National Audit Office

REPORT

Government cyber resilience

Cabinet Office

SESSION 2024-25
29 JANUARY 2025
HC 546

Key facts

Multiple

system controls fundamental to departments' cyber resilience were at low levels of maturity in 2024, including asset management, protective monitoring and response planning

At least 228

'legacy' IT systems in use by departments in March 2024, and the government does not know how vulnerable these are to cyber attack

More than 50%

of roles in several departments' cyber security teams were vacant in 2023-24

89 of the 430 incidents managed by the National Cyber Security Centre between September 2023 and August 2024 were assessed as "nationally significant"

£600,000 the British Library's assessment of the financial costs that could be directly attributed to the October 2023 cyber attack it experienced, by March 2024

32% of roles in the Government Security Group's (GSG) cyber directorate were vacant when GSG established it in November 2022

£1.3 billion additional funding provided to departments and intended for investment in cyber and 'legacy' IT over the 2021 Spending Review period

Summary

Introduction

1 Cyber attack is one of the most serious risks to the UK and the government's resilience. The COVID-19 pandemic highlighted that the UK needed to strengthen its national resilience and prepare for future emergencies. The government defines cyber resilience as "the ability of an organisation to maintain the delivery of its key functions and services and ensure the protection of its data, despite adverse cyber security events".

2 The need for the government to improve its cyber resilience is becoming more urgent in an increasingly digital world. The last decade has seen rapid growth in the government's digital ambitions, the number of government services available online, and the devices and IT systems that connect people, organisations and businesses globally. This provides significant opportunities for society and the economy. It also makes it easier for those with malicious intent to cause disruption, which can have a devastating impact on individuals, government organisations and public services. The cyber threat to the UK comes from a range of 'threat actors' (individuals, groups or organisations that intentionally cause harm to digital devices or systems). Threat actors include those who are 'state-affiliated' and funded by states and governments; those who are 'state-aligned', who are often not subject to state control and are ideologically rather than financially motivated; and financially motivated cyber criminals or groups.

3 The UK's cyber security and resilience has been a strategic priority for government for at least a decade. In 2010, the National Security Strategy described cyber attack as a top threat and priority for action. The government supported its 2011 UK Cyber Security Strategy with a £650 million cross-government National Cyber Security programme. It supported the subsequent National Cyber Security Strategy 2016–2021 with funding of £1.9 billion. We examined both strategies and programmes in previous reports. We found that the government had made some good progress with its 2016 programme, such as by creating the National Cyber Security Centre (NCSC), the UK's technical authority on cyber security, but that it was unclear whether the government would achieve its strategic objectives.

4 In January 2022, the Cabinet Office published the Government Cyber Security Strategy: 2022–2030 ('the Strategy') which, for the first time, set out the challenges facing government cyber security and a vision for improving it. The Strategy aligns with the 2021 Integrated Review of Security, Defence, Development and Foreign Policy and the National Cyber Strategy 2022 in supporting the government's ambition to make the UK a democratic and responsible cyber power. The vision of the Strategy is to "ensure that core government functions, from the delivery of public services to the operation of national security apparatus, are resilient to cyber attack".

5 In the July 2024 King's Speech, the government announced it would introduce a Cyber Security and Resilience Bill. The aim of the Bill is to strengthen the UK's cyber defences to ensure that the critical infrastructure and digital services companies rely on are secure.

6 The Government Security Group (GSG) in the Cabinet Office leads the government's security function, including cyber security. It is responsible for leading implementation of the Strategy and supporting government departments to improve their cyber resilience. GSG works closely with the NCSC and the Central Digital and Data Office (CDDO), which leads the government's digital and data function. Departments are responsible for their own cyber resilience and meeting the security standards set by GSG. They also are responsible for ensuring their sectors and arm's-length bodies meet strategic resilience targets.

7 In December 2022, government published the *UK Government Resilience Framework*, setting out its strategic approach to strengthening resilience. Our report is part of our programme of work on resilience and follows our previous reports on *Government resilience: extreme weather* and *Resilience to flooding*.[1]

Scope of this report

8 This report examines whether the government's efforts to improve its cyber resilience are keeping pace with the cyber threat it faces. The report aims to: hold government to account for its performance; increase transparency about how cyber resilient government is; and help government improve its cyber resilience. To do this, we examined:

- the threat to government cyber security;
- progress with implementing the Strategy;
- the government's cyber resilience position in 2024; and
- the challenges for departments in building cyber resilience.

