APPG ON CYBER SECURITY AND BUSINESS RESILIENCE MEETING
7th July 2025, 3.30 P.M. Portcullis House

Title: Review and expand on the work of the two previous APPG meetings to prepare a brief for Parliamentarians to cover the forthcoming Bill on Cyber Security and Resilience.

Chairman's welcome: Lord Arbuthnot took the Chair and welcomed everyone.

Present: Baroness Neville-Jones, Admiral Lord West of Spithead

Apologies: Lords Mackenzie of Framwellgate, Sharpe and Taylor of Warwick and Kit Malthouse MP (APPG Chair)

Speakers:

1) **Gary Fildes, CGI**

Thank you for the opportunity to speak today on the **Cyber Security and Resilience Bill (CSRB)**. We are here not simply to examine its legislative construction, but to ensure that its **intended outcomes translate into real-world resilience**—across sectors, across systems, and across the layered infrastructure that underpins our national life.

This Bill represents more than regulatory refinement—**it is a defining evolution in our national approach to cyber security**, signalling a maturing understanding of the threats we face and the resilience we must build. Its importance must be understood in the broader context of safeguarding:

- **Critical National Infrastructure**,
- **Economic Integrity and Innovation,**
- **Public Safety**, and
- **The UK's National Security**.

Cyber risk is no longer confined to the realm of technical teams. It is a strategic business issue. **The CSRB rightly recognises the need for stronger governance**, particularly through enhancing the duties of operators of essential services (OES's) and relevant digital service providers (RDSPs).

While the Bill does not mandate board appointments, it signals that **senior leadership must engage meaningfully** with cyber resilience.

This aligns with NCSC **CAF Objective A1: Governance**, where effective oversight, defined responsibilities, and risk-informed decision-making are the cornerstones of security maturity.

Organisations should and must be encouraged to:

- Ensure there is a board-level individual who has overall accountability for the security of network and information systems

- Treat cyber risk as a standing board-level agenda item,
- Ensure investment in resilience is proportionate to the threat environment, and
- View incident response readiness as an operational strength, not a reactive process.

While the Bill introduces stronger requirements to mitigate risks from supply chains and managed service providers, it's important that we stay grounded in the **core vulnerabilities currently exploited by threat actors**.

The most significant incidents affecting UK citizens are still those exploiting **legacy infrastructure**, **out-of-support platforms**, and **technical debt** that has accumulated over decades.

This is the contradiction we must resolve: whilst **we are innovating rapidly while remaining anchored to outdated systems**.

To support progress, the regulatory framework must:

- Encourage risk-led prioritisation of **legacy system retirement**,
- Offer structured guidance for **secure digital modernisation**, and
- Acknowledge the **cost and complexity constraints** that many organisations, especially in public services, must navigate.

The CSRB's intention to strengthen regulatory oversight is well-founded. We support the extension of powers to audit, investigate, and enforce—provided these remain **proportionate, transparent, and improvement-oriented**.

The **Regulators' Code** must remain a living principle within the enforcement landscape.

- Thus, ensuring that **cost recovery mechanisms** are tied to tangible outcomes—supporting measurable improvements in UK-wide cyber resilience and maturity, rather than imposing additional regulatory burdens, financial or resource scarcity on Operators of Essential Services (OES).
- Again**, Audits and assessments** must evaluate real-world, threat capability—not only the existence of documented policies.
- And regulatory guidance must remain **consistent, actionable, and adapted to sector-specific realities**—particularly for those newly entering scope under the updated legislation.

However, no regulatory framework can succeed without the **people** who make security happen. The UK still faces a **shortage of cyber professionals**—not only in regulated sectors, but within the very regulators and competent authorities tasked with oversight.

We must strengthen capacity across the ecosystem:

- Expand **cyber skills initiatives**, including governance, assurance, and technical training across IT, OT, and AI systems,
- Open and diversify **accredited entry pathways** for early-career professionals,
- And build **incident response muscle** through hands-on sector-based training and national exercises.

A skilled workforce is the backbone of operational resilience. And that workforce must be supported at all levels—from SOC analysts to CISOs to CEO.

Cyber incident response must be recognised as a **strategic capability**, not a procedural obligation. The Bill's support for incident reporting and regulator-led information sharing is a vital step—but this must evolve into a culture of **collaborative defence**.

