

Cybersecurity in police forces and fire and rescue services

Contents

Foreword	1
Recommendations	5
Introduction	9
1. Cybersecurity government policy and associated risks	12
2. Cybersecurity approaches in police forces and fire and rescue services	23
3. Local cybersecurity leadership and governance	33
4. Legacy ICT systems	43
5. Third-party ICT suppliers	48
6. Cybersecurity and the workforce	57
7. Cybersecurity monitoring and detection	61
8. Cybersecurity preparedness, resilience and recovery	65
9. How police forces and fire and rescue services operate within national cybersecurity arrangements	71

Foreword

Since 2020, [cybersecurity](#) risks have changed, shifting from those posed primarily by criminal activity to a more systemic threat involving hostile states. There have been successful [cyberattacks](#) on police forces and fire and rescue services. These attacks were disruptive, put the public at risk and were expensive to fix.

Successive governments have recognised this risk. As a result, the status of cybersecurity was increased in the UK's [National Risk Register 2025](#). Then, in 2026, the [National Cyber Strategy 2022](#) was updated through the [Government Cyber Action Plan](#). Successive governments have also updated the law to reflect the growing cybersecurity risk. For example, through the [Network and Information Systems Regulations 2018](#) and the [Cyber Security and Resilience Bill](#), which, at the time of our inspection, was before Parliament. But, given the vital role of policing and the fire and rescue service in securing public safety, it is concerning that the cybersecurity risk facing these sectors isn't mentioned in any of these initiatives.

For the police service, the white paper on police reform '[From local to national: a new model for policing](#)' provides an opportunity to improve and better co-ordinate the strategic approach to cybersecurity. A new, more centralised ICT model under stronger national leadership and co-ordination will help policing to improve its information security and cybersecurity. It is also an opportunity for policing to optimise and professionalise its legal and contractual arrangements with third-party ICT suppliers and across other ICT partnerships. Cybersecurity should be an integral part of police ICT reform.

The fire and rescue service could seize similar opportunities as part of [local government reorganisation](#). Investment and reorganisation decisions could support improvements in fire and rescue service and local government ICT, making them more cybersecure. Greater collaboration could also help the fire and rescue service improve its ICT and cybersecurity solutions. For example, through more collaborative ICT investment, it could develop its own security operations centre, employing a team of ICT security professionals to use specialist tools to continuously monitor, detect, analyse and respond to [cyber threats](#). These opportunities to strengthen cybersecurity cannot be missed.

In this context, we inspected how effectively the police and fire and rescue sectors manage their cybersecurity arrangements. We visited three police forces and three fire and rescue services. We spoke with officers and staff at all levels, including leaders, cybersecurity specialists and operational staff. We reviewed the work of several national bodies with relevant responsibilities, including the [Police Digital Service](#). And we examined reports and documents to gain insight into the sectors' cybersecurity arrangements.

We found that organisations in both sectors carried out regular assessments of the effectiveness of their cybersecurity arrangements. Fire and rescue services use the [Cyber Assessment Framework](#), designed by the government's [National Cyber Security Centre](#). The police use a modified Security Assessment for Policing framework. The data from these assessments shows both sectors are gradually improving, which is positive. However, it also shows that many forces and services have a long way to go to effectively secure their systems. The Security Assessment for Policing and Cyber Assessment Framework assessments also demonstrate recurring themes around the areas of weakness that forces and services need to address.

Many police forces and fire and rescue services need to update their ICT systems to improve resilience. Leaders we spoke to in both sectors identified these 'legacy systems' as their highest strategic risk for cybersecurity. Modernising ICT across both sectors must become a priority. All the organisations we inspected relied on legacy systems to a greater or lesser extent.

Third-party ICT arrangements (where forces and services use external suppliers to manage their ICT systems and/or hold their data) create additional cybersecurity governance and assurance challenges. This is because data and the systems it is held on are often outside the remit of the force or service's protective monitoring arrangements. This risk is particularly critical where suppliers store or manage sensitive police data, which can include information about [victims](#), [safeguarding](#), [intelligence](#) and ongoing investigations. Fire and rescue services don't hold as much sensitive data as the police. But, as many of them operate through ICT arrangements with local authorities, there is a risk to their data that is beyond their control.

The way people use ICT systems and data can create cybersecurity risks in organisations of any kind. So it was no surprise that we found this to be a significant problem in police forces and fire and rescue services. It wasn't just a lack of training and awareness that created opportunities for cyberattackers. In some of the organisations we inspected, we found poor security controls for staff joining, moving within and leaving the organisation. We also found poor password management and a lack of up-to-date approaches, such as multi-factor authentication (where users must provide two or more verification methods to gain access to systems). Some forces and services simply aren't doing enough to prevent human error from increasing the risk of cyberattacks.

We found that forces and services were improving their ability to monitor their ICT systems and detect cyberattacks. But, in many cases, there wasn't enough monitoring coverage and capability. Many of the police leaders we spoke to highlighted the benefits of the Police Digital Service's [National Management Centre](#), which has a cyber services team that can detect, identify, prevent and respond to cyberattacks across policing. However, there isn't an equivalent organisation for fire and rescue services, putting them at greater risk.

We found that preparedness and resilience arrangements were often underdeveloped in the forces and services we inspected. Effective cybersecurity depends not only on preventing attacks, but also on being prepared to respond and recover when an incident happens. All the organisations we inspected had business continuity and incident response plans in place. But some forces and services didn't have strong and tested cybersecurity-specific arrangements. Exercising and preparedness were often confined to specialist teams. We also found examples in both sectors of unsatisfactory arrangements for ICT backups and restoration, which are critical for recovering from cyberattacks.

Underpinning all these problems is a leadership issue. Several senior police and fire leaders we interviewed told us that they didn't consider cybersecurity to be part of daily operational decision-making. This has led to financial investment being directed to other more operational and tangible priorities. It is difficult for both sectors to keep up with rapid technological change and cybersecurity-related threats as a result. Most senior leaders in both sectors have operational backgrounds. They have an expert understanding of operational risks and the investment needed to mitigate them. Often, they rely on more junior technical specialists to identify and explain cybersecurity risks and mitigations.

In this report, we make 13 recommendations intended to strengthen cybersecurity by:

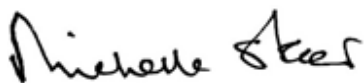
- making sure all police forces and fire and rescue services achieve baseline standards for cybersecurity capabilities;
- introducing robust external validation of fire and rescue services' assessments of their cybersecurity capabilities (as is already in place in policing);
- improving the procurement and contract management of third-party ICT suppliers in both sectors;
- enhancing collaborative arrangements between government and policing cybersecurity leads;
- promoting the use of the Police Digital Service's National Management Centre among police leaders, and creating a similar national capability for fire and rescue services;
- increasing the preparedness of fire and rescue services to respond to a cyberattack; and

- better supporting learning and development for senior leaders and cybersecurity staff in both sectors.

We intend to carry out a reinspection in due course, to assess each sector's progress in implementing these recommendations.

The full report of our inspection findings included detail of operational matters that weren't suitable for the public domain. As a result, we have prepared this version of the report with the relevant operational matters excluded.

I encourage leaders from both sectors, and those in central government who support them, to act on the recommendations in this report. Police and fire and rescue ICT systems need to become much more secure.



Michelle Skeer OBE QPM

His Majesty's Inspector of Constabulary

His Majesty's Inspector of Fire & Rescue Services

Recommendations

In this report, we make 13 recommendations. In this chapter, we have grouped the recommendations by topic. In the rest of the report, we have listed them in numerical order.

Regarding the cybersecurity of police forces

Recommendation 1

By May 2027, the [National Police Chiefs' Council](#) and the [Police Digital Service](#) should work with the following organisations to review and improve their [cybersecurity](#) processes, relationships and collaborative arrangements:

- [Report Fraud](#)
- [National Crime Agency](#)'s Triage, Incident Co-ordination and Tasking function
- [National Cyber Security Centre](#)
- Home Office Cyber Security Operations Centre
- Department for Business, Innovation, Science and Trade
- Department for Digital, Culture, Media and Sport.

Recommendation 2

By May 2027, the [National Police Chiefs' Council](#) should promote the capacity and capabilities of the [Police Digital Service](#) to help forces understand and improve their [cybersecurity](#) approaches. All forces' senior information risk owners, chief information security officers and relevant [chief officers](#) should visit the Police Digital Service [National Management Centre](#). This will help them to better understand what it does, including its use of the national police 'Defend as one' cybersecurity [critical incident](#) process.

Recommendation 3

By September 2028, each chief constable in England and Wales should make sure their force achieves and subsequently maintains a Security Assessment for Policing framework maturity level of at least 3.0.

Recommendation 10

By May 2027, each chief constable in England and Wales should:

- review existing police ICT contracts and procurement processes, and improve those that don't include adequate [cybersecurity](#) assurance; and
- adopt the government's [Secure by Design principles](#) and the [Police Digital Service's Third-Party Assurance for Policing standards](#).

Regarding the cybersecurity of fire and rescue services

Recommendation 4

By February 2027, the Ministry of Housing, Communities and Local Government should encourage all fire and rescue services in England to:

- use the [National Cyber Security Centre's Cyber Assessment Framework](#) and achieve its baseline standard; and
- implement the [Digital and Cyber Fire Standard](#).

Recommendation 5

By November 2027, all chief fire officers in England should adopt the [National Cyber Security Centre's Cyber Assessment Framework](#). All fire and rescue services in England should achieve and maintain at least the baseline Cyber Assessment Framework standard. This will also make sure that all English fire and rescue services meet the [Digital and Cyber Fire Standard](#).

Recommendation 6

By February 2027, the Ministry of Housing, Communities and Local Government should review its departmental structure and consider combining the teams responsible for overseeing the [cybersecurity](#) of local authorities and fire and rescue services. It should make sure that local government reorganisation doesn't create cybersecurity risks for fire and rescue services.

Recommendation 7

By February 2027, the [National Fire Chiefs Council](#), in consultation with the Ministry of Housing, Communities and Local Government, should refresh its '[Digital, Data and Technology strategy](#)' to include annual external validation of all English fire and rescue services' [Cyber Assessment Framework](#) assessments.

Recommendation 8

By February 2027, the [National Fire Chiefs Council](#), in consultation with the Ministry of Housing, Communities and Local Government, should update its '[Digital, Data and Technology strategy](#)' to support the procurement of cybersecure ICT and the management of third-party [cybersecurity](#) risks in all English fire and rescue services.

Recommendation 9

By May 2027, all chief fire officers in England should put measures in place to make sure that all new or renewed contracts with public sector partners or private sector third-party suppliers meet the standards set out in the [Cyber Essentials certification scheme](#) and the [Secure by Design principles](#).

Recommendation 12

By February 2027, the [National Fire Chiefs Council](#), in consultation with the Ministry of Housing, Communities and Local Government, should update its '[Digital, Data and Technology strategy](#)' to support the development of proactive [cybersecurity](#) monitoring and detection capabilities, available at all times, in all English fire and rescue services.

Recommendation 13

By February 2027, the [National Fire Chiefs Council](#), in consultation with the Ministry of Housing, Communities and Local Government, should update its '[Digital, Data and Technology strategy](#)' to support the preparedness of all English fire and rescue services to respond to a [cyberattack](#).

Regarding the cybersecurity of both police forces and fire and rescue services

Recommendation 11

By November 2027, the [National Police Chiefs' Council](#) in consultation with the [Police Digital Service](#) and the [College of Policing](#) on behalf of the police sector, and the [National Fire Chiefs Council](#) on behalf of the fire and rescue sector, should each develop their understanding of [cybersecurity](#) roles and responsibilities. They should also provide accredited learning and development to senior leaders and specialist staff.

Introduction

Background

[Cyberattacks](#) are one of the most serious risks to the UK's resilience. In 2024, there were several major cyberattacks across the private and public sectors. For example, the BBC reported that [around 10 million people had their data stolen when Transport for London \(TfL\) was hacked](#). The cyberattack also disrupted TfL's online services for months and left all 27,000 TfL employees needing to reset their passwords in person. The two men who carried out the cyberattack as teenagers were each sentenced to five years and six months in prison.

In the same year, [NHS England reported a ransomware attack on Synnovis](#) – a company that provided NHS pathology services. NHS England stated that the [ransomware](#) cyberattack caused delays to over 11,000 outpatient and elective appointments. And that the criminals responsible had published data files they had stolen during the cyberattack. A [statement made in Parliament](#) reported that, for Synnovis, the financial impact of the cyberattack was estimated to be £32.7 million.

The volume and severity of cyberattacks grew in 2025, as did media headlines highlighting their devastating effects. Incidents including high-profile attacks on Marks & Spencer, the Co-op Group and Jaguar Land Rover are a stark reminder that the [cyber threat](#) isn't just an abstract concept. It is a real threat with real-world costs.

The police and fire and rescue sectors aren't immune from cyberattack

The cyber threat to police forces and fire and rescue services is significant and expanding rapidly. Forces and services must protect their ICT systems and the data stored in them.

A major cyberattack isn't a hypothetical scenario. It has already happened to some forces and services. Many of these incidents never made headline news, largely because widespread knowledge of them could have an adverse effect on national security and public safety.

During our inspection, organisations from both sectors told us about cyberattacks they had experienced. Each one was dealt with in a way that kept the public safe. There were differences in how each sector was affected by these cyberattacks, and in their responses to manage or avert the threats and return to business as usual. But common to both sectors were the significant financial and HR costs involved in restoring normal operational activity and protecting ICT systems from further attack.

About us

His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) independently assesses the effectiveness and efficiency of police forces and fire and rescue services to make communities safer. In preparing our reports, we ask the questions that the public would ask and publish the answers in accessible form. We use our expertise to interpret the evidence and make recommendations for improvement.

Terms of reference

Our terms of reference were as follows:

"HMICFRS will carry out a [thematic inspection](#) to determine how effectively police forces and FRSs [fire and rescue services] manage [cybersecurity](#) risks.

In our inspection, we will consider how effectively police forces and FRSs:

- understand, assess and manage cybersecurity risks;
- protect their IT systems and networks from cybersecurity risks;
- implement cybersecurity detection measures that are proportionate to the known threat, harm and risk; and
- prepare for, and recover from, cybersecurity events or incidents."

Methodology

We gathered a wide range of views from policing, the fire and rescue service and other stakeholders. The inspection took place between January and May 2026, in three phases:

1. We carried out fieldwork in three police forces and three fire and rescue services.
2. We interviewed national and regional cybersecurity stakeholders.
3. We reviewed innovative or promising cybersecurity practices.

We also spoke with national organisations, regional bodies and stakeholders with responsibility for cybersecurity.

