EoL technology have been relatively underdiscussed.

Yet addressing EoL technology should be a key part of CNI cybersecurity strategies.

How products become "End of Life" and come out of the market.

Currently information about hardware and software product life cycles is often fragmented and inconsistent. There are industry efforts looking to standardise how information is shared.

The OpenEoX model establishes four common stages [11]:

1. **General availability** – This is a published notice establishing a product's initial release.
2. **End-of-Sale** – This published notice establishes the last day when a particular product can be ordered by a consumer from a vendor. The product may still be supported by the vendor after this date. Customers may still be able to get the product from other sources.
3. **End-of-Security-Support** – This is the last day for when the vendor has committed to providing security remediations, fixes or patches, for the product.
4. **End-of-Life** – This is the last day when the vendor provides support in any way for the product.

The benefits of this standardised approach include:

- The ability for vendors to communicate clearly with customers about a product's lifespan.
- Enabling easier integration with industry tools and platforms, enabling greater automation in the monitoring of product lifespans.
- Providing greater transparency and a more predictable environment for product support.

9 ENISA (2024), Foresight Cybersecurity Threats For 2030 – Update, March 2024. https://www.enisa.europa.eu/sites/default/files/2024-11/Foresight%20Cybersecurity%20Threats%20for%202030-Update-fullreport_en_0.pdf

10 ENISA (2024), NIS Investments 2024, https://www.enisa.europa.eu/sites/default/files/2024-11/CSPA%20-%20NIS%20Investments%20-%202024_0.pdf

11 Oasis (2025), A Standardized Framework for Managing End of Life and other Product Lifecycle Information, https://docs.oasis-open.org/openeox/standardization-framework/openeox-standardization-framework-technical-report.pdf

Effectively dealing with EoL technology directly addresses two major cybersecurity issues:

- **Encouraging greater asset management and cyber hygiene** - putting in approaches that regularly patch and update technology as standard practice, hardening the threat surface that bad actors face; and
- **Proactively tackling risk through remediation** – rather than responding to incidents alone, remediation enables system owners to anticipate and reduce potential risks by planning and dealing with obsolescence proactively.

This is important for a third reason: newer technology products typically share some common code base with older technology. This means that new patches for current technology can be used to expose vulnerabilities in that common code base shared with obsolete technology.

Threat actors can reverse engineer new patches to identify the initial vulnerability and develop exploits. The risk to unpatched newer equipment (emphasising the importance of ensuring assets are maintained and up to date) is compounded by the risk to the older unsupported products that are vulnerable to the same exploit because they share the same code base.

Part of the ongoing challenge in tackling this issue has been the uncertainty about how much of a contribution does EoL technology play in cyber threats on CNI.

This WPI Strategy research, commissioned by Cisco, seeks to explore this further by looking at the relative potential impact of EoL technology on key CNI sectors in four key geographies: US, the EU, UK and Japan.

We then look at what countries can practically learn from the approaches taken in these geographies to protect and build the cyber resilience of their CNI.

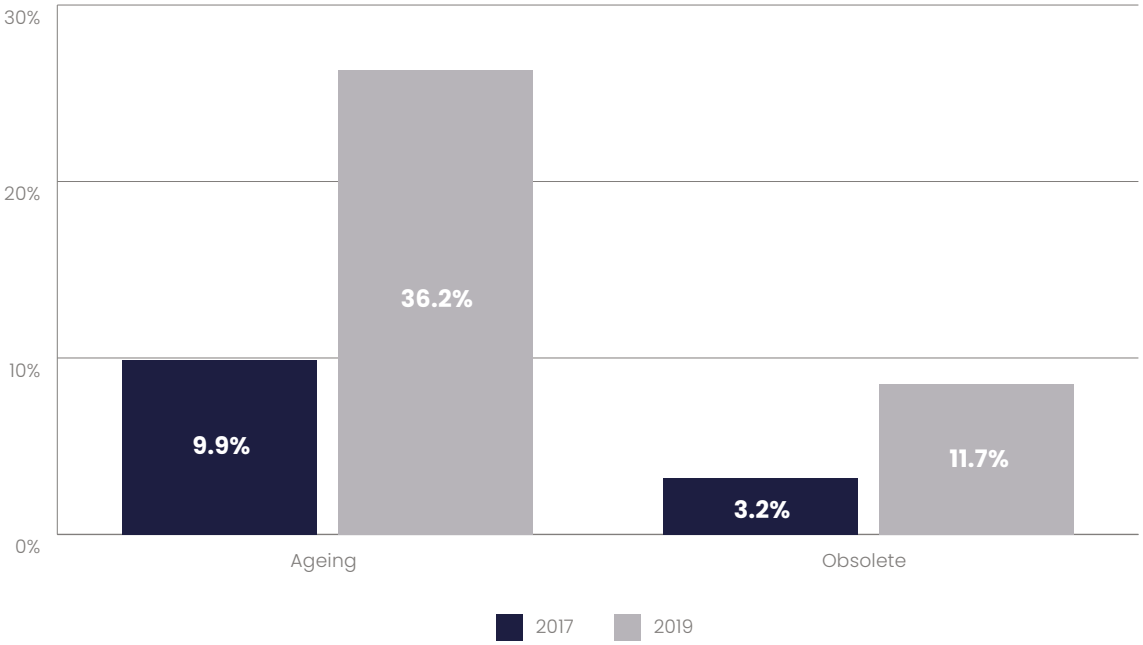
CHAPTER 2

A growing, costly problem

The scale of the legacy mountain

A 2020 study by NTT found that businesses were facing a three-fold growth in old or obsolete assets between 2017-19.[1]

The growth in ageing assets



Source: NTT 2020 Global Network Insights Report

But the growing scale and prevalence of legacy technology within CNI systems represents a different scale and a growing mountain of a problem.

In 2024, 228 legacy IT systems were identified across UK Government departments, with over 1-in-4 of those "red rated" with a high likelihood and impact of operational and security risks occurring. [2]

Similarly, a 2019 US Government study analysed 65 systems most in need of modernisation across 24 federal agencies. The age of the 10 most critical systems in that study were between 8-51 years old. Whilst the modern IT industry has been focused on cloud computing and AI services, many of these critical systems still rely on much older technologies and programming languages, like assembly and COBOL.[3]

1 NTT (2020), 2020 Global Network Insights Report (infographic), https://services.global.ntt/-/media/ntt/global/insights/2020-global-network-insights-report/pdfs/2020-global-network-insights-report-overarching-infographic.pdf

2 NAO (2024), Government cyber resilience, https://www.nao.org.uk/wp-content/uploads/2025/01/government-cyber-resilience.pdf

3 GAO (2019), Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems, https://www.gao.gov/assets/gao-19-471.pdf

This isn't uncommon. The UK's Police National Computer is 51 years old and has been in service since its inception in 1974.