The CSRB should further enable:

- Embedding of **incident response planning** into organisational governance frameworks,
- Encourage a positive reporting culture without fear of penalty or disproportionate action from the competent authority or regulator.
- **Post-incident reviews** to be shared in **cross-sector forums** —anonymised where needed—to support cross-sector learning,

My Lords and colleagues, the Cyber Security and Resilience Bill is a welcome and necessary evolution of the NIS Regulation. But its success will be judged not by its wording, but by its **outcomes**—by how well it strengthens the security of our people, our services, and our national prosperity.
This is our opportunity to shape a cyber strategy that is:

- **Robust** enough to address today's threats,
- **Adaptive** enough to meet tomorrow's innovations, and
- **Proportionate** enough to foster growth, not hinder it.

Thank you again for the opportunity to speak today.

2) **Renata Vincoletto, Civica**

Civica is a global GovTech champion focused on developing cloud software and services that are integral to the daily lives of citizens worldwide. From central and local government to education, workforce, health and care, more than 6,000 customers trust and partner with Civica, using our software to deliver critical services to more than 100 million citizens. We are the UK's No1 public sector software provider.

We're a GovTech provider working across critical public sector systems, so we see both the potential and the practical challenges of resilience every day.

It's encouraging to see resilience and supply chain risk being taken seriously at a legislative level. Aligning the Bill with existing frameworks like the NCSC's CAF and NIS2 helps with clarity — especially for organisations already working under those models.

The focus on operational resilience, not just risk prevention, is overdue and welcome. Cybersecurity is no longer just an IT issue, it's a board-level imperative; and operational resilience is a must

But from the industry side, there are key concerns we hope the Bill will address.

1. **Capacity gaps in the public sector and supply chain:** Many councils, NHS trusts, and SMEs don't have the teams or budgets to meet rising expectations. We risk mandating compliance that's impossible to deliver. We need clear support and a phased implementation.

2. **Ambiguity in obligations:** Ambiguity leads to inconsistent adoption and confusion. Voluntary vs. mandatory controls need to be crystal clear

3**. Third-party risk is underdefined:** We need minimum, enforceable standards for managing supplier cyber risk — especially in shared service models and joint delivery ecosystems.

4. **Reporting burden:** There's fatigue around incident reporting. It needs to be streamlined — align it with existing requirements from the ICO and NCSC to avoid duplication.

From my perspective, **here's what should be built into the Bill:**

- Baseline expectations tied to maturity — CAF Tier 1–3 gives us a scalable way to do this.
- Phased timelines to reflect sector readiness — a one-size rollout won't work.
- Incentives, not just penalties — procurement preference or grant funding for those exceeding the baseline would drive adoption faster.
- A safe, structured way to share threat intelligence across industries and with government not just compliance, but collaboration.

At Civica, we've already taken steps in this direction. For example, we align our internal cyber maturity assessments to CAF tiers, enabling differentiated expectations across business units based on risk. We've also created secure collaboration channels for sharing intelligence and response insights with key partners — including suppliers and local authorities — to improve collective defence. Incentives such as supplier scorecard weighting for security maturity have proven effective in accelerating adoption.

Just as important is what not to include:

- Avoid overly prescriptive controls — let organisations achieve outcomes in ways that fit their risk and context.
- Don't duplicate reporting channels — build on what exists.
- And don't expect the same level of resilience from vastly different organisations without offering proportional support.

Industry is ready to partner on this — but we need clarity, realistic expectations, and meaningful support.

Happy to continue the conversation beyond today. Thank you.

3) Richard Starnes

For over three decades, I have worked on the front lines of UK and US cyber defence, from being a cybercrime detective to being a Chief Information Security Officer, I have served critical organisations like the London Metropolitan Police Service and Heathrow Airport. I am the Chairman of the Security Panel for the Worshipful Company of Information Technologists, the City Livery Company for the Tech Sector, a non-executive director and chair of the advisory board for the Cyber Resilience Centre for London, COO and Director at the Kent & Medway Cyber Cluster and a Governor at the Lenham School in Kent. Today, I am speaking to you as a practitioner who has seen firsthand the escalating cybersecurity and privacy threats facing UK SMEs. To put the size of the market at risk into perspective, there are approximately 5.5 million businesses in the UK, and 5.4 million are small to medium-sized. Those are companies with between 0 and 249 employees. SMEs account for three-fifths of employment and over half of private sector turnover in the United Kingdom.

Last year, over 600,000 UK businesses suffered a cyberattack that we are aware of. Criminals and nation-states are not just targeting His Majesty's government or FTSE 100 companies; they are attacking the local solicitor, the family-run manufacturers, the family GP, the local corner shop and small businesses that serve our critical national infrastructure. They see SMEs as low-risk, high-volume targets.