During our inspection, we:

- carried out over 30 interviews;
- completed [reality testing](#) with officers and staff across both sectors;
- consulted with over 70 other people – including from government departments, private sector cybersecurity companies, national cyber award winners and wherever we found [innovative practice](#);
- scrutinised more than 260 police service and fire and rescue service documents;
- gathered and assessed over 1,250 pieces of evidence;

- reviewed over 50 media publications and research documents; and
- gathered data from various sources for inclusion in this report.

Terminology in this report

Our reports contain references to, among other things, ‘national’ definitions, priorities, policies, systems, responsibilities and processes. In some instances, ‘national’ means applying to England, or England and Wales. In others, it means applying to England, Wales and Scotland, or the whole of the United Kingdom.

References in this report to:

- ‘the police service’ or ‘policing’ relate to the 43 Home Office police forces in England and Wales;
- ‘the fire and rescue sector’ or ‘the fire and rescue service’ relate to the 44 fire and rescue services in England;
- the ‘sectors’ or the ‘inspected sectors’ relate to the police service and the fire and rescue service taken together; and
- ‘the inspected organisations’ relate to the three police forces and three fire and rescue services we inspected during our fieldwork.

1. Cybersecurity government policy and associated risks

Cybersecurity risks in the UK and globally are increasing in scale, complexity and impact

[Cybersecurity](#) presents a growing risk to the UK's economy, [critical infrastructure](#) and public services. The [National Cyber Security Centre \(NCSC\)](#), part of Government Communications Headquarters, is the National Technical Authority for cybersecurity. The NCSC told us that it “co-ordinates the response to the majority of serious cyber incidents affecting the UK and supports the defence of the UK's most critical systems”.

The NCSC has consistently warned that the [cyber threat](#) facing the UK is becoming more complex and severe. In its annual reviews, it highlights increasing activity by hostile states and [organised crime groups](#), among others. It also emphasises that many organisations underestimate the scale of the risk and the consequences of a successful [cyberattack](#).

In its '[Annual Review 2025](#)', the NCSC reported that almost half of the cyber incidents it managed during the previous year were of national significance. Some were assessed as having the potential to cause serious disruption to government, essential services and the wider economy.

Police forces and fire and rescue services operate within an increasingly hostile cyber environment. This makes effective cybersecurity arrangements essential to maintaining public safety and operational resilience.

The Police Digital Service has an important role in policing's cybersecurity

In 2021, the government established the [Police Digital Service \(PDS\)](#). The PDS is governed jointly by [police and crime commissioners](#), chief officers (through the [National Police Chiefs' Council](#)) and the Home Office.

It works with the 43 police forces in England and Wales, the [National Crime Agency \(NCA\)](#), the [College of Policing](#) and the [Association of Police and Crime Commissioners](#).

The PDS also provides support to British Transport Police, the Civil Nuclear Constabulary, Guernsey Police, the Ministry of Defence Police, the Police Service of Northern Ireland, Police Scotland, the Service Police and the States of Jersey Police.

Police and crime commissioners provide core funding for the PDS. It also receives a combination of Home Office funding and contributions from policing, including subscriptions paid by police and crime commissioners on behalf of their forces.

The PDS works with law enforcement organisations, industry, charities, public bodies and government to provide digital services and solutions for policing. It also co-ordinates, develops, implements and manages digital services and solutions that help UK policing to safely use and harness technology to improve public safety.

It helps forces manage cybersecurity risk by, among other things:

- setting cybersecurity standards;
- providing cybersecurity leadership training;
- designing and implementing the Police Cyber Assurance Framework;
- establishing and independently evaluating the Security Assessment for Policing framework;
- gathering, assessing and communicating cybersecurity threat [intelligence](#); and
- providing specialist cybersecurity capabilities through its [National Management Centre](#) that monitor, identify, detect and respond to local force cybersecurity breaches and national police cyberattacks.

The PDS shares information on cybersecurity threats

The PDS records and analyses information and intelligence relating to cybersecurity threats to policing. It shares this with police forces to help them to understand the global cyber threat landscape and the different types of cyber risks and threats.

The fire and rescue sector doesn't have an equivalent cybersecurity threat intelligence capability. We think it should.

The National Police Chiefs' Council and the PDS gave us the latest data about global cybersecurity threats. The data showed that:

- cyberattacks happen every 11 seconds;
- [ransomware](#) cyberattacks happen every 120 seconds; and
- phishing attempts (when criminals send scam emails or texts that share links to websites containing harmful software, or trick users into revealing sensitive information) happen every 2 seconds.

The PDS also collects data and analyses cyberattacks on policing, as well as other cybersecurity incidents it classifies as ‘near misses’. A near miss, in this context, is where there has been a cybersecurity incident but no harmful data or ICT systems breach. Between January and March 2026, its data showed that there were 252 cybersecurity incidents and 796 near misses. These included:

- malware attacks – the use of malicious computer software designed by cybercriminals to disrupt, damage or gain unauthorised access to police computer systems;
- someone trying to access police systems without the right level of authorisation; or
- accidental but unauthorised data disclosures by the police workforce.

Government cybersecurity policy doesn’t adequately recognise or prioritise risks to policing and the fire and rescue service

Government strategy and policy miss opportunities to improve cyber resilience in both sectors

Cybersecurity risks and actions are included in several government strategies, policies and action plans, as well as in the National Risk Register (NRR). The [Cyber Security and Resilience Bill 2025](#) also contains proposals for stronger cybersecurity regulation. But we are concerned that the risks to police forces and fire and rescue services aren’t properly represented or given a high enough priority.

The National Cyber Strategy 2022

The ‘[National Cyber Strategy 2022](#)’ set out the then government’s approach to protecting and promoting the UK’s cybersecurity interests. Strategic cybersecurity objectives include:

- improving the understanding of cyber risk;
- preventing and resisting cyberattacks; and
- strengthening resilience to respond to and recover from cyberattacks.

In the strategy, the government envisaged a significant role for policing and other law enforcement bodies in tackling cybercrime, including:

- the NCA [National Cyber Crime Unit](#);
- regional cyber crime units;
- the Metropolitan Police’s cyber crime unit;
- local cyber crime units in each police force; and
- [Report Fraud](#) (formerly Action Fraud).

But the strategy didn’t include anything about securing police forces and fire and rescue services from cyberattack. We think this was a missed opportunity to set clear direction and expectations for protecting these critical public safety services.

The Government Cyber Action Plan 2026

In January 2026, the government introduced the '[Government Cyber Action Plan](#)', updating the 2022 strategy. Through the action plan, the government aims to address many of the issues we identified as concerns in our inspection. But it focuses on the cybersecurity of the national government and governmental investment only – and not on policing or the fire and rescue service. For example, the action plan sets out how the government will:

- create investment in cybersecurity through a new Government Cyber Unit in the Department for Science, Innovation and Technology at a cost of £210 million;
- make civil service leaders directly accountable for mitigating the cybersecurity risk to their departments;
- raise concerns about the vulnerability of legacy systems and historical underinvestment in cybersecurity (an important finding in our inspection, across both sectors, which we discuss further in [chapter 4, 'Legacy ICT systems'](#)); and
- introduce a new government cybersecurity profession to attract talent and develop skills.

Police forces and fire and rescue services face many cybersecurity challenges. But the plan contains little to improve or invest in their cybersecurity. We were surprised that the plan didn't include references to either of these sectors. No government cybersecurity stakeholder that we interviewed could explain why policing and the fire and rescue sector were excluded from the action plan.

As with the 2022 strategy, the government didn't explicitly consider the police and fire and rescue sectors within the remit of the new 2026 action plan. This is another missed opportunity. For example, it could have supported both sectors by requiring them to appoint a board-level cybersecurity expert, as government departments must do. Bringing their cybersecurity staff in line with the new government profession would strengthen the cybersecurity capability of forces and services.

The Cyber Security and Resilience Bill 2025

In November 2025, the government introduced the Cyber Security and Resilience Bill 2025 (the Bill) to Parliament. The Bill proposes new cybersecurity duties that would apply to a much wider range of public services than before.

The Bill sets out proposed reforms to the [Network and Information Systems Regulations 2018](#) (NIS regulations) that place security and resilience duties on organisations providing essential services and some digital services. At the time of our inspection, the NIS regulations applied to operators of essential services including energy suppliers, transport networks, the health sector, water companies and digital infrastructure.

But these regulations don't apply to the police or the fire and rescue service. This omission seems strange, especially as they do apply to other public and emergency services. [Schedule 1 of the Civil Contingencies Act 2004](#) – that defines and categorises emergency responders – classifies the police service and the fire and rescue service as the highest category of responders (category 1). Other category 1 responders include local authorities, the NHS and the Environment Agency, some of which are included in the NIS regulations.

The Bill changes and expands the original NIS regulations in three main ways:

1. It extends the regulations to organisations that weren't previously in scope, including medium and large data centres and managed service providers of ICT helpdesks and cybersecurity facilities. This may protect forces and services that use these third-party suppliers from the risks associated with vulnerabilities in their cybersecurity arrangements.
2. It strengthens the powers that regulators will have to make sure organisations meet the duties placed on them by the NIS regulations.
3. It provides the government with more powers to make changes to the regulatory regime via secondary legislation and by issuing directions; this would help the government to regulate policing and fire and rescue service cybersecurity arrangements in the future.

It is helpful that the Bill will bring some of the third-party suppliers that policing and the fire and rescue service rely on within the scope of the NIS regulations.

However, the Bill stops short of providing any specific guidance or regulations relating to policing and the fire and rescue service. During our inspection, we asked various government cybersecurity leaders whether they could explain this. None were able to.

It is concerning that neither sector is considered in the Bill. Because if either sector was seriously disrupted by a cyberattack – and unable to respond to emergencies or carry out their core functions – there would be serious consequences.

The National Risk Register

Since 2020, cybersecurity risks have changed, shifting from those posed primarily by criminal activity to a more systemic threat involving hostile states. Successive governments have recognised the threat to the UK's essential services and economic stability by increasing the status of cybersecurity in the UK's National Risk Register (NRR).

Chapter 4 of the [National Risk Register 2025](#) (the most recent NRR) sets out the register's risk summaries under thematic headings, one of which is Cyber. The risks identified under this heading relate to cyberattacks on the health and social care system, the transport sector and telecommunications systems.

This chapter also contains cyber elements under other headings. For example, the Terrorism category includes cyberattacks affecting civil nuclear systems and on gas, electricity or fuel supply infrastructure. The State Threats category includes the risk of a cyberattack on a UK retail bank.

An attack on police or fire and rescue service networks and systems isn't included in the NRR as a risk. However, forces and services are a crucial part of the planned response to many of the risks that the NRR does focus on. Disruption to police and fire and rescue ICT systems and networks, and their ability to operate to keep the public safe, is a significant risk. We support the government's focus on the risks presented by cyberattacks. But given the public safety role of policing and the fire and rescue service, it seems unusual that neither sector is mentioned in the NRR in the context of their cybersecurity risks or responses.

The national cybersecurity network across both sectors and government departments is fragmented

National co-ordination and governance roles and responsibilities are unclear

During our inspection, we found widespread concern about fragmented governance, unclear accountabilities and inconsistent collaboration across the national cybersecurity landscape.

Senior leaders from policing, government departments and other national bodies described a complex network of organisations with overlapping responsibilities but limited co-ordination. We found little evidence of co-ordinated planning between the Home Office and the Ministry of Housing, Communities and Local Government. There was also limited evidence of joint exercising (planned emergency testing) between policing and the fire and rescue sector to test cyber resilience.

Several stakeholders described siloed working and inconsistent approaches to information sharing. This reduces the effectiveness of national cybersecurity arrangements and hinders efforts to improve resilience.

Many others told us that leadership and governance arrangements for cybersecurity at a national level remained unclear. We heard concerns about fragmented responsibilities, duplication of effort, inconsistent decision-making, gaps in oversight and limited strategic co-ordination. This uncertainty about roles and responsibilities can reduce the effectiveness of national cybersecurity arrangements.

Some interviewees believed that a clearer national model for cybersecurity was needed. They said there should be greater clarity about who was responsible for national cyber resilience, how organisations should work together and where accountability sat.

A clearer governance framework would help organisations understand their responsibilities, improve collaboration and strengthen national cyber resilience.

The National Cyber Security Centre has an important role but support for both sectors is limited

The National Cyber Security Centre (NCSC) told us that responsibility for cybersecurity rested primarily with individual organisations and their lead government departments. It also stated that it didn't routinely assess the cybersecurity of police forces and fire and rescue services. But it does share threat assessments, where appropriate.

While this position is clear, many people we interviewed believed there was still uncertainty about the responsibilities of national organisations involved in cybersecurity. We found differing views about the level of support available and the extent to which national organisations should help forces and services to improve their cyber resilience.

The '[Government Cyber Security Strategy: 2022 to 2030](#)' states that all public sector organisations should comply with guidance contained within it. It also states that they should be working to identify, prevent, detect and respond to cybersecurity threats. And that they should 'Defend as one' in response to a cyberattack, a concept explained in pillar 2 of the strategy. But we found that this wasn't always the case.

We found that, in practice, the NCSC provided only limited support, advice and cybersecurity threat intelligence to the policing and fire and rescue sectors. The NCSC attended both sectors' national cybersecurity meetings. But many of the people we spoke to were frustrated that the NCSC shared little information and intelligence about specific cybersecurity threats with them. Several PDS representatives told us they gave the NCSC lots of information about police cybersecurity threats and risks but received very little in return.

Information sharing and co-ordination can be challenging

The effectiveness of cybersecurity arrangements depends on timely information sharing and co-ordinated responses. Some interviewees expressed frustration about how things worked at the time of our inspection. Some police leaders and PDS representatives believed intelligence sharing was inconsistent and that national co-ordination could be improved. We also found examples where fragmented reporting arrangements delayed information sharing and reduced the effectiveness of incident responses.

Given the importance of cybersecurity to public safety, we consider that stronger collaboration and clearer communication are needed across all organisations involved.

Recommendation 1

By May 2027, the [National Police Chiefs' Council](#) and the [Police Digital Service](#) should work with the following organisations to review and improve their [cybersecurity](#) processes, relationships and collaborative arrangements:

- [Report Fraud](#)
- [National Crime Agency](#)'s Triage, Incident Co-ordination and Tasking function
- [National Cyber Security Centre](#)
- Home Office Cyber Security Operations Centre
- Department for Business, Innovation, Science and Trade
- Department for Digital, Culture, Media and Sport.

Cyberattacks are already causing significant disruption to policing and the fire and rescue service

Cyberattacks affecting emergency services aren't theoretical risks. Recent incidents have demonstrated their potential to disrupt vital services.