In many CNI systems, approaches to managing legacy operational technology poses an additional challenge. In the US, there are 170,000 water systems; across these systems older technology has been overlaid with digital technology but was never intended with smart functionality or the hyperconnectivity of the newer technology in mind.[4] A US Government study in 2024 found that some operators preferred not to install updates that could disrupt legacy systems and interrupt operations.[5]

The cost of legacy

The need to tackle this widespread challenge is thrown further into focus when considered against the national cost of IT and cyber investments, which is significant and growing.

Costs are rising and the proportion of spending needed to maintain systems is a significant issue. In 2023 the US federal government spent $100 billion on IT and cyber-related investments.[6] Estimates are that $80 billion of this will be spent on operating and maintaining existing systems including legacy systems, an increase of 12% on 2021 spending.

And in 2024 the US government planned to increase spending on cybersecurity by 13% over the previous year, with $12.1 billion allocated in the pursuit of the National Institute for Standards and Technology's (NIST) cybersecurity core functions: Identify, Protect, Detect, Respond and Recover.[7] [8]

Technical debt

The ever-increasing costs of maintaining aging technology should focus policymakers on whether they are making the right investment decisions. The need for increased budgets needs to go hand in hand with tackling a key problem of how investments are made when it comes to IT spend by both public and private critical national infrastructure operators.

Public sector IT projects have tended to focus on capital investment in owned hardware/software, with maintenance costs dealt with as operating expenditure. With continued pressure on finding savings in public sector budgets, that encourages a tendency towards short-term savings on operating costs. This forgoes the benefits of managing technology and stores up more costly, long-term maintenance.

4 Cisco, How do OT and IT differ?, https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html

5 GAO (2024), Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems, https://www.gao.gov/assets/gao-24-106744.pdf

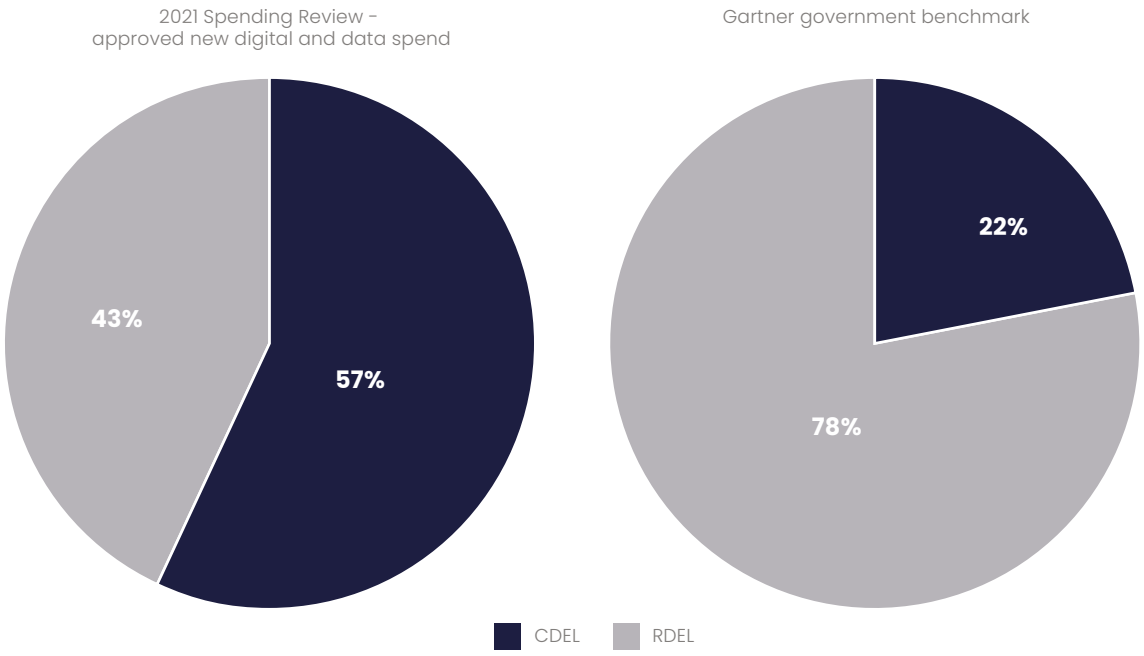
6 GAO (2023), Agencies need to continue to address critical legacy systems, https://www.gao.gov/assets/gao-23-106821.pdf

7 Federal News Network reporting (2023), https://federalnewsnetwork.com/budget/2023/03/federal-it-spending-in-2024-request-up-by-13-in-part-thanks-to-cyber-cx-plans/

8 The current NIST Cybersecurity Framework (2.0), published in 2024, has expanded the framework's core functions to include a sixth function, Govern, which addresses an organisation's cybersecurity risk management strategy. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

In the UK, the Government has identified the challenges this poses. Budgets and plans are frequently buffeted by the demands of new policy. The focus is on 'build', with too little investment in 'run'. The result of this is that operating budgets accounted for less than half of total digital and data funding in the UK's 2021 spending plans, a decrease from the previous settlement. That contrasts with the ratio of capital (22%) vs operational expenditure (78%) amongst peers.[9]

Build vs Run



Source: UK Government 2025, State of Digital Government Review

This approach has resulted in two major challenges:

- **An increase in the proportion of spending going on maintenance, rather than modernisation or enhancement.**

  In the US, between 2010 and 2017, spending on operating and maintenance (O&M) increased by 9%. By 2017, 77% of the US Federal IT budget was O&M spending. In the UK, nearly half of the government's 2019 planned £4.7 billion IT spend was focused on keeping legacy systems running.

- **Poor financial planning and underfunding of remediation.**

  The challenge to public finances has encouraged under-investment in remediation, a persistent problem. In the UK, the National Audit Office found that Government departments did not have fully funded plans to remediate around half (53%) of its legacy IT assets, "leaving these systems increasingly vulnerable to cyber-attack".[10]

9 UK Government (2025), State of Digital Government Review, https://www.gov.uk/government/publications/state-of-digital-government-review/state-of-digital-government-review

10 NAO (2025), Government Cyber Resilience, p12, https://www.nao.org.uk/wp-content/uploads/2025/01/government-cyber-resilience.pdf

Overall, the cost of maintaining aging technology can be seen as two-fold: a "technical debt" paid by having to manage outdated devices and software, and a "tax" against deploying enhancements or innovations.

In the private sector, the model has moved to be more revenue focused, leaning on leveraging managed services and an emphasis on continuous improvement. This has resulted in more fixed cost, subscription-based services.