1 Comptroller and Auditor General, *Government resilience: extreme weather*, Session 2023-24, HC 314, National Audit Office, December 2023; and Comptroller and Auditor General, *Resilience to flooding*, Session 2023-24, HC 189, National Audit Office, November 2023.

9 We have undertaken this report at this time because the government has assessed that the cyber threat is rapidly increasing, has started collecting detailed and reliable data on its cyber resilience in 2024, and planned to achieve key parts of the Strategy by 2025. This report focuses on the cyber resilience of ministerial and non-ministerial departments and their arm's-length bodies (which we refer to in this report as 'departments'). This report does not cover the cyber resilience of local government, public corporations, businesses or UK society more widely. This report focuses on the cyber resilience of IT systems at the 'official' level of security classification and not systems classified as 'secret' or above.

Evaluative criteria

10 To assess if the government's efforts to improve its cyber security are providing value for money, we considered whether:

- the centre of government has set clear, risk-based cyber resilience outcomes for departments to meet; or
- provided the right support and incentives to allow departments to do so; and whether
- departments have appropriately prioritised, and built the capability to deliver, the cyber security they need to operate effectively.

Key findings

The threat to government cyber security

11 The size, diversity and age of the government's digital estate makes it challenging for government to be cyber resilient. Departments, arm's-length bodies and their partners use a wide range of IT systems and technology to provide public services. The breadth and diversity of these systems make it difficult for the government to assess overall cyber resilience. Many of these systems can be described as 'legacy', because they are ageing and outdated but still in use. Legacy systems are often more vulnerable to cyber attack because their creators no longer update or support their use, few people have the skills to maintain them, and they have known vulnerabilities. The government estimated that it used nearly half of its £4.7 billion IT expenditure in 2019 to keep legacy systems running. Risks to public services posed by legacy technology have built up over many years (paragraphs 1.2 to 1.3).

12 **The threat the government faces from cyber attack is rapidly evolving and is the most sophisticated it has ever been.** In December 2024, the NCSC warned of a "diffuse and dangerous" cyber threat to UK society, which grows more complex every year. Highly capable state and state-aligned actors, including from China, Russia and Iran, are using increasingly sophisticated methods to carry out malicious cyber activity. Cyber threat actors can easily access commercially and publicly available tools and services, including those provided by criminals. This enables them to perform a variety of cyber attacks, which could affect the government and the wider public sector. In December 2024, the NCSC described a "widening gap between the increasingly complex threats and our collective defensive capabilities in the UK, particularly around our critical national infrastructure". In December 2023, Parliament's Joint Committee on the National Security Strategy warned there was a high risk of a catastrophic ransomware attack at any moment. Both the cyber threat and government's cyber security capability continue to evolve as technology develops. For example, artificial intelligence can help to improve the government's cyber security but it can also help threat actors looking to interfere or undermine trust in our democratic system (paragraphs 1.4 to 1.8).

13 **Cyber attacks have devastating effects on government organisations, public services and people's lives**. Cyber threat actors routinely target government organisations. Between September 2020 and August 2021, around 40% (around 310) of the 777 incidents managed by the NCSC, because of their potential severity, were aimed at public sector organisations, including central and local government, emergency and health services, and law enforcement. The NCSC assessed that 89 of the 430 incidents it managed because of their potential severity, between September 2023 and August 2024, were "nationally significant". Cyber attacks can affect every aspect of an organisation's operation, and recovery is often lengthy and costly. For example, in October 2024, the British Library was still rebuilding its research services and IT systems a year after the cyber attack it experienced. Although the Library remained open following the attack, its research services were severely restricted in the first two months and remained incomplete following the return of a searchable version of its online catalogue in January 2024. The Library reported that the directly attributable additional costs resulting from the cyber attack totalled £600,000 by March 2024. Cyber attacks can have devastating consequences for individuals if they cannot access critical services or if their data are stolen. In June 2024, the cyber attack on a supplier of pathology services to the NHS in south-east London led to two NHS foundation trusts postponing 10,152 acute outpatient appointments and 1,710 elective procedures (paragraphs 1.9 to 1.11, Figure 1 and Appendix Two).