During our inspection, we identified examples of police forces and fire and rescue services experiencing cyberattacks. These incidents affected operational systems, compromised data and disrupted services that help protect the public. Many leaders told us that further attacks were highly likely.

We found varying levels of understanding of cyber risk across both sectors. In some organisations, cybersecurity was viewed primarily as a technical issue. In others, particularly those that had experienced cyberattacks, leaders had a much greater appreciation of the operational consequences and associated risks to public safety.

The increasing sophistication of cyber threats, combined with growing dependence on technology, means that these risks are likely to continue increasing. But cyber threats are growing faster than both sectors' capacity to respond.

We acknowledge that it is difficult for both sectors to keep up with rapid technological change and the many cybersecurity risks they face. But police and fire and rescue leaders need to prioritise and invest money and resources in their cybersecurity. Cybersecurity should be viewed as a core organisational priority and not solely a technical risk. Both sectors need to improve their ability to prevent, detect, respond to and recover from cyberattacks.

Lack of funding is a barrier to improving cybersecurity, particularly in the fire and rescue sector

During our inspection, there was one message we heard repeatedly from many senior leaders in police forces and fire and rescue services. They told us they couldn't invest in the technology needed to secure their systems and networks from cyberattack because of a lack of funding. For example, they pointed to a need for capital funding to replace legacy ICT systems and buy cybersecurity software.

We agree that this is a significant barrier and that cybersecurity isn't cheap. According to the Department for Science, Innovation and Technology, in 2023 alone, public sector organisations, including police forces and fire and rescue services, awarded 963 contracts to UK-based cybersecurity businesses. These were worth a combined £772 million. Some capabilities can be particularly costly. One example of this is a security operations centre where a team of ICT security professionals uses specialist tools to continuously monitor, detect, analyse and respond to cyber threats. This is part of the reason why, in 2025, only seven English fire and rescue services had a security operations centre in place, according to the [National Fire Chiefs Council](#).

But the cost of investing in cybersecurity is only part of the picture. We asked for a breakdown of what each sector spent on its cybersecurity, but these figures weren't available. However, in 2024/25, police forces spent more than £16 billion, of which £1 billion was spent on ICT (6.4 percent of total expenditure). While fire and rescue services spent £2.76 billion, of which £24 million was spent on ICT (only 0.88 percent of their total expenditure). This shows that fire and rescue services spend a relatively small percentage of their overall budget on ICT. So we conclude that the cost barrier is as much about prioritisation as it is affordability.

Prioritising investment in cybersecurity over other operational needs is difficult

Almost all senior leaders we interviewed told us a lack of funding was a barrier to improving cybersecurity. Some said they could theoretically increase their ICT spending. But some also clarified that this would only be affordable if they reduced spending on operational requirements; a choice they were unwilling to make.

Balancing frontline operational needs against those of supporting functions, such as ICT, is a challenging test of leadership, especially when in a tight financial position. The primary concern of police and fire and rescue leaders in these cases is, rightly, the protection of the public.

But we identified other factors that influenced investment decisions. Senior leaders in police forces and fire and rescue services usually have operational backgrounds, having risen through the ranks of their organisations. This means they have an expert understanding of operational risks and the investment needed to mitigate them.

However, leaders often rely on more junior technical specialists to identify and explain non-operational risks and mitigations. Many of the cybersecurity experts we spoke to said it was a challenge to communicate technical risks in a clear and compelling way to their seniors without this expertise.

Compared to operational risks, cybersecurity risks can be difficult to describe and understand. They often involve subjective judgment about how likely incidents are to happen and what their effects might be.

Other factors include governance bodies, the media and the public holding sector leaders more strongly to account for how they manage operational risks than cybersecurity risks. And, in some cases, government specifies that funding has to be spent on a specific operational purpose.

Collaboration could make investment in cybersecurity more affordable

During our inspection, we were struck by the difference between the police and fire and rescue sectors regarding the extent to which they collaborated and used national solutions.

Security operations centre capabilities illustrate this point. The PDS provides a security operations centre function, through its National Management Centre's cyber security team, to 42 police forces in England and Wales and other national police organisations. The Metropolitan Police Service has a different security operations centre arrangement.

The PDS also provides cybersecurity assurance support to other law enforcement agencies, including the British Transport Police, the College of Policing, the Mayor's Office for Policing and Crime, the NCA and the Police Service of Northern Ireland. The PDS is a not-for-profit membership organisation. Its cyber services team functions are funded by contributions from the forces and agencies it supports.

Unlike policing, the fire and rescue service doesn't have any centralised service-wide security operations centre capacity and capability. The 2025 fire and rescue service Cyber Assessment Framework assessments highlighted this as a weakness.

The National Fire Chiefs Council identified this as a critical issue for the sector. There is an opportunity here for the fire and rescue sector to adopt a more collaborative approach to improve resilience, strengthen capability and reduce duplication. Doing this could make cybersecurity measures more affordable. Fire and rescue leaders should consider cybersecurity investment as a means of protecting operational effectiveness rather than competing with it.

Prevention is more effective and less costly than responding to a cyberattack

Both sectors urgently need to prioritise and invest in cybersecurity. Evidence from recent cyberattacks shows there are real consequences if action is delayed.

Without improvement, risks will continue to grow, and effects will become more severe.

Prevention is more effective and less costly than responding to major incidents.

Early, sustained investment in cybersecurity can reduce or avoid attacks and prevent far greater financial and operational damage later.

Modern, secure systems must be treated as a core strategic and operational priority.

The threat is increasing, and the likelihood of a significant cyberattack isn't a question of if, but when. Police forces, fire and rescue services and government departments should therefore prioritise cybersecurity investment, improve collaboration and strengthen resilience before a serious cyberattack happens.

2. Cybersecurity approaches in police forces and fire and rescue services

Policing has a strong national cybersecurity approach, but performance and consistency need to improve

Policing nationally has a clear strategic direction and robust approach to [cybersecurity](#). It understands the cybersecurity risks and what is needed to mitigate and manage them. There are two [National Police Chiefs' Council \(NPCC\)](#) portfolios that lead the work on information and cybersecurity:

- the NPCC Digital, Data and Technology structure, which endorses and promotes this work through the '[National Policing Digital Strategy 2025–2030](#)'; and
- the Police Information Assurance Board (PIAB), which governs national cybersecurity work through an agreed NPCC [National Policing Cyber Security Strategy](#) and provides the strategic lead for information security, risk management and cyber resilience across UK policing.

The police cybersecurity strategy is consistent with the objectives and outcomes set out in the '[Government Cyber Security Strategy: 2022 to 2030](#)'. It follows the government's "core pillars of building organisational cyber resilience" and the concept of 'Defend as one' (pillar 2). It recognises that the scale and pace of cybersecurity risks demand a comprehensive and joined-up response. And acknowledges the need for a more mature and robust approach to cybersecurity prioritisation and assurance.

A chief constable chairs each portfolio and board. Both boards have deputy chairs with specialist technological and information security backgrounds and accreditation. We found there was robust leadership, governance and processes across both portfolios. Both boards had action plans or frameworks to implement critical pieces of work. Taken together, policing has a strong ICT reform strategy that places great importance on cybersecure and resilient digital services.

But, because all police forces have operational independence, neither NPCC board has the power to make an individual force or a chief constable act.

We reviewed PIAB cybersecurity governance arrangements, including board papers, risk registers and threat [intelligence](#) documents. We found the board was well managed and supported by the [Police Digital Service \(PDS\)](#), which provides specialist expertise and detailed performance analysis. All police forces were represented.

The PIAB oversees cybersecurity assurance and maturity, cyber risks, legacy technology, third-party supplier risks, threat intelligence and guidance. It also monitors performance and promotes [Secure by Design principles](#) for police ICT.

Policing has made substantial progress in recent years, including on its work to standardise technical security controls. The establishment of the PDS cyber services team has also improved cybersecurity risk management, threat intelligence and independent assurance processes. It has also helped to build stronger relationships with national cybersecurity partners.

Despite this progress, policing recognises that further improvement is needed. Significant variation remains between forces. More work is required to improve cyber maturity, replace legacy technology and strengthen oversight of third-party ICT suppliers.

The PDS has an important role in supporting police forces with their cybersecurity

The PDS provides vital national digital leadership, technical expertise and operational co-ordination where forces don't have the specialist knowledge and resources to manage growing cybersecurity risks.

The PDS supports forces to manage digital risk, protect sensitive information and maintain critical systems. It helps them to detect [cyber threats](#) and respond to serious cybersecurity incidents that could disrupt policing or cause harm to the public. The PDS also works with forces to identify shared threats, manage common dependencies and reduce duplication.

Its role includes setting and improving digital standards and guidance, particularly where systems are shared nationally or present a higher cybersecurity risk.

The PDS also produces a wide range of training modules for senior police leaders and cybersecurity specialists. It has professionalised the police approach to cybersecurity standards, guidance, and learning and development. And it supports national police cybersecurity exercises (planned emergency testing).

It has helped policing to build its cybersecurity capacity, capability and specialist support. Many police forces have limited cybersecurity capacity and rely on small numbers of specialists. The PDS supports forces by providing access to specialist cybersecurity expertise. This includes advice on technical architecture, monitoring, incident response and recovery. In this way, the PDS helps strengthen resilience across policing, particularly in smaller forces or those with limited resources.

The PDS National Management Centre co-ordinates the national police response to cyberattacks

In 2019, the PDS introduced its [National Management Centre \(NMC\)](#) to provide policing with protective cybersecurity monitoring across a range of ICT systems. The NMC acts as the national police security operations centre. It employs a team of ICT security professionals to use specialist tools to continuously monitor, detect, analyse and respond to cyber threats affecting policing. This role is particularly important as it helps policing to have an effective and joined-up response to [cyberattacks](#) or incidents. It provides protective monitoring and threat intelligence to help forces to identify threats earlier. It also offers co-ordination support to make sure policing can respond consistently to cyber threats and complex incidents across multiple forces.

Since 2020, the NMC has expanded in both scale and capability. In 2026, when we visited, the NMC had more than 70 specialists in its cyber services team. And it now supports all police forces and national policing systems. This growth reflects the increasing scale, frequency and complexity of cybersecurity threats affecting policing. It has been able to strengthen its protective monitoring, analytical and co-ordination functions. It also adopted emerging technologies to improve threat intelligence, detection and incident response. This has helped to improve the ability of policing to identify threats earlier and co-ordinate risk-based responses across multiple forces.

The NMC provides the national policing critical incident response to a cyberattack. It does this using an operating framework known as 'Defend as one' (DA1). It follows the strategic concept set out in the 'Government Cyber Security Strategy: 2022 to 2030' (see pillar 2).

The DA1 process provides a nationally co-ordinated police gold command and control approach to managing the most serious cybersecurity incidents affecting police ICT systems, data and supply chains. It is intended to reduce the risk of police system compromise, prevent further data loss and limit harm to [vulnerable people](#).

When DA1 is activated, the NMC:

- appoints a trained gold incident commander (normally a senior [police officer](#) from the NPCC DA1 cadre);
- analyses the national threat and risks to policing;
- issues clear instructions to police forces;
- manages communications with suppliers and national partners; and
- supports transition from a technical cybersecurity response to actions that might be needed to [safeguard](#) people or personal information.

During DA1 responses to cyberattacks on third-party suppliers or nationally used systems, the NMC supports policing to quickly understand the situation and co-ordinate a consistent, risk-based response. It provides technical analysis and advice to forces, and gathers, analyses and shares cybersecurity threat intelligence across policing.

The NMC collaborates with other cybersecurity partners. It shares information about vulnerabilities, active threats and emerging risks. This information helps forces and other organisations prioritise action, strengthen controls and make informed decisions about risk. The NMC also supports national police learning and development following cyberattacks, by carrying out national debriefing events.

The PDS manages and supports cybersecurity assurance in policing

Digital systems support almost every aspect of modern policing. Policing relies on secure and resilient technology to support intelligence, safeguarding, investigations and partnership working. Effective cybersecurity assurance is essential.

In 2023, as part of its Police Cyber Assurance Framework, the PDS introduced the Security Assessment for Policing (SyAP) framework. SyAP replaced earlier assurance arrangements and provides a more structured and consistent assessment framework.

SyAP assesses cybersecurity maturity across five functions – identify, protect, detect, respond and recover – using a scoring scale from 1.0 (lowest maturity) to 5.0 (highest maturity).

At the time of our inspection, forces were expected to achieve at least maturity level 2.0 across all assessment areas. The framework gives forces a consistent understanding of cybersecurity risk. It helps identify vulnerabilities, measure progress and highlight areas needing improvement.

Police cybersecurity maturity levels vary across different capabilities and between forces

National SyAP results indicate that policing has improved its cybersecurity maturity over time. National performance now generally exceeds the expected baseline requirement. The PDS produces annual reports for each force to help them to understand their level of cyber maturity and identify areas where they need to improve.

Many cybersecurity specialists told us that SyAP had improved consistency across policing. They said it reduced duplication and created a common framework for discussing cybersecurity risks. It also helps identify shared vulnerabilities, including legacy technology, supplier dependencies and weaknesses in monitoring and detection capabilities.

Despite these strengths, we found considerable variation in cybersecurity maturity between forces. The SyAP framework on its own doesn't guarantee consistent cybersecurity outcomes. Forces remain responsible for acting on assurance findings, investing in improvements and managing risks within their own ICT systems. Several police cybersecurity leaders told us that significant risks remained. For example, where forces didn't have enough cybersecurity resources or capability, or where cybersecurity wasn't an organisational priority.

We found that some forces used the SyAP framework as a tool to improve cybersecurity and support informed decision-making. Others appeared to treat it primarily as a compliance exercise. In these cases, we found less evidence that weaknesses identified during the SyAP process led to meaningful action.

The framework also relies heavily on evidence provided by forces. The PDS provides scrutiny and challenge. But it can't independently validate every force's assessment because it doesn't have direct access to all the technology resources that forces use.

We are concerned that national assurance arrangements don't extend across the whole of policing's ICT estate. This means all the ICT assets an organisation owns or uses to support its operations, including hardware, software, data, networks and [cloud services](#). This is particularly challenging where forces rely on third-party suppliers, partner organisations and shared ICT environments. In many cases, neither forces nor the PDS have direct control over these systems. As a result, significant parts of the policing technology landscape sit outside national monitoring and assurance arrangements. This creates additional cybersecurity risks.

As cybersecurity risks to policing increase, the sector's performance must improve

Policing faces increasing cyber threats and must continue improving its cybersecurity resilience. The NMC provides protective monitoring and threat intelligence across elements of policing's digital infrastructure. However, the PDS acknowledged that it didn't have complete visibility across the full policing ICT estate.