Many of these businesses are trapped below the "Cyber Poverty Line." They lack the resources for adequate defence, with many spending less than £100 annually on security. They lack specialist knowledge, with two million SMEs providing no staff training. And they dangerously believe they are "too small to be a target"—a myth that organised crime and nation state actors are all too willing to exploit through automated attacks. This is a significant risk to the UK economy, as every large enterprise and government department relies on a supply chain of these smaller, vulnerable businesses. When 60% of small firms fail within six months of a major breach, it creates a domino effect that undermines our economy.

The government's National Cyber Security Centre (NCSC) provides high-quality guidance, but that guidance is failing to reach those who need it most. The 2025 Cyber Security Breaches Survey revealed that awareness of the flagship "Cyber Aware" campaign has fallen to just 24% among businesses, with only 1% of businesses who would turn to the NCSC for information. This highlights the central challenge in the current strategy: the "engagement paradox." The government operates a passive, "supply-driven" model, creating excellent resources; however, business owners do not proactively seek out those resources. SME owners, juggle countless responsibilities and may not feel they have the time and technical ability to become a cybersecurity expert.

This challenge has been implicitly acknowledged. The "Funded Cyber Essentials Programme," which offered hands-on support to small companies, was a success. However, it was a temporary, narrowly focused pilot that has now closed—a significant missed opportunity. This has created a "last mile" delivery problem. We have the central infrastructure but lack the mechanisms to get support to the end-user.

Furthermore, the UK's Cyber Cluster programme, a vital support structure for SMEs, is facing instability. A government shift from core operational funding to short-term, competitive grants threatens the programme's long-term viability, forcing clusters to chase funding rather than provide consistent support.

The solution is not to ask 5.4 million business owners to become cybersecurity experts. The solution is a new "National Cyber Compact," a partnership between government and industry. I urge you to champion three near-term priorities:

1. A National SME 'Cyber Health Check' and Resilience Voucher Scheme: A government-funded expert assessment for every SME to diagnose risks, followed by a co-funded voucher to help implement necessary security controls. A broad-based and fully Funded Cyber Essentials Programme being a core element for both SMEs and suppliers to SMEs.
2. A 'Cyber Skills for Business' Fund: A dedicated fund providing grants for SMEs to hire cyber apprentices and upskill existing staff, building sustainable in-house capability.
3. Mandating and Subsidising Supply Chain Cyber Audits: Require large enterprises to verify the cyber hygiene of their critical SME suppliers, using Cyber Essentials as the benchmark. This must be paired with a subsidy for the SME to ensure the cost burden is shared, creating a market-driven security uplift across the economy.

Securing our SME sector is not a cost; it is a critical investment in our national resilience and economic prosperity. We have models that will work. We now need the political will to deploy them at the scale and speed this threat demands.

Thank you.

4) Amar Patel, Fundsmith LLP

To strengthen the UK’s national cyber resilience, it’s vital that the legislation achieves this in a way that is practical, proportionate, and aligned with existing frameworks.

What We'd Welcome in the Bill

• Clear scope and proportionality – Focus the highest obligations on truly critical infrastructure, recognising the mature cyber frameworks already governing financial services.

For example, financial services firms like Fundsmith already operate under FCA rules that require regular cyber resilience testing, board-level oversight, and mandatory reporting of operational incidents. Adding overlapping requirements without recognising this risks creating unnecessary compliance work without improving security.

• Streamlined incident reporting – Support a single reporting route (e.g. via NCSC) to satisfy multiple regulators. Establish clear thresholds to avoid over-reporting.

For instance, during the MOVEit file transfer software breach in 2023, many firms had to report the same incident to multiple regulators in different formats, on different timelines — duplicating effort that could have been spent on resolving the incident.

• Supply chain security that is achievable – Focus on collective assurance and standard certifications. Avoid imposing audit expectations that firms cannot deliver over global providers.

We rely on global providers like Microsoft and AWS. No UK firm can demand direct audit rights from such suppliers. Instead, collective approaches, such as ISO certifications or NCSC-endorsed schemes, are the practical way forward.

• Alignment with international standards – Build compatibility with DORA, NIS2 and other frameworks to avoid fragmented compliance.

What We Hope the Bill Avoids

• Duplicative or conflicting obligations – Avoid layering on parallel rules that confuse rather than strengthen resilience.

Right now, a financial firm might already conduct cyber stress tests for the FCA, operational resilience mapping for the PRA (Prudential Regulation Authority), and privacy assessments under GDPR. Adding another layer could divert resources from actual security work.