Downtime costs

When attacked, a critical factor will be how quickly infrastructure can get back online. The cost and impact of that 'downtime' on people and the potential knock-on effects on other sectors can be significant.

At one end of the scale, research last year by Splunk revealed that system downtime costs the world's biggest companies $400 billion annually, or $9000 every minute, with 56% of that downtime was due to cybersecurity incidents. More worryingly, 54% of executives admitted to intentionally leaving the root causes of downtime unfixed, potentially to limit the cost of legacy systems.[11]

The time taken to recover from a cyber incident has also been increasing. Last year, research by Fastly found that, on average, organisations took on average of 7.34 months to recover from attacks. That is 25%, or almost two months, longer than expected. Worse still, those organisations who chose to invest less in cybersecurity found their recovery time a third longer - almost 11 months. .[12]

At the other end of the scale, the human impact can be just as severe and long running. In 2020, the UK local authority Hackney Council was hit by a ransomware cyberattack severely crippling its systems. A ransomware gang called Pysa claimed responsibility.

Many council services, including health, housing and benefits, were not available for almost a year as crucial council systems failed to function properly. More than two years later, in 2023, and with the cost of the attack more than £12 million - the council found itself still struggling to recover.[13]

11 Splunk (2024), The Hidden Cost of Downtime, https://www.splunk.com/en_us/pdfs/gated/ebooks/the-hidden-costs-of-downtime.pdf

12 Fastly (2024), Cybersecurity at the Crossroads, p2, https://learn.fastly.com/rs/025-XKO-469/images/Fastly_Cybersecurity_at_the_Crossroads.pdf?version=0

13 Wired (2023), The untold story of a crippling ransomware attack, https://www.wired.com/story/ransomware-attack-recovery-hackney/

The increasing threat

The speed, volume and severity of attacks is increasing. Incidents of significant impact almost trebled across EU financial services between 2020-23, driven in part by better reporting mechanisms. Over 1-in-4 of the system failures reported by EU financial entities under the NIS directive were down to "errors in software changes and updates" or "hardware failures". [14]

In 2024, the UK's NCSC responded to 50% more nationally significant incidents compared to the previous year, with a 3x increase in incident severity.[15]

Added to this is the speed at which vulnerabilities are now being exploited. Google researchers found the time taken to exploit a vulnerability, typically measured as the average 'time-to-exploit' (TTE), has reduced drastically from 63 days in 2018-19, through to just five days in 2023.[16]

As the number, impact and speed at which vulnerabilities are exploited continues to grow, the importance of IT leaders recognising the need for efficient patching has only increased.

14 ENISA (2024), ENISA Threat Landscape: Financial Sector, https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf

15 DSIT (2025), State of digital government review, https://www.gov.uk/government/publications/state-of-digital-government-review/state-of-digital-government-review

16 Google (2024), How low can you go? An analysis of 2023 Time-to-Exploit Trends, https://cloud.google.com/blog/topics/threat-intelligence/time-to-exploit-trends-2023

CHAPTER 3

Measuring the relative risk of EoL exposure

We have looked in-depth at four geographies, the US, EU, UK and Japan to understand the different approaches to tackling obsolete technology and the vulnerabilities that exploit it. The Critical National Infrastructure (CNI) sectors included in this analysis are water, healthcare, manufacturing, energy and finance.

One of the key challenges to assessing the effectiveness of different approaches has been a lack of any clear measure of exposure to EoL risk. As part of this, we have developed a model to establish a relative EoL risk score at a national and CNI sector level (see Methodology section below for a full description of our approach). The model evaluates the structural and systemic risk factors, beyond just the frequency of cyberattacks, that contribute to a nation's relative risk.

It brings together publicly available national and sectoral level data, with available industry data, to establish a multi-dimensional vulnerability measure for each sector and country.

Our aim is to support national policymakers and CNI operators to identify the contribution that EoL exposure makes to overall cybersecurity risk within and across national systems.

Our results

We have presented our analytical results along two specific lens: national and sectoral. It provides a measure of relative EoL risk, rather than an absolute prediction of future cyber incidents, by creating composite scores which allow meaningful comparisons both within countries (e.g. UK health vs UK finance) and between them (e.g. UK healthcare vs US healthcare).

National results

Our analysis has produced the following national risk scores:

	Country	EoL Risk Score
	United Kingdom	92.0
	United States	88.0
EU	Germany	87.8
EU	France	83.0
	Japan	65.0

The UK has the highest relative risk score out of the five advanced economies assessed, reflecting particularly high-risk scores across UK's healthcare and water sectors.

This highlights some UK specific factors:

- Industry data pointing to a higher exposure to EoL systems;
- A higher attack frequency; and
- More highly concentrated CNI sectors which increases the impact of incidents.

This contrasts with a significantly lower EoL risk score for Japan. This also reflects some specific national factors:

- Industry data pointing to a lower exposure to EoL systems;
- A more diverse CNI base; and
- A more consistent national focus on digital resilience.

The variation between the relative risk scores for the US, Germany and France reflects the differences between key sectors, such as water and finance.

We have explored key differences in approaches across these four geographies in Annex A.

Ultimately, these findings suggest that a country's vulnerability is less determined by attack frequency alone, and more about structural weaknesses – e.g. technological obsolescence, operator concentration, and the potential scale of disruption.

CHAPTER 4

Lessons to learn

Our research has highlighted several lessons that countries should consider as they seek to reduce cyber threats to the CNI sectors.

1. **Without more active requirements on CNI operators to manage of End-of-Life technology, Governments risk growing hidden cyber risks.**

   Governments should look at where requirements similar to those included in the EU's NIS 2 regulations, the EU's Cyber Resilience Act or Japan's Economic Security Promotion Act, can be implemented to ensure that CNI operators get the basics right.

   This could include putting in place requirements that emphasise the need for clear maintenance and management plans (like Japan's Economic Security Promotion Act), active vulnerability management (like the EU's Cyber Resilience Act) and more coordinated vulnerability disclosure (like the EU's NIS2 directive).

   Requirements should also address the need to focus attention on End-of-Life technology. They should require clearer lifecycle management processes, including the maintenance of asset registers and ensured the timely reporting of incidents. The evidence is that this approach has led to CNI sectors in the EU growing in maturity when it comes to network and information security.

   Equally important, it would allow more defined reporting and monitoring on the challenge of EoL technology. This would allow governments to assess the scale of risk within different sectors and target responses to improve cyber resilience.

2. **The funding model for dealing with obsolete technology needs to change, it is too often geared towards servicing technical debt, rather than remediation.**

   Governments should modernise the way they approach IT investment. The UK government is already exploring how alternative approaches to IT investment could address this problem. A move to a more operating expenditure leaning model would even out costs over the lifecycle of technology.