We are concerned that the number and complexity of systems in use across policing create additional risk. Greater oversight is needed to manage these risks effectively.

Some forces have chosen to invest in cybersecurity capabilities beyond those provided nationally. One force has invested in additional protective monitoring arrangements covering its whole ICT estate. However, this level of investment may not be affordable for all forces.

PIAB has recognised the need to increase cybersecurity maturity across policing. In April 2026, it approved an increase in the SyAP baseline requirement from level 2.0 to level 3.0 for all assessment categories by September 2028. The PDS describes maturity level 3.0 as: “A process that has sets of defined and documented standard processes. That enables consistency of process performance across the organisation.”

We support the decision to increase the baseline maturity requirement. This is a necessary step towards improving resilience and reducing cyber risk across policing.

Recommendation 2

By May 2027, the [National Police Chiefs' Council](#) should promote the capacity and capabilities of the [Police Digital Service](#) to help forces understand and improve their [cybersecurity](#) approaches. All forces' senior information risk owners, chief information security officers and relevant [chief officers](#) should visit the Police Digital Service [National Management Centre](#). This will help them to better understand what it does, including its use of the national police 'Defend as one' cybersecurity [critical incident](#) process.

Recommendation 3

By September 2028, each chief constable in England and Wales should make sure their force achieves and subsequently maintains a Security Assessment for Policing framework maturity level of at least 3.0.

Progress has been made in fire and rescue cybersecurity, but capability and co-ordination remain limited

Compared to policing, the fire and rescue sector is less advanced in its approach to cybersecurity. The absence of a national organisation comparable to the PDS limits the sector's ability to co-ordinate activity, share intelligence and respond collectively to cyber threats.

The fire and rescue sector also has no equivalent to the PDS NMC. This means responsibility for monitoring and protecting ICT systems remains largely with individual fire and rescue services. Many services have limited cybersecurity resources and expertise. We found this to be a significant weakness.

Some fire and rescue leaders we interviewed perceived the cybersecurity risks to be lower for their sector than for policing. Their views were based on the belief that the fire and rescue service holds less sensitive information than policing. And that it operates using less complex ICT estates.

While this is true, we found that the sector still held a wide range of sensitive information. This includes the personal, operational and organisational data the fire and rescue service needs to carry out its role. Examples include personal information held in fire safety records and site-specific information about [critical national infrastructure](#). Such information could be valuable to cyberattackers who want to disrupt services or steal data.

Fire and rescue services shouldn't underestimate the value of the information they hold or the consequences of a successful cyberattack. The risk to the sector isn't necessarily lower than that faced by policing. In some cases, its reliance on outdated technology and legacy systems may increase its vulnerability.

The fire and rescue service has improved its cyber assurance

In 2022, there was a cyberattack on Humberside Fire and Rescue Service. In response to this, and the increasing threat from state-sponsored hacking groups, the Home Office commissioned a piece of work from IBM Security. It was asked to support 20 of the 44 fire and rescue services to complete a [National Cyber Security Centre Cyber Assessment Framework \(CAF\)](#) questionnaire. The Home Office and the National Fire Chiefs Council selected the 20 services that took part.

This initial assessment identified wide variation in cyber maturity across the sector. It resulted in 13 recommendations for improvement. But, at the time of our inspection, the sector hadn't fully implemented many of these recommendations.

Since then, the fire and rescue sector's use of the CAF has become more widespread. Services now carry out annual assessments of both corporate systems and [control room](#) technology and processes. The results show gradual improvement. At the time of our inspection, more services were meeting the baseline standard than in previous years. However, progress remains slow and significant improvement is still needed across the sector.

The most common areas needing improvement relate to asset and device management, incident response planning, assurance processes and planned emergency testing arrangements. We think services could improve these areas quickly through stronger prioritisation and governance. All services should work towards achieving the baseline CAF standard as soon as practicable.

The government has a role to play in improving the fire and rescue service's cybersecurity assurance

Fire and rescue services governed by council-based [fire and rescue authorities](#) often use their council's corporate systems rather than maintaining their own. But within the Ministry of Housing, Communities and Local Government (MHCLG), the team overseeing local authorities' cybersecurity is different to the one that oversees cybersecurity in fire and rescue services. This is a consequence of [the 2025 Machinery of Government changes](#), prior to which the Home Office had responsibility for the fire and rescue sector and MHCLG was responsible for local authorities.

The two MHCLG teams are working to integrate their cyber response. But, at the time of our inspection, they weren't yet closely aligned. Specifically, we found differences in priorities and levels of investment, and in how CAF assessments were carried out.

Without adequate co-ordination between these teams, the government's programme of local government reorganisation is likely to create cybersecurity risks for fire and rescue services. For example, when services move their corporate systems from one local authority to another or if they establish their own systems under the new structures.

It is also possible that organisational attention, leadership capacity, investment decisions and scarce specialist resources could become increasingly directed towards structural reform. This could delay essential work to replace legacy ICT systems and assurance activity. There is a risk that difficult investment decisions could be deferred in the hope that reorganisation will resolve existing challenges. MHCLG should consider these risks and provide the necessary support to fire and rescue services in this position.

Recommendation 4

By February 2027, the Ministry of Housing, Communities and Local Government should encourage all fire and rescue services in England to:

- use the [National Cyber Security Centre's Cyber Assessment Framework](#) and achieve its baseline standard; and
- implement the [Digital and Cyber Fire Standard](#).

Recommendation 5

By November 2027, all chief fire officers in England should adopt the [National Cyber Security Centre's Cyber Assessment Framework](#). All fire and rescue services in England should achieve and maintain at least the baseline Cyber Assessment Framework standard. This will also make sure that all English fire and rescue services meet the [Digital and Cyber Fire Standard](#).

Recommendation 6

By February 2027, the Ministry of Housing, Communities and Local Government should review its departmental structure and consider combining the teams responsible for overseeing the [cybersecurity](#) of local authorities and fire and rescue services. It should make sure that local government reorganisation doesn't create cybersecurity risks for fire and rescue services.

The role of the National Fire Chiefs Council

In 2022, the National Fire Chiefs Council established its cybersecurity programme. Since then, it has:

- established national cyber working groups;
- developed a sector cyber action plan;
- appointed strategic cyber leadership roles;
- introduced cyber learning products;
- improved cyber threat intelligence sharing; and
- developed a '[Digital, Data and Technology strategy](#)'.

Overall, this is a considerable improvement in a short time, with limited financial investment. However, much more remains to be done.

Recommendation 7

By February 2027, the [National Fire Chiefs Council](#), in consultation with the Ministry of Housing, Communities and Local Government, should refresh its '[Digital, Data and Technology strategy](#)' to include annual external validation of all English fire and rescue services' [Cyber Assessment Framework](#) assessments.

Recommendation 8

By February 2027, the [National Fire Chiefs Council](#), in consultation with the Ministry of Housing, Communities and Local Government, should update its '[Digital, Data and Technology strategy](#)' to support the procurement of cybersecure ICT and the management of third-party [cybersecurity](#) risks in all English fire and rescue services.

The role of the Fire Standards Board

In August 2024, the [Fire Standards Board](#) introduced the Digital and Cyber Fire Standard. This sets out how fire and rescue services should govern and manage cybersecurity. It details how to balance the protection of ICT services, assets and data with making sure staff using ICT have the correct authorisation to do their work. It covers how services should proactively monitor and mitigate against changing cyber threats while continuing to carry out their duties successfully in the event of a cyber incident. The standard is compatible with the CAF assessment that services use to track their progress. So actions to implement the fire standard will also help services to meet the CAF standards.

In September 2024, the Fire Standards Board introduced its [Procurement and Commercial Fire Standard](#). It describes how services should manage risks, including cyber risks and data breaches, within their supply chains.

3. Local cybersecurity leadership and governance

Cybersecurity risk is recognised, but leadership, governance and capability are inconsistent

Strategic risk recognition and governance arrangements need to be aligned

Across the police forces and fire and rescue services we inspected, senior leaders typically recognised [cybersecurity](#) as a significant organisational risk. Many described it as a rapidly growing threat. They expressed concern about the potential impact of a major cybersecurity incident on their ability to provide essential services and protect the public.

Many leaders demonstrated a clear understanding of the risks. They were able to communicate the potential consequences of a [cyberattack](#), including losing operational systems and disruption to [safeguarding](#) and public protection. They spoke candidly about incidents they had experienced and the lessons they had learned. All the inspected organisations had governance structures for managing cybersecurity risks. They had cybersecurity listed on their corporate risk registers, sometimes described as a top tier or strategic risk.

In many cases, cybersecurity was a standing agenda item for senior leadership teams and boards. Several of the inspected organisations had recently updated their risk scoring to reflect national cybersecurity incidents.

But we found some cybersecurity governance structures didn't have clear accountability, strong enough grip or the capability required to make the necessary improvements. As a result, in some forces and services:

- leadership and governance capability for cybersecurity is unreliable;
- accountability is unclear;
- oversight lacks depth;
- governance doesn't always promote improvement;
- cultural and structural barriers remain; and
- independent assurance is limited.

Not all leaders demonstrated the level of practical understanding needed to strengthen cybersecurity. We found that senior leaders often relied heavily on ICT teams for cybersecurity assurance. This meant:

- a lack of active oversight in some cases, with some leaders receiving updates but not always scrutinising them properly;
- some leaders were unclear what a proportionate level of cybersecurity resilience would be;
- cybersecurity governance sometimes lacked clear outcome measures or milestones; and
- the amount and type of cybersecurity risk they were willing to take was rarely expressed in practical, decision-making terms.

In some organisations, leaders spoke confidently about cybersecurity threats but couldn't explain important controls, dependencies or vulnerabilities within their own systems. This lack of awareness and practical understanding reduces leaders' abilities to scrutinise progress, prioritise investment or make informed and proportionate decisions on cybersecurity issues.

We found wide variation in both sectors in the confidence and capability of senior leaders in managing cybersecurity risks. Some leaders demonstrated a strong understanding of cybersecurity threats. They worked proactively with ICT teams, asked for external assurance and led improvement programmes. But, in some forces and services, leaders were focused on other competing operational priorities, at the expense of cybersecurity. Some leaders were unaware of the full extent of cybersecurity risks posed by their legacy ICT systems.

We also found examples where limited technical understanding among senior leaders made it difficult for them to challenge ICT teams or fully interpret cybersecurity information. It meant leaders were more cautious and needed more information and assurance to make decisions on cybersecurity.

Cybersecurity is a complex area. Its technical nature can make risks difficult to translate into strategic discussions. Nevertheless, leaders need enough practical understanding to provide effective challenge, oversight and direction.

Senior information risk owner roles and responsibilities vary

All organisations we inspected had appointed a senior information risk owner (SIRO) or an equivalent. A SIRO is a senior-level executive role responsible for overseeing corporate information and cybersecurity risks. But their capability, confidence and influence varied considerably.

Some SIROs demonstrated a strong understanding of cybersecurity risk and provided effective challenge and oversight. Others had limited cyber knowledge or experience and viewed the role primarily as a compliance requirement.

We found that some SIROs lacked access to independent assurance, didn't have enough time to dedicate to the role and relied heavily on ICT specialists for advice. In several organisations, SIROs had received limited formal training in cybersecurity or information risk management.

Across both sectors, leadership was strongest where SIROs actively championed cybersecurity and heads of ICT helped shape strategic decisions. We also found cybersecurity specialists were more effective when they could directly challenge senior leaders.

Clear reporting, action plans and milestones also helped organisations monitor their cybersecurity maturity and progress. We found forces and services performed better when they defined and understood the amount and type of cybersecurity risk they were willing to take.

Cybersecurity leadership was weaker where SIRO responsibilities were unclear. And governance was less effective where reporting was too technical or lacked detail.

We found that some organisations only made decisions to invest in cybersecurity after problems emerged. Others accepted legacy technology risks as unavoidable and treated cybersecurity solely as an ICT responsibility.

Some organisations didn't learn effectively from previous incidents and reviews. And in others, the scrutiny of cybersecurity risks and performance was limited.

SIROs need enough authority, capability and time to do their job effectively. Senior leaders also need a stronger practical understanding of cybersecurity risks, system dependencies and information security controls. This will help them provide effective oversight and challenge.

Governance structures and effectiveness also vary across organisations

All organisations we inspected had cybersecurity governance arrangements, reporting processes and risk escalation routes.

In policing, governance commonly operated through information assurance boards, risk committees and digital transformation programmes. In fire and rescue services, governance was usually provided through senior leadership teams and fire authorities.

The quality of governance varied considerably. The strongest organisations held regular and structured discussions about cybersecurity, maintained clear reporting arrangements and effectively tracked risks and actions. They also benefited from independent challenge and assurance.

But in other organisations we inspected, governance was less effective. We found meetings where cybersecurity was discussed, but risk actions weren't reviewed in detail and progress wasn't measured. We also found examples where dependencies and risks weren't questioned or examined sufficiently. Sometimes decisions were made without a full understanding of ICT system implications and organisations didn't routinely ask for advice from external specialists. In several forces and services, we found that an established cybersecurity governance structure existed, but there was little evidence that it improved their effectiveness and efficiency.

Cybersecurity governance arrangements in both sectors should go beyond reporting risks. They should focus on active scrutiny, informed decision-making and measurable improvement. Stronger independent assurance would also help leaders better understand risk, performance and progress.

Without more effective governance, sustained investment and informed leadership, forces and services will remain vulnerable to avoidable cybersecurity risks.

Police cybersecurity incident management and reporting arrangements were fragmented

Incident reporting was fragmented in all three police forces we inspected. Cybersecurity incidents and data breaches were often routed through different systems or teams. In one force, some incidents were reported to the data protection officer and others through ICT helpdesks or operational structures, indicating inconsistency in internal processes.

This fragmentation makes it more difficult to identify incidents quickly, determine which are most important and assess risk. It also means sometimes the right people aren't made aware of a cybersecurity incident at the right time, especially cybersecurity and ICT specialists who need to be briefed and involved at the earliest opportunity.

Across forces, we found that [personnel](#) didn't always understand whether certain events constituted cybersecurity incidents, data breaches or both. This lack of clarity risks delaying escalation and reducing the effectiveness of incident response.

Fire and rescue service governance models are complex

The fire and rescue services we inspected operated within varied cybersecurity governance models. They often involve complex relationships with local authorities or joint governance arrangements for shared services. These models shape cybersecurity resilience in several ways.