Progress with implementing the Government Cyber Security Strategy

14 GSG's resource constraints have limited how quickly it could implement centrally led interventions and the extent it could support departments. In November 2022, GSG created a cyber directorate to lead the government's cyber security function, support departments to implement the Strategy, and to lead interventions to improve government cyber resilience. The cyber directorate consistently reported resourcing, including recruitment and retention of staff, as a significant problem affecting the progress of its work. It had a significant shortage of staff, with around 32% of posts vacant, when it was first established. Given its resource constraints, the cyber directorate prioritised the interventions it could lead from the centre of government. Between 2022 and 2024, its work included developing 'GovAssure' (a cyber security assurance scheme) to build organisational resilience and creating a Government Cyber Coordination Centre (GC3) to help government "defend as one". The cyber directorate made limited progress in leading work to meet other strategic objectives that would help to improve government cyber resilience, such as helping departments to develop the right cyber security skills, knowledge and culture (paragraphs 2.2 to 2.5 and Figure 2).

15 Until April 2023, the government did not collect detailed, reliable data about the cyber resilience of departments. Before 2023, GSG asked departments to self-assess their performance against the minimum cyber security measures it had set for them. This did not give the government a good understanding of the cyber resilience of departments or specific IT systems. GSG used these limited and subjective data to estimate that 25% of government organisations were meeting the minimum standards in 2022. In April 2023, GSG started using the NCSC's cyber assessment framework (CAF) to agree with departments what cyber resilience outcomes they needed to achieve based on their role, likelihood of being targeted by a threat actor, IT estate, and the level of risk they were prepared to take. GSG asked departments to use GovAssure to assess their cyber resilience and get independent reviewers to verify their performance. Between April 2023 and July 2024, GSG used GovAssure to begin collecting detailed, reliable data about how cyber resilient some of departments' most important IT systems were. This has provided better information than its previous approach of relying on departments' self-reported cyber resilience (paragraphs 2.6 to 2.9 and Figure 3).

16 The government has not improved its cyber resilience quickly enough to meet its aim to be "significantly hardened" to cyber attack by 2025. The GovAssure process involves GSG agreeing targeted improvement plans (TIPs) with departments to remediate the priority issues identified. By August 2024, GSG had agreed TIPs with departments. By November 2024, GSG had not commissioned progress updates but planned to do so once departments had had more opportunity to implement their TIPs. Departments will not be able to confirm whether TIPs are fully funded until the 2025 Spending Review concludes. CDDO has created an approach known as 'Secure by Design', which aims to build effective cyber security practices into new digital services and technical infrastructure. This approach could help departments in the long term, but CDDO does not expect that it will start improving services across the whole public sector until 2026. It is therefore unlikely to significantly contribute towards the Strategy's aims for the government to be "significantly hardened" to cyber attack by 2025, and the whole public sector to be resilient to known attacks by 2030 (paragraphs 2.10 to 2.14).

17 Although the government has improved its coordination of cyber security, departments still find it difficult to understand the roles and responsibilities of the cyber organisations at the centre of government. In 2016, we reported that the government's failure to coordinate how it protects information meant that many organisations had overlapping mandates and activities. In October 2016, the government successfully consolidated four organisations into the NCSC. In 2023, the Cabinet Office created the GC3. The GC3 is a collaborative partnership between GSG, CDDO and the NCSC to coordinate cyber security efforts across government so that it can "defend as one". Nonetheless, some departments did not understand the extent to which GSG or the NCSC are responsible for government's cyber resilience and incident management. There are opportunities for GSG to improve how the centre of government communicates with departments, for example, in providing advice on the cyber threat and how to respond to it. There are still challenges for GSG and CDDO to overcome in how they coordinate to build cyber security into government's digital strategies and services following the government's decision to move CDDO from the Cabinet Office to the Department for Science, Innovation & Technology (paragraphs 2.15 to 2.19 and Figure 4).

18 GSG has not had sufficient measures in place to show whether its work to strengthen government's cyber security is effective, nor does it have a plan for how government organisations could become cyber resilient by 2030. By January 2025, GSG had not created a comprehensive monitoring and evaluation framework or shared a cross-government strategy implementation plan with departments. This means GSG has not yet been able to effectively measure, monitor and evaluate the government's progress towards the Strategy's aims for 2025 and 2030, or show how well its initiatives are working, and why. Without a cross-government implementation plan, various parts of government, including departments, do not know what they need to do and by when. GSG's shortage of staff meant it has not put in place robust arrangements to oversee how departments are implementing the Strategy. For instance, in April 2024, GSG asked departments to start developing their own implementation plans, but since then it has not asked for regular progress reports. GSG is learning from the experience of international partners on how to provide more centralised capability and support to departments (paragraphs 2.20 to 2.23).