   Countries could also look at where innovative approaches to funding IT investment are being taken. One example is the US's Technology Modernization Fund (TMF). Project proposals to the fund are encouraged to consider how they decrease technical debt and how they can "improve the posture of unsupported and/or unpatchable hardware or software relative to similar systems."[1] TMF projects are required to pay at least 50% of their funding back into the fund, to encourage the realisation of savings.

   Learning from the experience of schemes like these and exploring more innovative approaches to funding could support CNI operators to tackle obsolescence directly by developing projects that align incentives for both the delivery both remediation and service enhancements.

1 Technology Modernization Fund (2025), Funding and Repayment guidance, https://tmf.cio.gov/files/2025/05/Funding-repayment_updated050225.pdf

Key steps to addressing technical debt

Step 1. *Establish a live asset inventory of technology* - highlighting technology that is already at or near the end of its supported lifespan.

Step 2. *Undertake a cost to replace assessment* – this would compare the cost of replacing equipment that can no longer be patched with alternative approaches, e.g. replacing with cloud-based services for software or "as-a-service" models for hardware.

Step 3. *Decide on a replace or mitigate strategy* – establish the gap between available resources and the estimated costs of replacement. If replacement is unachievable, put in place active mitigation strategies to minimise risk. There should be a record of what compensating controls or mitigations are used, their ongoing cost and how they will be implemented. Active minimisation of risk includes:

a. Additional monitoring of technology

b. Active isolation of components and software

c. Segmentation

Step 4. *Institute a lifecycle process* - with periodic review and reassessment.

3. **Guidance on managing legacy technology should be clearer and explicit about tackling the challenge of end-of-life technology.**

   To often, guidance for CNI operators' can be unclear about any strategic priorities they should be taking in tackling technical debt. Guidance should specifically reference the importance of installing patches, updates and adopting a proactive plan for technological obsolescence, which includes key steps for addressing technical debt.

4. **Encourage more information sharing, more public post-incident reporting and cross-sector analysis.**

   Cybersecurity issues are incredibly sensitive and sharing information poses risks. Yet more reporting and monitoring of the challenge of EoL technology is needed to allow governments and sectors to assess the scale of risk they face and target their responses.

   Enabling better sharing of information about threats, incidents and vulnerabilities would encourage greater attention across sectors and more active risk management. It would also drive attention towards the available patches and upgrades capable of addressing and reducing vulnerabilities.

   More post-incident reporting would also put a spotlight on rising sectoral threats, using public scrutiny to ensure that CNI operators take active measures to reduce risk.

To further address this, we make the following recommendations -

1. **CNI operators should be responsible for maintaining live technology asset registers, alongside standardised lifecycle management and risk assessment requirements.**
   This would encourage operators to proactively identify technology assets reaching near EoL and assess whether to invest to replace, or put in place active risk management procedures.

2. **Governments should adopt a more active approach to managing End-of-Life technology in critical systems. This could be achieved through a range of approaches:**

   i. **Procurement – Encouraging minimum cyber hygiene standards from vendors and IT partners.** This would encourage services like regular patching to be incorporated into procurement contracts.

   ii. **Procurement – Reform the approach to IT investment to encourage innovative partnerships to enhance the maintenance and servicing of systems.** This would support the rebalancing of IT budgets away from servicing technical debt, towards active patching and replacement.

   iii. **Funding – Explore opportunities to pilot and prioritise 'rip and replace' programmes for EoL technology.** Given the scale of the challenge within IT systems, there is an opportunity to both pilot programmes to specifically tackle EoL technology where they don't already exist and prioritise EoL in the programs that do exist. A focus on funding incentives to prioritise the highest-risk EoL technology would reduce risks significantly. Programmes could look at how to support both the direct replacement of assets and transitional support where feasible.

   iv. **Regulation - Ensuring that where policymakers have voluntary or mandatory incident reporting mechanisms in place, they collect data on the involvement of EoL technology and provide post-incident analysis on its impact on the severity of the incident.** Incident reporting requirements should be risk-based, proportional, and enable the use modern cybersecurity approaches including machine-generation and automation cyber tools. Ensuring greater transparency and cross-sector early warning related to technology beyond its supported lifespan would support operators.

   v. **Visibility – Encourage industry-wide data sharing frameworks and standards.** Establishing greater data sharing between sectors would improve the visibility of threats and make early warning of known vulnerabilities easier.

   vi. **Developing industry requirements further – explore how new advances in AI can support more efficient approaches to update deployment.** Reducing Mean Time to Patch (MTTP) decreases risk by narrowing the window malicious actors have to exploit vulnerabilities. Automatic security updates, however, are not suitable for all operational environments, particularly for highly critical systems where deploying under-tested patches present unacceptable service disruption risks. As such, there should be further work to explore new advances in AI can support operators with that allow for real-time testing and deployment of patches, and for the isolation, segmentation, and protection of technologies that cannot be immediately patched or replaced if unpatchable.

Government should consider similar approaches as they continue to evolve their cybersecurity environment. These recommendations are aimed at supporting governments and CNI operators to tackle this important but underappreciated area of cyber risk. Adopting measures like these would both provide a better picture of where those risks exist but also focus operators' attention on managing their assets.

Crucially, actively tackling EoL technology offers governments a clear route to raising cyber resilience across critical sectors of the economy by tackling vulnerabilities before they can be exploited.

Annex A – Analysis of international approaches to cybersecurity

This analysis looks at four geographies, the UK, US, EU (with a focus on France and Germany) and Japan. For each geography we have looked at the localised EoL risk scores for the sectors considered and the national approach to cybersecurity

United States

Sector	Economic Impact	Impact on Life	Attack Surface	End-of-Life x Attack Frequency	EoL risk score
Healthcare	5	5	1	8.5	19.5
Manufacturing	2.25	2	1	11.5	16.75
Finance	3.5	1.5	1	11.5	17.25
Water	5	3.5	1	7.5	17
Energy	3.25	4.5	1	8.5	17.25

Impact of EoL technology

- The US's Healthcare sector stands out with a higher relative risk compared to other sectors analysed. Reducing exposure to EoL technology in this sector would see relatively big reductions in the overall US score.
- The scores for both Water and Energy sectors reflect the ongoing targeting of these sectors and the relatively high impact attacks have on ordinary people.