In some fire and rescue services, it was unclear who had responsibility for ICT systems. This was made worse by the fact that some third-party suppliers provided services across multiple organisations, each with different definitions of the type and amount of risk they were willing to take. We also found examples where cybersecurity programmes were constrained by local authority ICT priorities and decision-making was slow where ICT services were shared.

In one service, we found outdated governance documents as well as a lack of clarity about who was responsible for systems. Leaders acknowledged that they didn't have full visibility of all ICT systems because their host local authority was responsible for them. The lack of clarity around cybersecurity governance structures reduces the fire and rescue sector's ability to adopt consistent standards or respond quickly enough to emerging risks.

Risk assessment and prioritisation need to improve

Both sectors face cultural barriers that slow progress. They recognised cybersecurity as an important strategic risk. However, it didn't always receive the same attention as more visible operational risks.

Weaknesses persisted even when risks were clearly documented. Factors such as financial pressures, workforce demands and competing priorities often delayed action to address known vulnerabilities.

Policing benefits from national assurance processes and support from the [Police Digital Service \(PDS\)](#). However, these arrangements don't provide complete assurance over all force ICT systems or local controls. And the PDS cybersecurity advice to forces doesn't always lead to prompt or effective local action.

The fire and rescue sector doesn't have a national cybersecurity assurance function equivalent to the PDS, or a national security operations centre capability, where a team of ICT security professionals uses specialist tools to continuously monitor, detect, analyse and respond to [cyber threats](#).

Although all the inspected organisations had some form of internal audit, few had strong independent cybersecurity assurance arrangements. Many relied on supplier reports, technical assessments or national frameworks. Few forces and services had commissioned independent cybersecurity maturity assessments, ICT reviews or penetration testing (planned tests that simulate a cyberattack) linked directly to governance decisions.

This lack of independent scrutiny reduces leaders' ability to understand whether cybersecurity controls are effective and whether progress is being made. It also prevents them having a full understanding of how their organisation compares to peers and where investment is most urgently needed.

Limited resources and support affect workforce capacity and capability

We found committed and capable personnel working hard to keep systems secure and protect their organisations. However, they often carried out this work with limited resources and support, placing an unsustainable burden on too few individuals.

Cybersecurity resilience in both sectors is limited by:

- a lack of specialist capacity;
- difficulty recruiting and retaining skilled personnel;
- limited role-based training;
- senior leaders' inconsistent cybersecurity knowledge;
- inadequate cybersecurity user behaviour at the most basic levels;
- not enough [control room](#) or operational preparation;
- cultural issues and underestimation of cybersecurity risk;
- difficulties in communication between ICT specialists and the wider workforce; and
- poor workforce awareness of cybersecurity risks and reporting requirements.

Across all organisations we inspected, we found small ICT and cybersecurity teams working hard and often beyond their capacity. They were frequently crisis-managing. These teams were typically committed and knowledgeable. They were respected by colleagues, relied on heavily during incidents and pragmatic in balancing security with operational needs.

However, specialist teams are typically too small to cope with prolonged or multiple incidents. This means forces and services have limited surge capacity (the ability of an organisation to rapidly increase its resources), which makes major incidents harder to manage.

Several ICT personnel we spoke to as part of our inspection described the major challenge they faced – the need to maintain core services while also modernising systems, implementing other large ICT development programmes or mitigating evolving threats. This creates a situation where organisational cybersecurity resilience heavily depends on the availability and well-being of a handful of specialists.

Both sectors rely too heavily on a small number of ICT specialists

Across both sectors, we found a heavy reliance on a small number of long-serving ICT personnel. They had the historical knowledge of legacy systems and were responsible for cybersecurity oversight and incident response. In several organisations, the same individuals acted as technical specialists, ICT system custodians and incident leads. They often did so without succession arrangements in place. This creates several risks:

- single points of dependency – if one person is unavailable during a major incident, resilience is compromised;
- not enough people with the right expertise – important technical knowledge is concentrated in a few individuals;
- burnout and workload pressure – ICT specialists described high workloads, frequent interruptions and limited recovery time; and

- constrained capacity for strategic work – routine and long-term improvements are often delayed because reactive work dominates.

Across both sectors, ICT personnel we spoke to highlighted concerns about resource constraints, single points of dependency and limited out-of-hours coverage. They told us these pressures could limit their ability to sustain effective support during a prolonged cybersecurity incident.

In the organisations we inspected, reliance on a small group of experts was primarily due to difficulties in recruiting and retaining cybersecurity talent. These included competition from private sector employers offering higher salaries to those with specialist qualifications, long recruitment cycles and limited dedicated cybersecurity roles. Restrictions on pay flexibility, limited career pathways for security roles and a small internal talent pool for promotion are also contributory factors.

We found that understanding of cybersecurity risk by senior leaders varied significantly across both sectors. Some senior leaders demonstrated strong awareness of technical and operational cybersecurity issues and a clear understanding of system dependencies. We found examples of close working and communication with ICT teams and confidence in scrutinising risk and challenging assumptions.

However, others relied heavily on ICT managers for interpretation and struggled to translate technical risk into real-world consequences. Similarly, we found cases where leaders focused on high-level concepts without understanding practical effects, or didn't routinely take part in cybersecurity-specific training and exercises provided by their organisations.

These factors affect decision-making. We found that where leaders lacked confidence, they took longer to make investment decisions, weren't rigorous enough in their [risk assessment](#) and carried out limited scrutiny of ICT programmes. They also allowed legacy system issues to persist and didn't effectively challenge suppliers where necessary. Collectively, these issues can reduce the speed and quality of operational decision-making, including during cybersecurity incidents, making it harder to respond quickly and manage risk effectively.

We found that most police and fire and rescue leaders we spoke to felt that improved digital leadership and training at all levels was crucial to cybersecurity. Others also stated that cybersecurity needed to be recognised as an accredited profession across both sectors.

Across several of the inspected organisations, ICT personnel told us that differing levels of technical understanding among leaders and personnel made it challenging to communicate cybersecurity risks clearly and in a way that was operationally meaningful. This was the case for communication between ICT specialists and leaders, and between leaders and their wider organisations. This is an important cultural barrier to effectively communicating about, and improving, cybersecurity resilience.

We found that both sectors needed to build workforce capability, capacity and culture at all levels. This includes increasing specialist resources, providing better training and improving recruitment and retention.

Compliance with mandatory training is inconsistent, affecting understanding

All the organisations we inspected made annual cybersecurity and data protection training mandatory. However, compliance varied considerably.

One police force reported a high level of compliance with its cybersecurity training, describing strong completion rates relative to previous years. Other forces' compliance rates were notably lower.

Fire and rescue service training completion rates also varied. Some services reported acceptable rates and others struggled to get personnel to do the training. Some fire and rescue sector interviewees attributed low completion rates to operational pressures. A lack of supervisory oversight, lack of access to completion-rate data and personnel not being held accountable if they didn't complete the training were also cited as reasons. We found that some training courses didn't require any active participation from the learner. And one fire and rescue service member of staff said they hadn't received any training on ICT system security and staff were effectively "learning as we go".

Across all the organisations we inspected, we found a need for more structured, role-appropriate training that reflects the realities of modern cybersecurity risk.

We found little evidence of:

- sufficient [continuing professional development](#) for all personnel;
- support for advanced cybersecurity training for ICT personnel and cybersecurity professionals;
- cybersecurity-specific training for operational leaders;
- scenario-based training for control room or operational managers; or
- training for contract managers on supplier cybersecurity risk.

Instead, training often focused on improving awareness of phishing (when criminals send scam emails or texts that share links to websites containing harmful software, or trick users into revealing sensitive information) and basic practices, such as good password management. While important, these modules don't provide all personnel with the knowledge they need to respond to modern threats.

One member of the [National Fire Chiefs Council](#) told us that basic training wasn't keeping up with hackers' more sophisticated tactics. Most leaders across both sectors acknowledged that more needed to be done to educate their workforce about cybersecurity.

In several of the inspected organisations, ICT and cybersecurity personnel described limited access to specialist training. This was mainly because of limited budgets, difficulties in securing protected learning time and national frameworks not including compulsory training on the competencies needed to do their jobs.

Control room personnel also have a crucial role during cybersecurity incidents. They must recognise system issues and use alternative [fallback](#) processes to keep operations running if systems are taken offline. They also need to communicate effectively with ICT teams and maintain operational continuity.

However, we found limited cybersecurity-specific training for control room personnel. There was limited scenario-based training and operational leaders weren't systematically required to understand cybersecurity dependencies. The lack of training and awareness increases the likelihood of confused, fragmented and delayed responses to a cyberattack. And this may have a knock-on effect leading to operational disruption.

Both sectors should also strengthen broader workforce cybersecurity awareness, learning and development. Everyone in the workforce must clearly understand their cybersecurity roles and responsibilities. This includes reporting, escalation and responding to any cybersecurity incidents or threats. Doing this will reduce both sectors' dependence on a few, often overstretched, cybersecurity specialists. And will challenge some cultural perceptions that cybersecurity is solely a corporate and technical issue. Cybersecurity should become part of business as usual and be seen as a shared organisational responsibility.

Cybersecurity awareness and prioritisation need to improve

Although both sectors increasingly recognised cybersecurity as a core strategic risk, we found this didn't consistently lead to sustained focus on cybersecurity improvement.

In the inspected police forces, we were told that operational pressures meant that cybersecurity-related initiatives often had to compete for funding and leadership attention. In the fire and rescue services, senior leaders acknowledged the strategic importance of cybersecurity. But they typically gave it less day-to-day attention than more immediate operational risks. This reflects a strong cultural focus on frontline response activity.

ICT and information security personnel sometimes struggled to secure commitment to longer-term cybersecurity work. This means that forces and services risk falling behind, reducing their ability to tackle the evolving threat. It leaves them increasingly exposed to preventable cybersecurity incidents and potentially unable to maintain critical services when they are needed most.

We found that relationships between ICT teams and other departments were generally positive. Personnel trusted ICT colleagues and appreciated their efforts under pressure. But we also found clear communication and understanding was limited. Non-technical personnel often underestimated the complexity of cybersecurity risk and believed ICT teams alone were responsible for cybersecurity. We also found cases where they didn't recognise their own role or were unclear about their responsibilities during a cybersecurity event.

Across several inspected organisations, ICT personnel told us that differing levels of technical understanding among non-technical staff made it challenging for them to communicate cybersecurity risks in an accurate and operationally meaningful way.

We also found inconsistent understanding of what constitutes a cybersecurity incident and confusion about reporting routes. This was particularly the case in policing, where separate cybersecurity and data breach reporting pathways created uncertainty for staff. This often led to delays in reporting, due to personnel checking first, and meant opportunities to detect incidents early were missed.

Additionally, varying levels of cybersecurity awareness in both sectors meant that operational personnel didn't always recognise the operational implications of cybersecurity risks. This left ICT teams responsible for bridging gaps in understanding.

4. Legacy ICT systems

Many police and fire and rescue ICT systems are outdated and highly vulnerable to cyberattack

Both sectors face ICT funding constraints

Both policing and the fire and rescue service have a limited budget to spend on ICT. The funding they do have needs to cover investment in new technology and/or maintenance of existing ICT. The reality is that many police forces and fire and rescue services use this budget to update or patch outdated legacy systems, rather than investing in new cybersecure technology.

The rise of sophisticated cybercrime and [cyberattacks](#) means that both sectors need to make sure their ICT systems are modernised and secure. During our inspection, we found that policing had adopted some new and advanced [cybersecurity](#) defences and technologies. This approach was less evident in the fire and rescue service. What was clear, across both sectors, was that funding other operational activity was a greater priority than replacing antiquated legacy ICT systems, servers and devices.

The [National Cyber Security Centre](#) told us that unsupported legacy systems presented a significant cybersecurity risk because they no longer received security updates. This leaves known vulnerabilities exposed and makes ICT systems more difficult to secure, monitor and integrate with modern security controls.

These challenges aren't unique to policing and the fire and rescue sector. Many public sector organisations face similar problems. However, the consequences of a successful cyberattack on emergency services could be severe, affecting public safety.

Progress towards achieving strategic ambitions is too slow

The [National Police Chiefs' Council's 'National Policing Digital Strategy 2025–2030'](#) states that:

“By 2030, policing will have access to modern solutions to enable them to protect the public, industry will have access to clear requirements to build those solutions, and the public will find it easier than ever to engage.”

It describes the journey to achieve “policing’s ambition to embrace digital capability in support of tangible, positive and measurable outcomes for both law enforcement and the public”.

Similarly, the [National Fire Chiefs Council’s ‘Digital, Data and Technology Strategy and Roadmap 2024–26’](#) states that it represents:

“A transformative vision for the future of fire and rescue services. Built on the foundation of innovation and collaboration, our strategy aims to harness the power of cutting-edge technology and data-driven insights to optimise every aspect of our operations.”

Both policing and the fire and rescue service have committed to strategic investment in modernising digital, data and technology, which is positive for the future. But, at the time of our inspection, we found a very different situation when examining the operational ICT and cybersecurity systems that forces and services used. On too many occasions we found they were using outdated systems and legacy technology. They also had inefficient processes for core tasks, such as record keeping, data collection and maintenance. This was more concerning when the data was sensitive or confidential.

We found that both sectors understood that older or outdated legacy technology was vulnerable to information security breaches or cyberattack. But many forces and services are slow to put it right. The main reason they gave us was the lack of capital investment or available budgets to fund new ICT ‘refresh’ programmes. Spending money on ICT systems was often perceived to be at the expense of frontline operations.

Both sectors need to address the biggest barrier to effective digital transformation – their legacy ICT systems and poor data quality. Much of both sectors’ ICT infrastructure is standalone and doesn’t work well with other systems and equipment. It is also sometimes outdated.

Some forces and services told us they couldn’t tackle these technological weaknesses because of limited funding allocations within their budgets. They highlighted a lack of central funding from government to meet the expense of replacing legacy systems. Others had delayed overhauling antiquated legacy systems and servers due to the perceived risk and complexity of the challenge. But postponing modernisation is likely to increase long-term costs and risks. And by failing to act promptly, both sectors open themselves up to an increased risk of cyberattack with potentially catastrophic consequences.

Legacy technology poses a national risk

The foreword to the national policing digital strategy highlights that the scale of the challenges around updating legacy systems is well known in policing. It states that:

“The challenges we face are stark; outdated legacy systems which are costly to maintain, poor quality data that cannot be utilised and a fragmented policing model built before borderless cyber-crime even existed. This, combined with severe digital skills gaps, a lack of interoperability and a rising tide of public demand leaves us vulnerable as a service.”

The National Police Chiefs’ Council acknowledges that vulnerable legacy systems are its highest strategic risk on the Police Information Assurance Board’s risk register. And, through the [Police Digital Service \(PDS\)](#), it provides forces with extensive analysis of legacy technology risks, system vulnerabilities and performance data.