• Overly rigid reporting deadlines – Allow for provisional reports and updates, recognising the complexity of incidents.

In a complex ransomware attack, it can take 48 to 72 hours to understand which systems and data are affected. A rigid 24-hour full reporting requirement risks pushing out incomplete or speculative information.

• Unrealistic supply chain mandates – Do not create obligations that firms cannot practically meet, especially for large cloud providers.

No firm will get audit rights over AWS, but we can require providers to hold certifications that demonstrate they meet recognised standards.

• Ambiguity about regulator roles – Clearly define the responsibilities of NCSC, FCA, PRA and others during incident response.

This Bill represents an important opportunity to strengthen the UK's resilience through genuine collaboration between government and industry. We would welcome the chance to contribute further to ensure these measures work in practice.

Questions and comments:

Lord West – what about chips, who is ensuring that these are safe?

RS – China will either attack or modify them. 50% of N Korea's economy is based on cyber crime.

RV – the Maersk attack was the result of an attack on a Ukrainian accountancy firm down the supply chain. We must protect the supply chain sufficiently well down to the chip manufacturers.

Baroness Neville-Jones – The Strategic Defence Review calls for a readiness strategy. Does the Bill have such a strategy?

GF – Bill should be about understanding the risks involved. It should include Board level accountability for failure.

Responses from the floor:

1. AI will speed up criminal activity. Any advantage that we have will therefore be lost quickly. SMEs and supply chain resilience should be the focus.
2. Bill must be written to cover future technology developments.
3. Uncertainty is bad for any organisation.
4. Bill must support sharing of intelligence about attacks. It should also bring in vendor checks to manage supply chains and grants for smaller businesses to build cyber defences. There are concerns about the confidentiality of proprietary information.
5. Bill should look at how to get senior executives to take action.
6. The role of the CISO needs to be better valued. We should remember the cyber risks are one amongst many. It can be difficult to bring matters to the Board and to avoid a culture of "career killing", it is recommended that the Government looks at Sarbanes-Oxley (SOX). This provides credible whistle blower protection. "Public interest" UK laws are difficult to manage and open to interpretation which discourages people from sharing concerns or "bad news".
7. The JIT model has created risk in supply chains this is why security is only as good as the weakest point.
8. Will the Bill address liability issues, who is liable when software becomes vulnerable to attack? In Financial Services we have a legislative, regulatory and accountability framework: Financial Services and Markets Act 2000
    i. Part II creates definitions of regulated activities
    ii. Part III creates the requirement for authorisation
    iii. Part IV creates permission
    iv. Part V creates duties and obligations for Senior Management Functions
        I. S.59ZA Senior Management Functions creates the concept of responsible persons

II. See: SUP 10C.4 Specification of functions - FCA Handbook
III. S.66 creates Disciplinary Powers
See Paras 1 & 3

9. Many SMEs rely on their Managed Service Provider so they need to be addressed by the Bill.
10. How will the Bill address the Critical National Infrastructure?
11. The UK needs a national Helpline for advice.
12. The Bill should also address whistleblowing and the right balance between privacy and monitoring.
13. What is the risk appetite for investing in cyber security defence vs paying the cost of a breach? Does the Government have a view itself on this?
14. We could learn from the civil nuclear business which has strong regulation and must avoid a tick box approach to security.
15. Liability for breaches ought to be made clear in the Bill which should include corporate executives. The Boards of organisations need to understand their responsibilities in regard to cyber security.
16. Reporting of cyber incidents should be anonymous.
17. Cyber security should be professionalised through the Bill.
18. The Bill needs for more clarity around how we will need to manage critical suppliers.
19. Should we be preparing to align fully to EU efforts such as DORA given the expansion to cover MSPs is similar to the EU NIS2 Directive?
20. Those using regulatory powers must have the correct skillset to ensure businesses are treated fairly under this legislation.

Conclusions: attendees were asked to email the Secretariat with more points. Parliamentarians will be keen to be kept informed and, when the Bill comes out, put questions to the relevant Minister.

Non-Parliamentarians present:
Andrew Henderson - Secretariat
Steve Penny, SANS Institute
Andrew Churchill, The CSBR
Dominic Connor
Gunnar Papendick Larsen
Richard Starnes
Bryan Altimas
Pauline Jorgensen
Mark Osborne
Tom Whipp
Max Kington

Paul Litherland
Brian Brackenborough
Jonathan Wood
Jon Plumfleet
Gary Fildes
Renata Vincoletto
Raj Kotecha
Alphus Hinds
Mario Platt
Kirsty Kelly