Legal framework

Whilst there is no overarching US cybersecurity law, there are several relevant federal laws:

- **Federal Information Security Modernization Act 2014 (FISMA)** – sets out roles and responsibilities for the cybersecurity of civilian agencies, defining the framework of guidelines and security standards.
- **Federal Information Technology Acquisition Reform Act 2014 (FITARA)** – this enables the President to appoint Chief Information Officers (CIOs) to federal agencies. These CIOs have an expanded role in managing IT investments for their agency and oversight of IT planning.
- **Modernizing Government Act (2018) (MGT)** – This Act authorises agencies to establish a working capital fund for dealing with legacy technology and established the Technology Modernising Fund
- **Modernizing Government Reform Act (2024)** – This Act establishes an inventory of federal legacy IT.

Key agencies include:

- **Cybersecurity and Infrastructure Security Agency (CISA)** – the agency is the national coordinator for Critical National Infrastructure Security and Resilience. CISA has the power to make binding operational directives on certain federal agencies. It also delivers a range of key programmes including the Known Exploited Vulnerability catalogue, Secure by Design, and Cybersecurity advisories.
- **National Institute for Science and Technology (NIST)** – owns the voluntary (but mandatory for federal agencies) Cybersecurity Framework which sets out high-level cybersecurity outcomes.

Commentary

- In June 2025 the White House issued its first Executive Order on cybersecurity issues.[1]

  As part of this order, NIST is required to issue new guidance by September on the secure and reliable deployment of patches and security updates. The administration has also removed the requirement for NIST to produce new guidance on "minimum cybersecurity practices".

  Guidance and standards provide an important mechanism for encouraging effective behaviours. There should be a focus on ensuring guidance reflects standards in managing end-of-life technology, as part of the emphasis on effective patch management and a natural process for technology lifecycle management.

- Whilst not mandated the House Oversight and Government Reform committee's bi-annual **FITARA Scorecard** has proved to be an important tool for improvement.

  The scorecard grades agencies across the work to improve FITARA and manage IT. It has enabled Congress to hold agencies falling behind accountable. Over time and through evolution, the scorecard has become a holistic cyber hygiene tool and an effective way to monitor progress.

Critical National Infrastructure sectors

- The US has 16 designated critical national infrastructure sectors:

1 White House (2025), Sustaining select efforts to strengthen the nation's cybersecurity and amending executive order 13694 and executive order 14144, https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/

Scale of current threats

In June 2024 US Cyber Threat Intelligence Integration Center (CTIIC) published analysis which recorded 29 direct cyberattacks on US critical national infrastructure systems between November 2023 to April 2024.[2] The work highlighted that in some cases attackers were able to manipulate critical US industrial control systems food and agriculture, healthcare, and water and wastewater sectors. Attacks on water plant facilities were particularly prevalent.

Recent incidents

- **June 2025** – Ransomware gangs exploited a vulnerability in remote support applications to target customers of a utility billing company. [3]
- **December 2024** – Chinese hackers breached a third-party vendor for the US Treasury to gain access to over 3,000 unclassified files. [4]
- **June 2023** – A Russian-linked worldwide cyberattack targeted several US federal government agencies, including entities within the Department of Energy. Several hundreds of US companies were also thought to have been affected. The attack exploited a vulnerability in commonly used software, highlighting the importance of timely updates and patches.[5]

2 CTIIC (2024), https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf
3 CISA (2025), https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-163a
4 Guardian (2024), https://www.theguardian.com/us-news/2024/dec/30/china-treasury-cyberattack
5 CNN (2023), https://edition.cnn.com/2023/06/15/politics/us-government-hit-cybeattack

UK

Sector	Economic Impact	Impact on Life	Attack Surface	End-of-Life x Attack Frequency	EoL risk score
Healthcare	3	5	5	9	22
Manufacturing	2.25	2	1	12	17.25
Finance	1	1.5	1	12	17.5
Water	2	3.5	5	8	18.5
Energy	2.25	4.5	3	9	18.75

Impact of End-of-Life technology

- The UK stands out with a much higher relative risk score compared to other countries in this analysis. Reducing exposure to EoL technology across these sectors would see relatively big reductions in its score.
- The scores for the UK's Healthcare, Water and Energy sectors particularly reflect the targeting of these sectors and the relatively high impact attacks have on ordinary people.

Legal framework

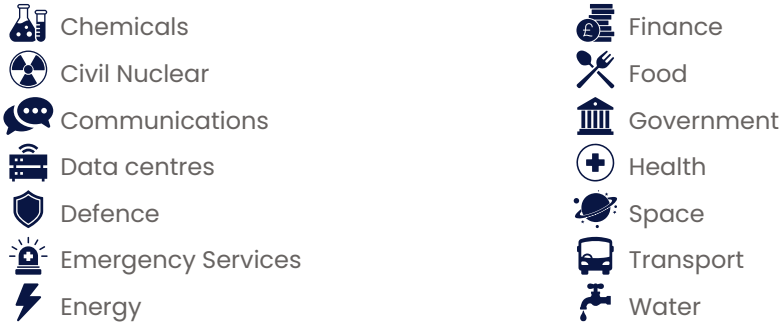
- The UK has only one cross-sector cybersecurity law, the Network and Information Systems (NIS) Regulations 2018 covering five sectors:
  - Transport,
  - Energy,
  - Water,
  - Health and
  - Digital Infrastructure
- It places duties on operators of infrastructure to safeguard the cyber resilience of the sectors covered by the legislation and to report incidents. Twelve national regulators are responsible for enforcing the regulations.
- The regulations also created the National Cyber Security Centre which is UK's technical authority for cyber threats.
- The Government has recently announced its plans for a Cyber Security and Resilience Bill. It will enable the UK to move into closer alignment with the EU's NIS2 directive, where appropriate. Like NIS2, the legislation will bring more entities into scope and put technical security requirements on a firmer footing.
- Current plans for the legislation include to:
  - bring into scope Managed Service Providers (MSPs) to enhance the security of IT infrastructure,
  - extend duties on operators of essential services (OES) and relevant digital service providers (RDSP) in order to strengthen supply chains,

- put regulators on a stronger footing to ensure essential cyber safety measures,
- improve incident reporting,
- provide a statement of strategic priorities to provide a clear framework for cybersecurity regulation across regulators and their sectors, alongside
- enable Ministers to direct regulated entities, requiring them to take action to address threats and incidents.

- Whilst not a central aim of the Bill, given the focus of the new legislation and subsequent guidance, it offers the government a good route to address cyber risks relating to EoL technologies.

Critical National Infrastructure sectors

- The UK has designated 14 sectors as critical national infrastructure:



Scale of Cyber Incidents

- Between Sept 2023-Aug 2024 there were **1,957** reported cyberattack incidents reported to NCSC. **430** of these required NCSC support (15.9% more than the previous year).
- **89** of these were considered nationally significant, with **12** deemed at the top of the scale and most severe (a x3 increase on the previous year).
- In 2024 there were a record **6 reported incidents** against the drinking water infrastructure, a three-fold increase on the year before.