The PDS told us that the challenges that policing faced around removing legacy technology were significant. But it also said steady progress was being made to make sure that the sector was using cybersecure ICT and operating systems.

Legacy technology is also a blocker to digital modernisation and progress. It creates what is known as ‘technical debt’, where money is spent to keep an outdated system running, rather than replacing it with new ICT. Several police leaders told us that, at the time of our inspection, a high percentage of police ICT spending went towards maintaining legacy systems, rather than investing in technology to transform policing.

To compound the problem further, legacy systems often create inefficient processes. Users may have to find ICT shortcuts or workarounds or duplicate effort to complete a task. Organisations shouldn’t wait until a critical failure happens, or an operational risk, such as a cyberattack, materialises before removing legacy ICT systems.

Both sectors need to work out how to deal with legacy ICT systems

Among interviewees, we found broad consensus that legacy ICT systems needed to be modernised. But there was a wide range of views expressed about how to go about it.

Some police leaders advocated for greater national standardisation and more shared technology solutions. Others highlighted the importance of including [Secure by Design principles](#) into every technology programme from the outset. Several leaders thought [cloud-based technology](#) presented an important opportunity to improve resilience, reduce technical debt and strengthen cybersecurity.

Whatever solution is adopted, it is fundamental that both policing and the fire and rescue sector remove or upgrade their legacy systems to include acceptable and effective levels of cybersecurity. Overlaying new technologies and advanced tools, such as artificial intelligence, on weak and insecure foundations may offer some short-term benefits. But it leaves core cybersecurity and information security risks and problems unresolved.

Failure to deal with legacy systems promptly could result in costly consequences which affect both sectors' ability to keep the public safe. Modernising the ICT estate – all the ICT assets an organisation owns or uses to support its operations, including hardware, software, data, networks and cloud services – across both sectors must become a priority.

We found that the fire and rescue sector's understanding of its ICT estate was far less mature than that of policing. Unlike for policing, there isn't a nationally co-ordinated technology framework, or equivalent capability, to provide a comprehensive view of systems and associated risks. Consequently, fire and rescue services routinely operate using different technology platforms and cybersecurity arrangements with limited national oversight. Several sector leaders acknowledged these challenges, but also highlighted the difficulties of reducing legacy technology risks without additional investment.

Secure by Design practice is weaker where organisations share ICT services

We found examples across both sectors where legacy systems lacked clear ownership, accountability and administration arrangements. These weaknesses increased information security and cybersecurity risks.

Interviewees from both sectors told us that their ICT infrastructure was built on the principles of 'Secure by Design'. But we found examples where:

- ICT management and design implementation was poor and inconsistently applied;
- new ICT projects were sped up without full cybersecurity [risk assessments](#);
- data protection impact assessments were incomplete or varied in quality;
- some organisations didn't carry out any cybersecurity testing before ICT systems went live; and
- cybersecurity risks were signed off based on partial or inadequate information.

We found some effective Secure by Design practice, but this was generally weaker in organisations with shared service ICT arrangements.

Both sectors need to do more to understand, secure and assure any ICT provision that is subject to a contract with, or hosted by, a third-party supplier, or where their data is held by an external third-party supplier for some other operational reason. These arrangements need to be made cybersecure through the robust application of Secure by Design principles. They should also be supported by a clear set of contractual terms and conditions. These should provide absolute clarity about lines of accountability, cybersecurity assurance processes and [critical incident](#) response procedures.

5. Third-party ICT suppliers

Cybersecurity risk is usually greater where third-party suppliers are responsible for police or fire and rescue ICT systems and data

Use of third-party ICT suppliers increases cybersecurity risk to both sectors

The [Police Digital Service \(PDS\)](#) told us that police data held on third-party suppliers' ICT systems was one of the most significant [cybersecurity](#) risks to policing. This is because this data and the systems that hold it aren't included in the PDS's protective monitoring. Such third-party supplier ICT systems are also often outside any police information security governance, oversight, review or standards. Given the evidence we found during our inspection, we conclude this creates a serious cybersecurity risk.

The risk is made worse because so many forces use different ICT suppliers, products and systems. And the problem is then magnified because the police sometimes share their data with public sector partners and other stakeholders. For example, local authorities, health services and [criminal justice system](#) partners, such as law firms. This risk is particularly critical where suppliers store or manage sensitive police data.

The PDS is developing a [Third-Party Assurance for Policing model](#); a set of standards to use when buying from or contracting with any third-party ICT system or product supplier. The model will set out the process police forces should follow to assess supplier compliance against the Security Assessment for Policing framework.

The risks are different but just as significant for the fire and rescue sector. We found fire and rescue services didn't hold as much confidential or sensitive data as police forces. Consequently, they don't need to share as much of this type of personal data with statutory partners or other stakeholders. But they do hold personal data about their staff, and about [vulnerable people](#) and their homes. And this data is still at risk from [cyberattacks](#).

Another vulnerability for the sector is that many services operate using ICT contractual arrangements with local authorities. There have been well-documented cases of cyberattacks on local authorities, so there is undoubtedly a risk to fire and rescue service data which is beyond their control.

The [National Fire Chiefs Council](#) understands that third-party ICT suppliers pose a cybersecurity risk to fire and rescue services. It is committed to creating an ICT risk ledger to better understand and manage third-party ICT provisions. But it stated that this would require funding from the Ministry of Housing, Communities and Local Government.

Cyberattacks on third parties that hold police data have already caused concerning risks and disruption

Cybersecurity risks are usually greater where third-party suppliers are responsible for police or fire and rescue ICT systems and data. This is because the data and the systems it is held on are often outside the remit of the force or service's protective monitoring arrangements.

During the inspection, we found that this risk was particularly critical where third-party suppliers stored or managed sensitive police data. This can include information about [victims](#), [safeguarding](#), [intelligence](#) and ongoing investigations.

The PDS and the [National Police Chiefs' Council](#) shared information on multiple cyberattacks that happened between 2021 and 2025 in which police data was at risk. None involved a direct attack on police ICT systems. Worryingly, it was the third-party ICT supply chains which held police information that had been compromised. The police successfully dealt with these cyberattacks as [critical incidents](#). They did this using the 'Defend as one' (pillar 2 of the '[Government Cyber Security Strategy: 2022 to 2030](#)') national co-ordination plan.

Despite the risks, both sectors rely heavily on third-party ICT suppliers

The [National Cyber Security Centre \(NCSC\)](#) told us reliance on third-party suppliers could present cybersecurity risks for all organisations, including policing and the fire and rescue service. The NCSC told us that weaknesses within third-party suppliers could provide criminal hackers with routes into ICT networks. The NCSC website provides [guidance on supply chain security](#). It states that:

"A series of high profile, very damaging attacks on companies has demonstrated that attackers have both the intent and ability to exploit vulnerabilities in supply chain security. This trend is real and growing."

These risks are made worse by the fact that each third party is dependent on its own supply chain. A cyberattack at any point in the supply chain can increase vulnerability in these sectors, even when there is no direct relationship with a force or service.

This vulnerability is on the National Police Chiefs' Council Police Information Assurance Board's risk register. But it is very difficult for the police to assess the effectiveness of third-party suppliers' cybersecurity. Particularly as the police don't usually have ICT contracts with third-party suppliers that meet [Secure by Design principles](#). We also found that most of these third-party contractual arrangements didn't include any ongoing cybersecurity assurance arrangements. Therefore, if the third-party ICT supplier's systems aren't secure, neither is the data held within them. Police forces and fire and rescue services need to fully understand this risk.

The National Fire Chiefs Council is revising its Digital, Data and Technology strategy for 2026–29 to reflect the enhanced risk management required when dealing with supply chains. The strategy recognises the need for the sector to strengthen its national influence on suppliers and procurement practices. And to improve its collaborative approaches and contractual arrangements with suppliers.

All the organisations we inspected depended heavily on external ICT suppliers for critical systems, infrastructure, hosting, software development and maintenance. In some cases, they relied on these contractual arrangements for all end-to-end ICT provision.

We found that third-party ICT provision either created new systems and infrastructure or used existing set-ups to host or store data. This was particularly evident where both sectors were working in partnership with other public sector bodies to share and store data. Third-party suppliers provided a wide and varied range of services. These included operational systems (such as case management, [control room](#) and [mobilisation](#) technologies, and identity services), data hosting and ICT infrastructure, and supporting systems (such as HR and payroll).

External third-party ICT providers that supply or host systems present one of the most challenging cybersecurity risk areas across both sectors. We found examples where:

- organisations lacked full visibility of hosting arrangements;
- suppliers controlled critical parts of the ICT infrastructure;
- logging of user activity for third-party systems was incomplete or outdated;
- monitoring coverage was inconsistent;
- responsibility for resilience and recovery wasn't clearly understood by the inspected organisations; and
- assurance of the third-party systems' cybersecurity relied heavily on supplier self-certification.

In the three police forces we inspected, we found there was also a reliance on national ICT systems, many of which were hosted by the Home Office. Some interviewees expressed concern that they had limited understanding or oversight of how cybersecure these systems were, or how cybersecurity risks were being managed. Forces aren't responsible for the cybersecurity of national police systems. But any weaknesses in national-level cybersecurity arrangements expose forces to incidents that they can't readily detect or manage.

In the three fire and rescue services we inspected, we found that shared ICT provision through partnership arrangements was more commonplace compared to policing. Interviewees expressed concerns that they had limited oversight of those ICT systems and how their data was being stored, secured, controlled and managed. They highlighted examples where host organisations or joint service providers managed systems on behalf of multiple partners. The fire and rescue services that weren't responsible for day-to-day ICT system management were less able to understand their exposure to cybersecurity risk.

We interviewed several cybersecurity company representatives, including a director of a company that provided protective monitoring for a fire and rescue service. He stated that the risk of using third-party ICT suppliers was significantly compounded by artificial intelligence. He was concerned that many third-party suppliers "operated like the Wild West and lacked controls, oversight and accountability".

Several of the organisations we inspected had experienced incidents where supply chain weaknesses had caused disruption. These included:

- system outages caused by suppliers misconfiguring the systems;
- vulnerabilities in hosted ICT infrastructure;
- failures by third parties to handle data securely;
- slow supplier notification following incidents;
- inability to access logs needed for incident response; and
- degraded services during supplier network failures.

All six inspected organisations depended on third-party suppliers. But none of them had comprehensive processes that were robust enough to assure their suppliers' cybersecurity. We found that:

- assurance processes were inconsistently applied and, even when strong at the point of procurement, they became weaker or absent as time went on;
- contract controls were outdated or incomplete; and
- multi-layered supply chains undermined accountability for cybersecurity by making it unclear who was responsible for what.

Police forces and fire and rescue services need to strengthen their supplier assurance, improve their visibility of hosted systems and consistently apply standards. Until they do, they will remain vulnerable to cybersecurity incidents that originate outside their own networks but directly affect their ability to provide critical services.

Both sectors have made initial progress in understanding supplier frameworks and risks

Across the organisations we inspected, we found some positive processes and practices regarding third-party ICT procurement and contractual arrangements that required information security standards and/or controls.

We were encouraged that work was underway across both sectors to develop a better understanding of their third-party supplier framework and ICT blueprint. This is often called developing a risk ledger for third-party suppliers.

Most organisations required suppliers to:

- meet the NCSC's [Cyber Essentials \(CE\)](#) or [Cyber Essentials Plus \(CE+\)](#) standards;
- meet the [International Organization for Standardization \(ISO\)](#) standard 27001 that relates to data risks;
- carry out data protection impact assessments (DPIA);
- complete security questionnaires provided by the force or service; and
- include clauses in contracts addressing data handling and breach reporting.

However, the inspected organisations rarely supplemented these controls with ongoing assurance. We found examples where:

- organisations accepted CE/CE+ and ISO certificates without verifying what systems they applied to;
- organisations didn't require suppliers to provide assurance annually;
- technical updates weren't requested;
- DPIAs regulated supplier contracts but didn't provide deeper assurance of supplier security;
- organisations didn't subject high-risk suppliers to enhanced scrutiny;
- contract managers had no cybersecurity-specific training;
- ICT teams weren't involved in contract reviews; and
- organisations didn't keep an authoritative list of all the suppliers they shared sensitive data with.

Forces and services need more information about supplier controls and assurance processes

Many of the systems used by the organisations we inspected were hosted in [cloud](#) or hybrid environments controlled by suppliers. In these cases, we found examples where:

- logging was limited and/or not shared;
- organisations had little visibility of supplier patching;
- monitoring depended entirely on supplier capability;
- vulnerability management was inconsistent;
- data location was unclear;
- resilience arrangements weren't tested; and
- backup and restoration processes weren't transparent.

In policing, national bodies provide oversight and support. But forces don't always have a clear view of how those national bodies identify and manage cybersecurity risks. This doesn't mean forces should be responsible for securing national systems. However, they do need enough information and assurance to understand how those responsible for ICT systems manage risks, and to hold them to account effectively.

In fire and rescue services, there were comparable challenges where ICT was provided by a local authority or shared service arrangements. In these cases, services didn't always have direct access to system information, assurance products or supplier documentation. While responsibility for cybersecurity remains with the system provider, services need clear assurance and transparent information to understand their exposure to risk.

This lack of visibility is concerning. Even if the organisation has strong internal controls, it may still be vulnerable to compromise if a supplier's network is breached.

Contractual arrangements and assurance vary

When we examined supplier contracts across the organisations we inspected, we found significant variation in:

- reporting timescales for cybersecurity breaches;
- audit and inspection rights;
- data retention requirements;
- incident notification obligations;
- access to logs and monitoring information;
- allocation of monitoring and detection responsibilities; and
- liability for cybersecurity incidents.

Contractual assurance also varied considerably across both sectors. Some of the inspected organisations had up-to-date contracts with explicit cybersecurity requirements. Others relied on older or legacy agreements that didn't reflect modern threat levels or the latest best practice. This was particularly common in fire and rescue services using shared service arrangements or, most concerningly, externally hosted command and control systems.

We also identified that some forces and services didn't hold the original contract documentation for systems provided through shared services or national arrangements. In these cases, personnel couldn't always confirm what security obligations applied to the supplier or whether the supplier was meeting security reporting requirements. We also found examples where they were unsure of what access control standards (put in place to make sure only authorised users or systems can access data or services) had been contractually agreed. Or whether the supplier was required to notify the organisation promptly in the event of a cybersecurity incident.

This lack of clarity left forces and services unable to determine whether suppliers were meeting minimum expectations for detection, reporting and resilience. Or whether the contractual terms provided the influence needed to demand improvement.