Government's cyber resilience position in 2024

19 The first year of GovAssure identified significant gaps in departments' cyber resilience, which means they are vulnerable to cyber attack. Between April 2023 and July 2024, 35 departments took part in the first year of GovAssure and self-assessed 72 IT systems, which they identified as critical to running their most important services. Independent reviewers assessed 58 of these. GovAssure data found significant gaps in departments' cyber resilience. The data highlighted multiple fundamental system controls that were at low levels of maturity across departments including asset management, protective monitoring, and response planning. GSG reported to ministers the implication of these findings: the cyber resilience risk to government was extremely high (paragraphs 3.2 to 3.4).

20 The government does not have a detailed understanding of the resilience of its legacy IT systems. In September 2023, CDDO published its legacy IT risk assessment framework. It used this to collect departments' assessments of the risks associated with their legacy systems and information on departments' plans to remediate them. These risk assessments were not detailed and included aspects of cyber security in addition to other criteria. In March 2024, departments reported using at least 228 legacy IT systems. Of these, 28% (63 of 228) were red-rated as there was a high likelihood and impact of operational and security risks occurring. GSG did not include legacy systems in GovAssure because many of its recommended system controls would not be applicable to legacy systems. This means GSG and CDDO do not have a detailed assessment of:

- the cyber security risk to departments and their essential services caused by using legacy IT; or
- how well departments have managed this risk, for example, by isolating legacy IT from the rest of their network or performing vulnerability assessments (paragraphs 3.5 to 3.7).

Challenges for departments in building cyber resilience

21 Departments have not met their responsibilities to improve their own and their wider sectors' cyber resilience. Leaders within departments have not always recognised how cyber risk is relevant to their strategic goals. Often, departments' most senior decision-making boards and non-executive boards do not include any digital leaders or directors with cyber expertise. In April 2024, GSG recommended to ministers that departments strengthen their accountability for cyber risk through improved reporting and risk management. In 2024, GovAssure data showed that departments were not meeting their responsibility to be cyber resilient. Additionally, the government did not have sufficient oversight of the cyber resilience of the wider public sector, which lead government departments are responsible for. In April 2024, GSG reported that departments cited insufficient funding, number of staff, and oversight mechanisms as barriers to understanding and improving cyber resilience across the bodies they oversee. Some departments have been reluctant to share information about their cyber incidents with other parts of government, which has limited the opportunities for other organisations to learn and improve their own cyber resilience (paragraphs 4.2 to 4.9).

22 Departments' funding of other priorities and management of their financial pressures has reduced the scope of departments' cyber security work, which could increase the severity of a cyber attack when it happens. Departments' accounting officers are responsible for making decisions that protect the security of their organisations. In the 2021 Spending Review, the government announced it would invest £2.6 billion in cyber, of which it allocated £1.3 billion to departments for cyber security and legacy IT remediation. By January 2023, departments had funded the most urgent cyber priorities but risked not meeting their cyber resilience targets due to financial pressures. Since January 2023, some departments have significantly reduced the scope of their cyber security improvement programmes to fund other priorities. In March 2024, departments did not have fully funded plans to remediate around half of the government's legacy IT assets (53%, or 120 out of 228), leaving these systems increasingly vulnerable to cyber attack. Under-investment in technology and cyber security played a role in the severity of the cyber attack on the British Library (paragraphs 4.10 to 4.14 and Figures 5 and 6).

23 The government finds it difficult to recruit and retain enough people with cyber skills and to upskill its existing workforce. For more than a decade, skilled cyber security professionals have been in short supply and high demand nationally and globally. In 2023-24:

- one in three cyber security roles in central government was either vacant or filled by temporary staff (contingent labour);
- the proportion of vacancies in several departments' cyber security teams was more than 50%; and
- 70% of specialist security architects in post were temporary staff.

Departments reported that the salaries they can pay and civil service recruitment processes are barriers to hiring and keeping people with cyber skills. The Cabinet Office's cyber skills initiatives overlap with departments' own cyber skills programmes, which departments cannot always use because of government restrictions on the number of people employed. In January 2025, GSG's strategy to reduce the gap between the cyber skills the government has and the cyber skills it needs by 2030 was partially funded. The persistence of cyber skills shortages shows that the government may need to take a different approach to get the right cyber skills in government (paragraphs 4.15 to 4.19 and Appendix Three).

Conclusion

24 Cyber attacks continue to have serious consequences for government organisations, public services and people's lives, undermining the value for money of government expenditure in affected services and systems. The cyber threat to the government is severe and advancing quickly. In response, the Cabinet Office has published and started leading work to implement the first cyber strategy for government. Its work on centrally led interventions such as GovAssure and Secure by Design should improve departments' cyber resilience.