Cost challenges of legacy technology

- As of March 2024, the Government's Central Digital and Data Office reported that central government departments did not have fully funded plans to remediate over half of its legacy systems.
- Remediation includes work to keep legacy systems functional, secure and compliant, applying patches, security updates or modernising equipment.
- In April 2024, the Government Security Group reported that both cost inflation and a lack of money for operating costs were affecting government departments ability to meet their cyber resilience targets.

Case studies

- **Sept 2024** – Transport for London (TfL) was the victim of a cyberattack across several of its services. The method and nature of the attack has not yet been reported.

  Most prominently, its Oyster Card system was attacked, resulting in the access to 5000 customer bank account details. TfL was forced to suspend numerous services across the capital.

  The impact lasted several months, costing TfL more than £30 million.[6]

- **June 2024** – a Russian-backed attack, by a group named Qilin, on the NHS health care services provider, Synnovis, affected 10,000 appointments and resulted in the cancellation of 1,700 elective procedures. The attack affected health services across London resulting in 2 cases of major harm, 11 cases of moderate harm and 120 cases of minor harm as a direct consequence. The cost to the company has been estimated at £32.7 million.[7,8]

6 Reporting by Computerweekly.com, https://www.computerweekly.com/news/366616875/TfL-cyber-attack-cost-over-30m-to-date

7 NHS England (2024), Update on cyber incident: Clinical impact in south east London , https://www.england.nhs.uk/london/2024/09/26/update-on-cyber-incident-clinical-impact-in-south-east-london-thursday-26-september-2024/

8 Reporting by FT, https://www.ft.com/content/d2be7c65-bf44-4a7d-9791-6deafe66659f

Japan

Sector	Economic Impact	Impact on Life	Attack Surface	End-of-Life x Attack Frequency	EoL risk score
Healthcare	3	5	5	3.5	16.5
Manufacturing	4.25	2	1	6.5	13.75
Finance	2.5	1.5	1	6.5	11.5
Water	3.5	3.5	1	2.5	10.5
Energy	2.75	4.5	2	3.5	12.75

Impact of End-of-Life technology

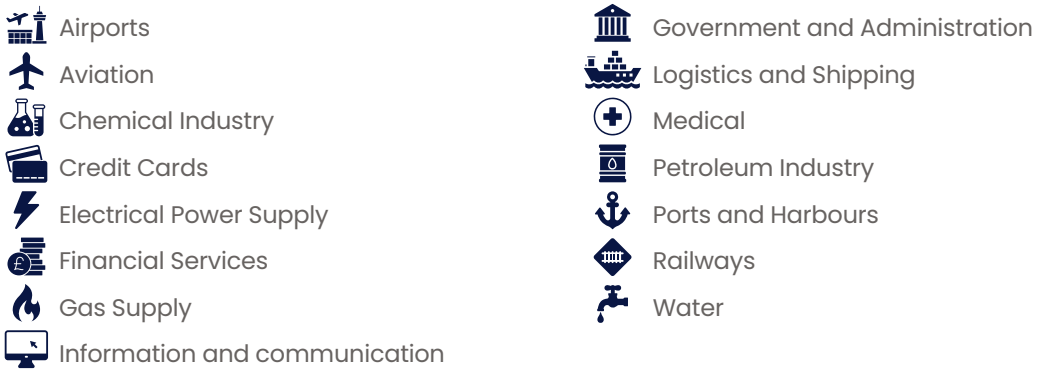
- Japan's sectors stand out with relatively low risk scores against the other countries. Like other countries, the healthcare sector is one area where further risk reduction is possible.

Legal framework

- The cornerstone of Japan's cybersecurity legislation is the Basic Act on Cybersecurity that regulates the responsibility of national and local governments for cybersecurity. It places obligations on critical infrastructure operators to ensure cybersecurity.
- Under its Economic Security Promotion Act, important critical infrastructure businesses are individually designated as Specified Essential Infrastructure Service Providers and are required to reduce or eliminate risk factors. It also requires mandatory "introduction plans" for equipment, with a focus on detailed maintenance and management plans and prohibitions on the use of unsupported devices. It also requires mandatory incident reporting for critical national infrastructure operators.
- The Japanese Diet passed a new Active Cyber Defence Act in May 2025 that will come into full effect by November 2027. The new law reflects a more national security focused stance, leading to a more proactive and coordinated approach to cybersecurity.
    - Japan's National Centre of Incident Readiness and Strategy for Cybersecurity (NISC) will be restructured and strengthened as a National Cybersecurity Office with a strengthened remit across the threat landscape across Japan's critical national infrastructure. This will be realised through new measures for setting standards for CNI operators, requiring operators to submit a list of their IT assets and reporting incidents to this Office.
    - This body will continue to act as the secretariat for the county's Cybersecurity Strategic Headquarters which develops national cybersecurity policy, coordinating efforts across government and implementing the county's national cybersecurity strategy. This will now be chaired by the Prime Minister and all Cabinet Ministers are included as members.
    - A vice-ministerial level Cabinet Cybersecurity Officer will be appointed to oversee cybersecurity affairs. Alongside this administrative post, there is the potential for the Prime Minister to appoint a minister of state for cybersecurity.
- There is also the Cybersecurity Policy for Critical Infrastructure Protection which provides a common action plan and sets out obligations on critical infrastructure operators.

Critical National Infrastructure sectors

- Japan has designated 15 sectors as critical national infrastructure:



Recent incidents

- **December 2024** – Japan Airlines reported that it had suffered a cyberattack to its network that caused delays to some of its domestic and international flights.
- **July 2023** – Japan's largest port, Nagoya, was the victim of a ransomware attack that forced it to suspend operations for several days. The Port accounts for 10% of Japan's total trade value.

EU

France

Sector	Economic Impact	Impact on Life	Attack Surface	End-of-Life x Attack Frequency	EoL risk score
Healthcare	3.75	5	4	7	19.75
Manufacturing	2.5	2	1	10	15.5
Finance	0.25	1.5	1	10	12.75
Water	2.75	3.5	4	6	16.25
Energy	2.25	4.5	5	7	18.75

Germany

Sector	Economic Impact	Impact on Life	Attack Surface	End-of-Life x Attack Frequency	EoL risk score
Healthcare	4.5	5	2	8	19.5
Manufacturing	4	2	1	11	18
Finance	3.75	1.5	1	11	17.25
Water	2.75	3.5	2	7	15.25
Energy	2.25	4.5	3	8	17.75

Impact of End-of-Life technology

- Like the other countries assessed, both France and Germany's relative risk scores reflect the challenge EoL technology presents.
- Whilst relatively lower than both the UK and US, the sectoral picture points to sectors where a focus on tackling EoL would meaningfully reduce risk.