We found widespread reliance on supplier self-certification without independent verification, such as accepting the CE/CE+ government cybersecurity standards and ISO 27001 certification without checking how recently they had been achieved or awarded. We also found examples where organisations relied on supplier assurances about patching and vulnerability management, accepted DPIAs at face value and didn't request annual confirmation of controls. This isn't satisfactory.

Self-certification has value, but it can't be relied on as the sole form of assurance. This is particularly important where suppliers provide services that, if compromised, could affect public safety. Organisations also need to carry out routine checks to confirm that certifications remain valid and suppliers continue to meet required security standards. We weren't confident this was always the case.

System outages from cyberattacks on third-party suppliers pose a risk to control room operations and mobilisation

Control room technology remains one of the highest impact targets for a cyberattack across both sectors. A compromise of this part of a police force or fire and rescue service could seriously affect operational capability and create a risk to the public.

During our inspection, we found several examples where cybersecurity risk to operations was particularly high. These included where third-party suppliers managed or were responsible for infrastructure being used for mobilisation and other critical functions. We also found that some forces and services were uncertain how soon after an attack their ICT would be available again for hosted command and control systems.

We found that some fire and rescue services couldn't maintain full operational capability if a third-party supplier experienced a significant outage. The sector has a well-established, routinely tested manual mobilisation process in place as a backup. But this doesn't remove the underlying risk. Even if the service can mobilise, restoring the hosted system can be complex and time-consuming. This is especially true where critical functions depend entirely on third-party recovery processes.

In one joint fire and rescue service control arrangement, personnel showed a clear understanding of contingency procedures. But they lacked confidence in the third-party supplier and highlighted previous delays in system restoration.

We also found risks relating to loss of information accessed via fire and rescue personnel's [mobile data terminals](#). This could include important information such as building and occupancy details or [vulnerability](#) markers. Personnel we spoke to were clear that the service could continue to function at a basic level during outages. But full operational capability relied on being able to quickly restore the supplier-hosted system.

Supply chain complexity and accountability create challenges

Many of the ICT systems that the organisations we inspected used had multi-layered supply chains. For example, a system owned by one supplier, developed by a second and maintained by a third. These were often integrated with a local authority's infrastructure or connected to a national system. In these cases, no single organisation had full visibility of the end-to-end ICT architecture. This creates a risk.

This complexity also creates challenges in areas such as incident response, logging and monitoring, vulnerability management and accountability. And it leads to weaker recovery and contract enforcement.

Police forces benefit from support provided by the PDS [National Management Centre](#) and Third-Party Assurance for Policing. But these processes don't cover all suppliers, and visibility sometimes ends where the supplier ICT network begins. There is no equivalent support for fire and rescue services.

Both sectors need to make sure they only buy from and contract with third-party ICT suppliers if there are robust cybersecurity arrangements and assurance processes in place. Otherwise, forces and services can't be confident that their suppliers operate securely in a rapidly evolving landscape of [cyber threat](#). Achieving this requires clear visibility of ICT infrastructure, data management and information security controls. This is especially important where third-party ICT systems cater for multiple partners and hold a wide range of sensitive or confidential data.

Assurance should be structured, risk-based and applied throughout the full life cycle of supplier relationships. It can't rely solely on procurement-stage checks or supplier self-certification. Responsibilities across complex supply chains must be clearly defined. High-risk services, such as mobilisation systems, should be subject to enhanced scrutiny. They also need robust, tested alternative [fallback](#) processes to keep operations running if systems are taken offline.

Both inspected sectors need far more robust procurement and contractual processes to reduce exposure to risks originating beyond their networks. They must be cybersecure through Secure by Design principles. And those responsible for the data and the ICT system provider must agree and commit to ongoing cybersecurity assurance processes. This will give both sectors, and their third-party ICT suppliers, reassurance that the cybersecurity risks are being reduced and/or mitigated.

Recommendation 9

By May 2027, all chief fire officers in England should put measures in place to make sure that all new or renewed contracts with public sector partners or private sector third-party suppliers meet the standards set out in the [Cyber Essentials certification scheme](#) and the [Secure by Design principles](#).

Recommendation 10

By May 2027, each chief constable in England and Wales should:

- review existing police ICT contracts and procurement processes, and improve those that don't include adequate [cybersecurity](#) assurance; and
- adopt the government's [Secure by Design principles](#) and the [Police Digital Service's Third-Party Assurance for Policing standards](#).

6. Cybersecurity and the workforce

The way people use ICT systems and data creates significant cybersecurity risks

Human error is a major factor in cybersecurity risk

Human error remains one of the most significant factors in [cybersecurity](#) breaches globally. Research consistently shows that mistakes by users, whether careless, negligent or deliberate, provide opportunities for cyberattackers. Common examples include people using weak passwords, failing to follow security procedures or responding to phishing emails (when criminals send scam messages that share links to websites containing harmful software or trick users into revealing sensitive information).

We found these risks across policing and the fire and rescue service. Workforce awareness, behaviours and compliance with cybersecurity requirements varied considerably between and within organisations.

Cyberattackers that go phishing for data remain a particular concern to both sectors. Attackers use increasingly sophisticated techniques to imitate trusted organisations and individuals to attempt to obtain passwords, personal information or other sensitive data.

Across both sectors, we found that human error continued to create opportunities for [cyberattacks](#). Until organisations mitigate or remove these vulnerabilities through better controls, training and supervision, the risk will remain.

Better awareness and security controls can reduce the risk of human error

A lack of cybersecurity awareness and training can create opportunities for cyberattackers. But cybersecurity vulnerabilities aren't caused by inadequate training and awareness alone.

During our inspection, we found examples where poor workforce behaviours and processes increased exposure to risk. These included weak access controls, poor password management and inconsistent use of multi-factor authentication (where users must provide two or more verification methods to gain access to systems). There were also weaknesses in joiners, movers and leavers processes and device management arrangements.

We acknowledge that both sectors have large and diverse workforces, often operating across multiple locations and technology platforms. This presents additional challenges. But police forces and fire and rescue services simply aren't doing enough to prevent human error from opening the door to cyberattacks. Across both sectors, we found limited cyber exercising (planned emergency testing) and relatively little testing of cyberattack or incident response plans. Workforce training was often focused on basic information security and data protection requirements rather than wider cybersecurity risks and operational impacts.

Until all these issues are addressed, human error will create significant risk to policing and the fire and rescue service, and significant opportunity for cyberattackers.

Cybersecurity should be formally recognised as both a leadership discipline and an accredited specialist profession

Several senior leaders and cybersecurity specialists told us that leadership capacity and capability relating to cybersecurity needed to improve across both sectors. We found there was broad agreement that cybersecurity was no longer solely a technical issue. It is viewed as an important leadership responsibility that requires informed decision-making at all levels.

Interviewees consistently highlighted the need for stronger digital leadership. They wanted to see professionalised cybersecurity roles, accredited learning and development, greater cyber awareness and clearer expectations of leadership roles and responsibilities relating to cybersecurity.

We agree. We found little evidence of structured cybersecurity learning beyond basic awareness training. [Continuing professional development](#) was often limited. Advanced training for cybersecurity specialists was inconsistent. Cybersecurity training for operational leaders, senior information risk owners, data protection officers and gold commanders was rare. We also found little evidence of scenario-based training for operational and [control room](#) managers, or specialist training for procurement and contract management personnel responsible for supplier risk.

The cybersecurity risks caused by human error will remain for both sectors until cybersecurity becomes a greater priority and leaders view it as part of daily operational activity. Those risks need to be mitigated by investment in accredited specialist cybersecurity training and continuing professional development for senior leaders and cybersecurity specialists alike.

Recommendation 11

By November 2027, the [National Police Chiefs' Council](#) in consultation with the [Police Digital Service](#) and the [College of Policing](#) on behalf of the police sector, and the [National Fire Chiefs Council](#) on behalf of the fire and rescue sector, should each develop their understanding of [cybersecurity](#) roles and responsibilities. They should also provide accredited learning and development to senior leaders and specialist staff.

Inconsistent identity and access management arrangements can increase vulnerability

Identity and access management is one of the most important aspects of cybersecurity. Yet across the organisations we inspected, access controls were often incomplete or applied inconsistently.

The use of multi-factor authentication varied considerably. Some organisations had implemented strong controls across most systems. Others had only partial coverage, particularly for third-party applications and externally hosted systems.

We found that all organisations we inspected relied on fully or partially manual HR joiners, movers and leavers processes. This creates avoidable vulnerabilities. We found examples where ICT teams relied on supervisors to notify them of leavers or movers. Where ICT teams missed the notification, or supervisors forgot to issue the notification, access to systems and/or data often remained open and accounts remained active for former personnel. In some cases, it also meant that people moving to different jobs within the organisation kept access long after their roles had changed. We also found that third-party accounts weren't consistently reviewed and third-party contractors continued to have access without validation.

ICT access reviews were also inconsistent. Some organisations carried out regular checks, while others relied on informal arrangements or periodic audits. The management of privileged accounts (securing, controlling and monitoring ICT accounts that have enhanced permissions to access sensitive data or carry out ICT administrative tasks) also varied. Although some organisations had introduced privileged identity management controls, these arrangements weren't always comprehensive.

Shared service arrangements created further challenges. In some cases, responsibility for removing access to and managing ICT accounts was unclear.

Both sectors should strengthen identity and access management. This includes increasing the use of multi-factor authentication, automating joiners, movers and leavers processes, improving privileged account management and carrying out regular access reviews. Responsibilities within shared service arrangements should also be clearly defined.

Endpoint security and data handling practices are inconsistent

The security of devices connected to an organisation's ICT network varied considerably. Some organisations used modern endpoint detection and response tools that continuously monitored devices and servers to identify and mitigate against malicious cyber activity. They also had strong device management arrangements. Others relied on older technology and less effective controls.

We found examples of unmanaged devices, legacy laptops, older mobile phones and [mobile data terminals](#) operating with limited security controls. Controls relating to removable media, such as USB sticks, and external devices were also inconsistent. Shared accounts and generic logins sometimes remained in use, reducing individual accountability and increasing risk.

Data handling practices also varied across both sectors. We found examples where organisations had limited understanding of where data was stored, routinely exported information to local devices and retained data longer than necessary. Other weaknesses included the use of paper-based workarounds, shared mailboxes and inconsistent approaches to managing and transferring information securely.

Many cybersecurity specialists understood these risks and had identified actions to improve controls. We also found examples of positive practice, including initiatives to identify unauthorised devices and reduce the use of removable media.

However, both sectors need a more consistent approach to endpoint security and data management. Organisations should maintain accurate records of where data is stored. They should strengthen controls governing storage and transfer, improve visibility of network-connected devices and remove unmanaged or unsupported technology. They should also address workforce behaviours that increase cybersecurity risk.

Without co-ordinated action to improve data handling and cybersecurity practices, policing and the fire and rescue service will continue to face elevated risks of unauthorised access, data breaches and cyberattacks.

7. Cybersecurity monitoring and detection

Monitoring and detection are improving, but more needs to be done

Monitoring and detection are vital to effective cybersecurity but there are stark differences in capability

Monitoring and detection capabilities are essential to managing modern [cybersecurity](#) threats. In this context, monitoring involves the continuous, real-time observation and analysis of, among other things, ICT system behaviour and security indicators to detect threats. Organisations cannot respond to what they cannot see. Being able to identify [cyber threats](#) and risks across ICT systems, networks and user activity is critical to containing incidents before they escalate.

Across the police forces and fire and rescue services we inspected, we found wide recognition of the importance of monitoring. Some had strengthened their detection capabilities through new technology, enhanced threat [intelligence](#) or improvements to security operations. But we found substantial variation in the maturity, capability and coverage of these arrangements.

Several of the inspected organisations had invested in a dedicated security operations centre (where a team of ICT security professionals uses specialist tools to continuously monitor, detect, analyse and respond to cyber threats), modern monitoring tools or enhanced out-of-hours support. Others relied heavily on third-party suppliers or national support services and had limited local capability.

But we found that no force or service had comprehensive end-to-end monitoring and detection coverage proportionate to its level of risk.

The quality of monitoring and detection varied considerably across the organisations we inspected. The strongest had dedicated security operations centre capabilities, regular vulnerability scanning (which automatically detects security defects across an organisation's networks, software and systems), clear escalation processes and structured incident response arrangements. Within policing, this complemented national support that the [Police Digital Service](#) provided and helped forces to identify and respond to threats promptly.

Other forces and services relied heavily on alerts and notifications from their third-party suppliers, with limited independent monitoring capability.

Out-of-hours monitoring arrangements also varied significantly. Some forces and services had continuous security operations centre coverage, managed detection and response services or formal [on-call](#) arrangements. Others had no dedicated out-of-hours monitoring capability. Both sectors should strengthen their out-of-hours monitoring arrangements, especially for critical systems.

We found that both sectors had limited visibility of ICT systems and data that they didn't own or manage. This is understandable because both are heavily reliant on partnership and third-party ICT provision. But these ICT arrangements can't be an excuse for not protecting systems and the sensitive and confidential data held in them. All policing and fire and rescue service data and ICT systems must be protected against [cyberattack](#). Central to this is the need for forces and services to build robust monitoring and detection capability and [critical incident](#) response processes into all contracts.

Recommendation 12

By February 2027, the [National Fire Chiefs Council](#), in consultation with the Ministry of Housing, Communities and Local Government, should update its '[Digital, Data and Technology strategy](#)' to support the development of proactive [cybersecurity](#) monitoring and detection capabilities, available at all times, in all English fire and rescue services.

Third-party supplier networks and processes aren't routinely visible to force or service ICT teams

In several organisations we inspected, third-party suppliers held and managed system logs. These logs generate, gather and store information on security-relevant events or behaviour from computer systems, such as login attempts or access to sensitive data. Organisations can retrospectively analyse and act on this information to protect against and respond to threats.

But these logs weren't routinely visible to local force or service ICT teams. We found examples where monitoring was incomplete or outdated, where vulnerability scanning wasn't permitted and where system changes weren't visible to the organisation.

Personnel from both sectors told us they relied heavily on third-party suppliers for core monitoring. In some cases, they couldn't confirm whether their suppliers offered continuous coverage and weren't confident that the supplier would detect any intrusion promptly.

We also found some of the inspected organisations couldn't say with certainty:

- how effectively their suppliers monitored cybersecurity incidents, or how and where they stored their system logs;

- whether suppliers monitored privileged accounts (those that give users enhanced permissions to access sensitive data or carry out ICT administrative tasks); or
- whether suppliers used endpoint detection and response solutions, which continuously monitor devices and servers to identify and mitigate against malicious cyber activity, or relied on older security tools.