25 However, progress is slow and cyber incidents with a significant impact on government and public services are likely to happen regularly, not least because of the growing cyber threat. The government's cyber resilience levels are lower than it previously estimated, and departments have significant gaps in their system controls that are fundamental to their cyber resilience. The resilience of the hundreds of ageing legacy IT systems that departments still use is likely to be worse, and departments have no fully funded remediation plans for half of these vulnerable systems. As a result, the government will not meet its aim for its "critical functions" to be resilient to cyber attack by 2025. GSG assesses that achieving this for the wider public sector by 2030 remains ambitious, in part because this relies on departments meeting their responsibilities to keep their systems cyber resilient.

26 To avoid serious incidents, build resilience and protect the value for money of its operations, government must catch up with the acute cyber threat it faces. The government will continue to find it difficult to do so until it successfully addresses the long-standing shortage of cyber skills, strengthens accountability for cyber risk, and better manages the risks posed by legacy IT.

Recommendations

The centre of government

a **Within six months, GSG should develop, share and start using a cross-government implementation plan for the Government Cyber Security Strategy: 2022–2030 ('the Strategy').** GSG should refresh it regularly, include how the government is responding to new and severe cyber threats not covered by the Strategy and:

- bring together a comprehensive monitoring and evaluation framework that allows GSG to measure departments' performance, track and show progress towards the Strategy's outcomes, and evaluate what is working well or not, including an assessment of lessons learned from previous efforts to attract, upskill and retain cyber skills in government; and
- identify the priority actions the government needs to take to be cyber resilient by 2030, the government organisations that are accountable for those actions, the timescales within which those actions need to be taken, and the extent to which those organisations have the resource and levers needed to complete their actions.

b **Within six months, GSG should set out how the whole of government needs to operate differently, and what is needed for this transformation to be effective, so that the government can achieve its goals for cyber security and resilience.** GSG should work with the relevant bodies at the centre of government to develop and agree what governance, type and amount of funding, people and skills, and organisational structure and mandate will best enable government to achieve its objectives. This should include setting out how the centre of government will:

- provide different types of support, capability and guidance to departments;
- build cyber security into its digital and technology strategies, plans and activity from the outset; and
- clarify which aspects of cyber risk and resilience departments, GSG and other organisations are responsible for and when that responsibility moves from one organisation to another.

c **GSG should strengthen GovAssure's focus on improving cyber resilience outcomes.** GSG should:

- continue building the capacity to support departments in developing and implementing targeted improvement plans, and monitoring and evaluating progress against them;
- continue developing how GovAssure data can be used to measure departments' performance as part of its comprehensive monitoring and evaluation framework; and
- baseline government organisations' cyber resilience against organisations that are responsible for UK critical national infrastructure.

d **GSG should work with CDDO to take a more rigorous approach to understanding and mitigating the risk to government organisations' cyber resilience caused by legacy IT systems.** Learning from GovAssure and the legacy IT risk assessment framework, this approach should:

- identify the legacy systems in use across government;
- understand the risk these legacy IT systems pose to cyber resilience, the extent of departments' remediation plans, and be risk-based when prioritising security enhancements;
- assess and strengthen the security enhancements that are in place; and
- be considered alongside GovAssure when measuring government organisations' cyber resilience and performance.

e **GSG should design regular communications to ensure that senior leaders and other decision-makers across government understand the cyber threat, how it is relevant to their business outcomes and what they can do about it.** GSG should embed this into departments' board and programme governance.

Departments

f **Government departments should urgently strengthen their own governance, accountability and reporting arrangements around cyber risk.** In their annual security appraisal, accounting officers should assess their progress and performance in meeting the cyber security standards set out in Functional Standard GovS 007: Security (the Security Standard), which HM Treasury mandated in 2021. To show the importance of building a cyber security culture, accounting officers should:

- ensure that membership of their most senior decision-making board includes at least one digital leader with cyber expertise and one non-executive director with cyber expertise;
- engage with GSG to agree how the department will contribute to GSG's cross-government implementation plan;
- understand the cyber risk posed by their most critical IT systems and create and test appropriate incident response plans; and
- commission reporting that shows progress made in implementing the Strategy.

g **Working in alignment with GSG's government skills strategy, departments should make and enact plans to fill the cyber skills gaps in their workforces.** Within the next year, they should:

- undertake a gap analysis of their current cyber workforce to identify what skills are needed to enable effective implementation of the Strategy; and
- present clear and detailed improvement plans to GSG.