Legal framework

- The Network and Information Systems (NIS) Directive was the EU's first piece of legislation aimed at securing network and information systems across the EU Member States. The Directive requires operators of essential services to adopt measures to protect their network and to mitigate the risk of cyber incidents.
- A revised directive, NIS2, builds on this by requiring each Member State to adopt a national cybersecurity strategy. The revised directive doubles the number of sectors in scope. It establishes more structured incident reporting to national competent authorities, including specific deadlines. The directive also requires individual organisations to address cybersecurity risks in their own supply chains and with supplier relationships. It sets out obligations on entities in relation to cyber security risk management.
- More recently, the EU has passed the Cyber Resilience Act which imposes strict cybersecurity requirements on manufactures, including in relation to security updates, vulnerability management and resilience to cyberattacks.
- The Act came into force in December last year, with implementation due to be completed by December 2027. However, the obligations on manufacturers to report actively exploited vulnerabilities and incidents will be in force from September 2026.

Critical National Infrastructure sectors

- Energy
- Transport
- Banking
- Financial market infrastructure
- Health
- Drinking Water
- Wastewater
- Digital Infrastructure
- Public Administration
- Space
- Post
- Waste Management
- Chemicals
- Manufacturing
- Production, Processing and Distribution of Food
- Digital providers
- Research

Glossary

- **End-of-Life (EoL)** – This refers to the point where a product is now obsolete, e.g no longer sold, improved, maintained nor supported by its manufacturer.
- **Legacy Systems** – This refers to either hardware or software systems that are outdated but may still be supported
- **Patches** - Patches are software and operating system updates that are installed to correct security and functionality problems in software and firmware. Patches can also serve other functions, such as adding new features to products; however they are used most often to mitigate software vulnerabilities.
- **Technical Debt** – This is the hidden liability from technology is considered legacy technology or outdated, which cannot be patched or operated securely. Managing this type of technology tends to lead to dependence on quick, stopgap IT fixes. Crucially, whilst saving time or money in the short term, this can lead to several important challenges:
    - higher maintenance costs in the long term,
    - a reliance on End-of-Life (EoL) devices,
    - higher risks of cyber intrusion,
    - reduced efficiencies through deferred modernisation, and
    - growing technical complexity.

  Not directly addressing technical debt also leads to its increase.
- **Threat actor** – This refers to individuals or groups that intentionally cause harm to digital devices or systems.
- **Threat surface** – This refers to all the possible avenues by which a threat actor can attempt to exploit a system, interfere with its operation or gain unauthorized access to data. It includes all technical, physical, and human exposure points.

Methodology

Introduction

In 2024 the United Kingdom was the most cyber attacked country across Europe, accounting for 27% of cyberattack cases[1]. However, our methodology goes beyond attack frequency and instead aims to bring out a relative vulnerability level for each country.

Cybersecurity vulnerability is influenced by three key factors:

1. **The type of threat?**

    - In our analysis the threat is centred around assessing the desire and capabilities of adversaries to attack vulnerable legacy systems within critical national infrastructure.

2. **How likely is the treat to occur?**

    Vulnerability is influenced by three factors.

    - **The attack surface** - When a single business dominates a large portion of a sector, the attack surface becomes highly concentrated, creating systemic risk. This centralisation means that if a virus or malware compromises the dominant firm, it can immediately affect a significant share of the entire sector. Homogeneity across systems, where most organisations rely on the same infrastructure, software, or service, allows threats to spread rapidly without needing to adapt, while also making the target more appealing to attackers due to the high potential impact. Furthermore, if the firm plays a key role in the supply chain, a breach can cascade to partners, clients, and end-users.

    - **Exposure to end-of-life (EoL) Technology** - software significantly increases the risk of malware infection and operational disruption across an industry. EoL technology no longer receives vendor support, including security patches or vulnerability remediation, leaving known exploits unmitigated and easily targeted by threat actors. In sectors reliant on legacy systems or where outdated technology underpins critical infrastructure, this creates a persistent vulnerability. A successful compromise can enable rapid lateral movement, data exfiltration, or system downtime, resulting in substantial operational, financial, and reputational damage.

    - **Attack Frequency** - A high frequency of attacks increases the likelihood that weaknesses will be discovered and exploited, making systems more susceptible.

3. **What are the consequences of a successful attack?**

    We analyse the incentive structure for attackers by examining the various factors that shape the overall risk landscape, thereby determining how vulnerable a system, organisation, or even an entire nation is to cyber threats. The return on investment (ROI) for attackers and the intent to cause disruption are the main drivers of motivation to implement cyberattacks.

    - The ROI of an attack—whether financial gain, data theft, or strategic advantage—further motivates cybercriminals to target systems with the highest potential rewards.

1 Germany accounted for 15%, Denmark 14%, Portugal 11%, and Italy and France each represented 8%.

Organisations that store sensitive data or oversee critical infrastructure are particularly at risk, as they present lucrative opportunities for attackers.

- Beyond financial incentives, the human impact of disruption plays a significant role in cybersecurity threats. Cybercriminals, hacktivists, and even nation-state actors may seek to undermine public trust, create panic, or destabilise institutions. Attacks targeting healthcare, government, or financial services can have severe social and economic consequences, amplifying their effectiveness.

Our modelling brings these factors together to generate a comparative score, enabling each country to assess how its sectors are performing. These scores also facilitate cross-national dialogue, allowing nations to benchmark their sectoral performance against that of their international counterparts.

EoL Score

1. To calculate an EoL score we use geolocated CVE-attributed attacks targeting telemetry systems more than five years old. From this, we can infer both the geographic distribution of these attacks and the expected frequency of attacks on equipment that is likely to be at or beyond its EoL stage.

2. Next, we use Checkpoint and IBM[2] data to create a range of estimates regarding the sectors that are most targeted by cyberattacks and overlay this data with the geographic distributions to **quantify total cyberattacks distributed by country and sector**.

Attack Surface

3. We estimate **attack surface** by evaluating the market dominance of the top five firms within each sector, by country. For example, the NHS operates a significant proportion (79%) of the UK's health sector market. Consequently, we rank the UK's health sector attack surface exposure as a 5 (the highest possible score) - this indicates that if a computer virus was to be successfully implemented it would have a significant damage on the entire sector within the country. We use a variety of market data sources to conclude the size of each sector.

Disruption Effects

4. The **economic impact** of a successful cyberattack is often a significant part of the incentive for adversaries to attack critical national infrastructure. The following data points are used to evaluate sector-wide disruption:

    a. Manufacturing as a % of GDP

    b. Health spending per capita

    c. Water use per capita

    d. Liquid assets to deposit ratio – A measure of financial stability

    e. Energy intensity per capita

2 Checkpoint 2025, https://engage.checkpoint.com/security-report-2025; IBM X-Force 2025, https://www.ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index

5. **Disruption to human life** is a second incentive to attack critical national infrastructure. We adopt a ceteris paribus approach, assuming that if each sector in each country experiences an identical cyber incident with the same level of severity, that the disruption is resolved within a consistent timeframe across all cases. As a result, we have an impact on human life score that is identical for each country for the same sector.

Scoring

Using a 1–5 ranking system based on standard deviation bands offers a statistically consistent way to evaluate how individual values compare to the rest of a dataset. Unlike a simple 1–5 ranking that assigns fixed ranks based purely on order (e.g., from lowest to highest), standard deviation banding reflects how far each value deviates from the average, capturing not just relative position but the **magnitude of difference**. This is especially useful when distinguishing between values that may be close to one another, or performing significantly differently.

One slight disadvantage of this method is that when comparing a group of fairly similar countries - such as advanced economies - the spread of values is naturally narrower. As a result, the standard deviation is smaller, and most observations fall within one or two bands of the mean. This results in a **more compressed ranking**, reflecting the fact that these countries are genuinely similar in performance.

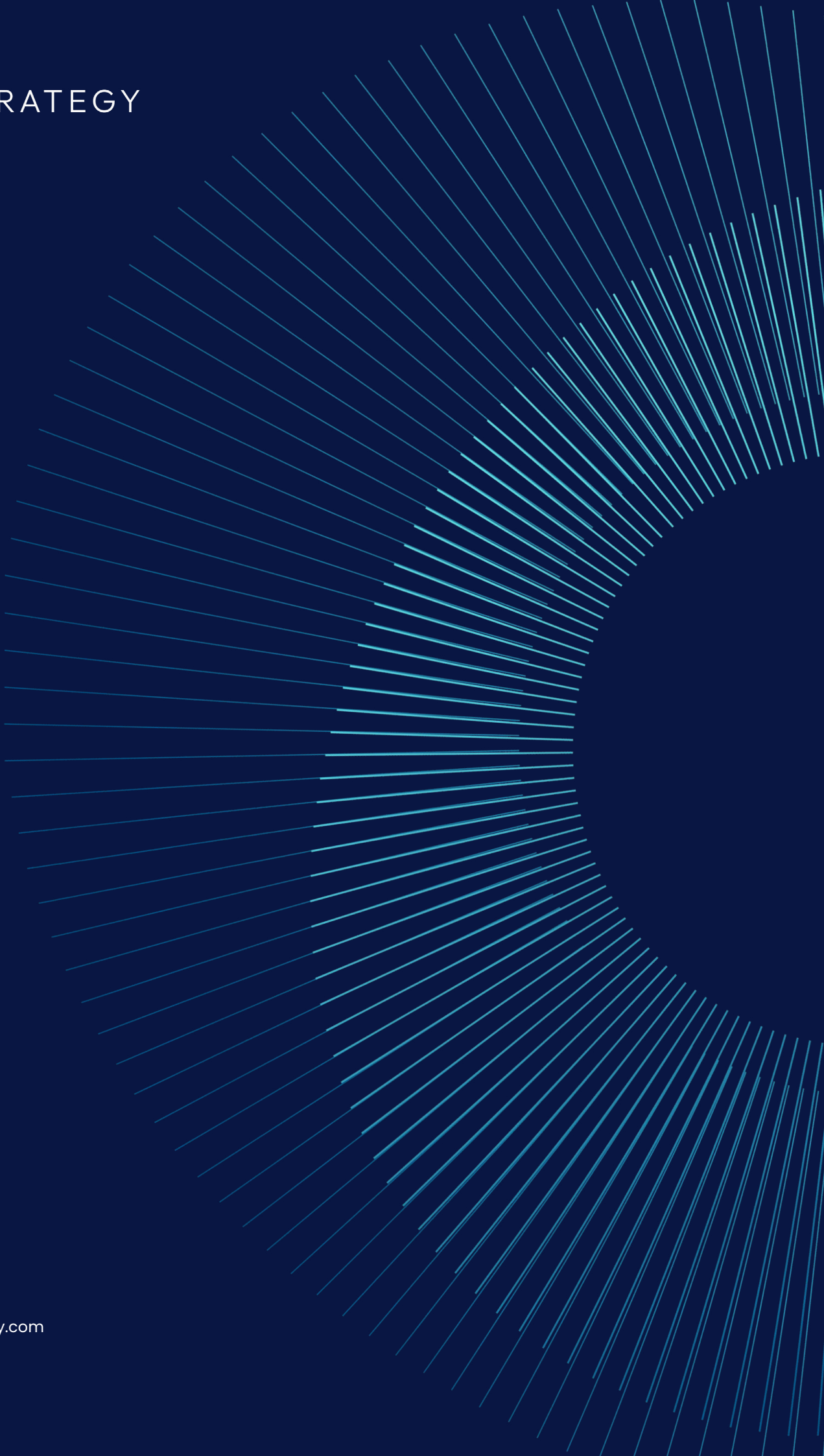
That being said, the 1–5 format itself remains easy to interpret, making it highly effective for non-technical audiences. Furthermore, this method allows different indicators - such as water use vs financial stability to be normalised onto a common scale, facilitating cross-metric comparisons.[3]

Placing a relative performance score on each sector allows us to do a cross-sector comparison and compare, for example, the vulnerability within the US healthcare system compared to the UK's water sector, or the UK's water sector against the UK's Finance sector. This type of analysis is particularly helpful for policymakers as it will highlight which sectors could be seen by adversaries and/or private attackers as relative weaknesses and thus will require further investment to achieve a heightened level of security. Evidently, this particular type of analysis is important when policymakers seek to improve the security of sectors which are deemed as nationally important.

This holistic approach provides a **comprehensive, multi-dimensional assessment of cyber risk**, ensuring that vulnerabilities are evaluated not just from a technical standpoint but also from economic and human impact perspectives.

3 Notably, the EoL ranking is between 1-15 as this represents the combination of three 1-5 scores: proportion of EoL equipment, attack frequency by country and attack frequency by sector.

WPI STRATEGY



WPI Strategy
5-6 St Matthew St
London
SW1P 2JT
@wpi_strategy
https://wpi-strategy.com

October 2025
Design: wond.co.uk