This lack of clarity is a strong indicator of significant underlying risks.

We found that both sectors need to prioritise and better manage cybersecurity monitoring and detection, whether they share ICT provision with public sector partners or rely on third-party supplier arrangements. They need to understand how such ICT partnership contracts will work to monitor, detect and prevent cyberattacks. And they must set clear contractual expectations around how these issues will be managed, how risks will be reduced and how cybersecurity information or intelligence will be shared effectively.

Until both sectors expand and standardise monitoring and detection across all systems, whether they use partnership ICT provision or a third-party ICT supplier, or operate with legacy systems, they will remain vulnerable to cyberattacks. We are concerned that without effective cybersecurity monitoring and detection, data breaches and cyberattacks may go undetected until significant harm has occurred.

The technological limitations of legacy systems present significant risks

Across all organisations we inspected, the limitations of legacy systems held back detection and monitoring efforts. Several had legacy systems that presented significant additional risks because of a lack of clarity around roles and responsibilities and how systems were configured, and limited cybersecurity assurance.

In some cases, uncertainty about where data was hosted or inconsistent logging meant that critical systems, including those supporting operational activity, didn't have comprehensive security oversight.

We found a range of legacy ICT platforms that:

- relied on outdated logging formats and didn't support modern logging;
- couldn't integrate with security information and event management tools;
- didn't have any application programming interfaces;
- couldn't run advanced endpoint detection software; and
- weren't compatible with modern authentication monitoring applications.

Both sectors' use of endpoint monitoring and detection varies widely

We found that the sectors' approaches to endpoint monitoring and detection varied widely. Some of the inspected organisations used modern endpoint detection and response tools and maintained strong internal monitoring arrangements. Others continued to rely on reactive antivirus products.

In several forces and services, we found evidence of unmanaged or partially managed devices, including legacy laptops, [mobile data terminals](#), multi-function devices and contractor equipment. These devices could operate outside standard controls, creating opportunities for attackers to evade detection.

The variation we saw in detection and monitoring coverage in the organisations we inspected was heightened by the design of their networks. A segmented ICT network is broken down into smaller networks to make it easier to control how traffic flows and what levels of access are allowed. But some forces and services operated flat or minimally segmented networks. In the event of a cyberattack, flat networks make it difficult to detect and prevent the spread of the attacker's activities, from one compromised device to others within the network. Without segmentation, a single compromised account could make it possible to access multiple systems, increasing the impact of an attack.

In some fire and rescue services, we saw that complex hosting arrangements could increase the risk of a cyberattack. Services using systems provided on local authority ICT networks often benefited from shared monitoring. But fire and rescue service-specific systems operating outside those environments weren't always included. This left some service-owned systems reliant on separate or less mature monitoring arrangements, potentially making them more vulnerable to a cyberattack.

Scanning and logging practices are inconsistent

We examined each inspected organisation's cyber vulnerability scanning activity. We found wide variations in the frequency of this activity, its level of sophistication and the extent of coverage across systems. Some ran regular scans to correct weaknesses in the system. Others relied on ad hoc scanning with incomplete coverage due to the limitations of legacy or hosted systems. In several cases, scanning didn't extend to supplier-managed or third-party networks. This limits an organisation's ability to identify broader vulnerabilities in systems supporting critical services.

We also found that the way forces and services logged and documented cybersecurity varied considerably. There were some examples of poor practice. For example, logs were often incomplete and retention periods varied – some logs could be overwritten within days. Access logging was missing on some legacy systems, and visibility of important logs was sometimes limited. In hosted environments, suppliers typically retained logs. But these weren't always accessible to, or routinely reviewed by, in-house ICT teams. The ICT teams sometimes kept logs but didn't actively analyse them, reducing their effectiveness.

8. Cybersecurity preparedness, resilience and recovery

Preparedness and resilience arrangements are underdeveloped and inconsistently applied

Preparedness for cyberattacks increases resilience

[Cybersecurity](#) resilience depends not only on preventing [cyberattacks](#) but also on being prepared to respond and recover when an incident happens. Even organisations with strong security controls can experience disruption, the extent of which depends largely on how quickly and effectively they can restore systems and maintain critical services.

All the organisations we inspected had business continuity and incident response arrangements. Senior leaders generally recognised the importance of maintaining services during disruption. But this awareness wasn't consistently supported by strong, tested and cybersecurity-specific preparedness. Across both sectors, we found weaknesses in business continuity planning, incident response, recovery arrangements, exercising (planned emergency testing) and organisational co-ordination.

These weaknesses increase the risk that a cybersecurity incident would result in prolonged disruption to critical services. This could include [control room](#) functions, [mobilisation](#) systems, [safeguarding](#) activity and access to operational information.

Effective cybersecurity preparedness requires every team to take part. The impact of a successful attack can extend far beyond ICT and affect every operational and support function.

Preparedness arrangements and planning shouldn't be confined to specialist teams

During our inspection, we were concerned to find that cybersecurity exercising and preparedness were often confined to specialist teams. Without regular, thorough cybersecurity exercising and clearly defined recovery arrangements, response efforts risk being slow, fragmented and overly dependent on a small number of specialists.

We found examples of good practice across both sectors. Some organisations had carried out cybersecurity exercises, developed cyber-specific response plans and improved recovery arrangements following previous incidents.

However, in others, preparedness was underdeveloped. Business continuity plans were often generic and didn't adequately address cybersecurity risks. Incident response plans were sometimes outdated, untested or unavailable offline. Exercises often lacked operational realism, and manual contingency arrangements hadn't always been tested. We also found limited co-ordination between operational and technical teams.

Many business continuity plans didn't reflect ICT recovery capabilities. Some relied on unrealistic assumptions, lacked clear recovery objectives or didn't clearly define responsibilities during a cyberattack. In several cases, plans depended on systems that would be unavailable during an attack.

We were particularly concerned where personnel were unable to explain their organisation's response plans and what they needed to do during a cyberattack.

Cybersecurity preparedness should become a routine organisational discipline. Planning, exercising and recovery arrangements should extend beyond ICT teams and form part of wider organisational resilience activity.

Based on the evidence we gathered, many forces and services would struggle to recover quickly from a successful cyberattack. This could affect operational performance, public confidence and public safety. Both sectors should review and clarify how they would respond to and recover from a cyberattack.

Incident response arrangements sometimes lack quality

All organisations we inspected had incident response documentation, but the quality of these plans varied considerably. In better-prepared organisations, incident response plans had clear activation triggers and clearly defined roles and escalation processes. In those forces and services, links between the incident response plans and business continuity plan were explicit. They also had documented decision-making structures, contact lists and communication templates.

However, in most cases, we found that plans hadn't been recently updated, weren't well understood by personnel and didn't reflect modern threats. This meant that those plans didn't reflect changes made to ICT systems. They lacked detail on communication with partners or suppliers and didn't include provisions for coping with prolonged incidents.

We also found several inspected organisations didn't have a clear protocol for determining when to ask for support from national bodies or suppliers. And unclear incident handling processes meant that personnel sometimes didn't understand how different types of digital incidents should be classified or escalated. This uncertainty increases the risk of delayed or inconsistent responses.

Control room preparedness for a cyberattack varied

Control rooms are critical to both policing and the fire and rescue service. They support call handling, mobilisation, communications, incident management and access to operational information.

Despite this, we found inconsistent approaches to control room cyber resilience arrangements. Common issues included:

- limited visibility of third-party ICT supplier resilience arrangements;
- insufficient testing of contingency plans;
- inconsistent training for control room personnel;
- reliance on untested alternative [fallback](#) processes to keep operations running if systems are taken offline; and
- dependence on legacy ICT systems.

Some organisations were confident they could continue to operate during a cyberattack. Others hadn't tested their arrangements under realistic conditions. And in some fire and rescue services, exercises hadn't tested contingency arrangements against cyber-specific scenarios. Many people we interviewed were uncertain how long critical services could be sustained during a cyberattack.

Given the importance of control room functions, we consider that both sectors need stronger co-ordination between ICT teams, cybersecurity specialists, operational personnel and control rooms. Cybersecurity resilience should form part of routine control room preparedness, exercising and contingency planning.

There isn't national, co-ordinated cybersecurity testing and exercising in either sector

Across both sectors, we found forces and services took part in a range of local operational cybersecurity testing and exercising activity, and had contingency and resilience plans. But we didn't find any evidence of an equivalent formal and nationally co-ordinated programme in either sector or between the two sectors. We couldn't find any evidence of joint collaborative cybersecurity testing and exercising programmes run between the Home Office or the Ministry of Housing, Communities and Local Government either.

Cybersecurity testing and exercising activity in both sectors is fragmented and lacks consistency. It varies considerably in content and method, so there isn't a coherent national approach. We found:

- there wasn't a mandatory programme of cybersecurity-specific exercising, and exercises were infrequent and uneven;
- exercises varied greatly in realism and technical depth;

- neither sector had a national requirement to test mobilising systems or control room functions under cybersecurity conditions;
- third-party suppliers weren't routinely incorporated into exercises, even where critical systems were outsourced;
- exercises tended to focus on operational disruption rather than technical detection, containment or recovery; and
- lessons weren't consistently consolidated and shared across organisations and sectors or used to inform national improvement activity or sector-wide standards.

This patchwork approach has some local value. But it falls short of providing the sector-wide assurance that would come from co-ordinated, repeatable national cybersecurity scenarios involving all police forces and fire and rescue services.

Local cybersecurity testing and exercising often has limited impact

We found that all the organisations we inspected had taken part in some form of cybersecurity training or exercising. These included tabletop exercises (discussing how the organisation would respond to an incident), workshops, incident response walkthroughs and phishing simulations (in which someone tricks users into revealing sensitive information).

We found examples where such exercises had produced useful insights. However, in most organisations, the impact of exercising was limited because:

- exercises focused on high-level scenarios without operational detail;
- technical teams took part but operational personnel, including control room staff, didn't;
- the organisations didn't use exercises to validate recovery timelines;
- lessons were documented but not accepted or understood by everyone;
- actions remained open for long periods; and
- exercises weren't repeated regularly or updated for new [cyber threats](#).

We also found that some of the inspected fire and rescue services struggled to carry out more disruptive forms of cybersecurity testing. For example, a temporary exercise involving a full or partial ICT system shutdown. Leaders in several of these services recognised the value of testing their organisation's resilience and dependency on digital systems. But because they didn't fully understand the process and its benefits, they had concerns about the potential impact on service provision and firefighter safety. As a result, testing was limited to tabletop exercises or technical simulations rather than live operational scenarios. While these approaches provide some assurance, they don't fully replicate the conditions of a real cyberattack or incident.

But we found some of the police forces we inspected didn't have such reservations. They were prepared to carry out live operational stress testing of their ICT systems and command and control functions. We commend them for taking this approach.

Some of the fire and rescue services we inspected had limited operational experience and lacked confidence that they could sustain critical functions during a cyberattack-related system outage. This was particularly the case if operational, communications or mobilisation systems were affected. We think that the sector must make improvements in this area.

Recommendation 13

By February 2027, the [National Fire Chiefs Council](#), in consultation with the Ministry of Housing, Communities and Local Government, should update its '[Digital, Data and Technology strategy](#)' to support the preparedness of all English fire and rescue services to respond to a [cyberattack](#).

Backup and recovery arrangements could be improved across both sectors

Backups and restoration are critical for recovering from [ransomware](#) attacks, data corruption or ICT system compromise. But, across both sectors, we found a range of unsatisfactory practices and processes that included:

- backup regimes that varied in quality;
- processes that were rarely tested end-to-end;
- backup ICT systems stored in locations that could be affected during an incident;
- incomplete or outdated backup documentation;
- uncertainty about recovery objectives; and
- suppliers that didn't provide clarity on their own backup regimes.

Across several of the inspected organisations, ICT and operational personnel highlighted their lack of understanding of cybersecurity backup processes, contingency plans and [service recovery](#) arrangements. Many interviewees were unsure how long ICT recovery would take. They didn't know whether all systems could be recovered or whether recovery processes had been tested recently. This potentially leaves forces and services exposed to systems being unavailable for long periods if a serious incident happens.

Opportunities for co-ordination and organisational learning are missed

An effective response to cybersecurity incidents requires clear co-ordination between ICT teams, operational leaders, control room managers and corporate functions, such as communications and data protection.

In some of the organisations we inspected, we found strong collaboration and good partnership working between ICT and operational response teams. But we also found examples of inconsistent involvement of operational personnel in exercises and unclear handover points during incident response. There was also evidence of some operational leaders having limited understanding of the technical impact of cybersecurity incidents.

Operations and ICT teams often worked in parallel rather than together to provide an integrated response. This was amplified in those fire and rescue services with shared service ICT arrangements that limited their ability to direct or co-ordinate their technical response.

We found that all organisations we inspected had experienced cybersecurity or ICT incidents that could have provided valuable [organisational learning](#). But neither sector consistently shared learning widely across the workforce. Nor did they maximise learning and development opportunities to encourage improvement. We found that, in many cases, cybersecurity learning and development outcomes weren't even documented properly.

Without effective cybersecurity learning and development processes and practices, both sectors will fail to improve their response to a cyberattack and may remain vulnerable to repeat incidents.

9. How police forces and fire and rescue services operate within national cybersecurity arrangements

National cybersecurity frameworks provide support, but don't provide consistent or sufficient resilience

National arrangements and frameworks provide valuable support

During our inspection, we found that national arrangements in the policing and fire and rescue sectors provided valuable support which strengthened the cyber resilience of local forces and services.

At a strategic level, the [National Police Chiefs' Council \(NPCC\)](#) and the [National Fire Chiefs Council \(NFCC\)](#), supported by the [Fire Standards Board](#), have developed [cybersecurity](#) standards, guidance and frameworks. These are all intended to improve resilience across policing and the fire and rescue sector. We found that these national bodies had an essential role in helping police forces and fire and rescue services to understand, manage and respond to cybersecurity risk.

Across the forces and services we inspected, we found that national arrangements provided valuable guidance, threat [intelligence](#), oversight and assurance. These arrangements help organisations identify emerging threats, share learning from incidents, raise awareness and highlight the priority status of strategic ICT and cybersecurity issues. In policing, the NPCC [National Assurance, Risk and Compliance service](#) manages the Security Assessment for Policing (SyAP) framework and provides expert support for police forces. And the [Police Digital Service \(PDS\)](#) carries out structured assurance against SyAP principles.

These arrangements are valuable but aren't mandatory across policing. The PDS told us that not all forces had enough local cybersecurity capacity and capability to prioritise the SyAP requirements. So the SyAP process alone can't guarantee consistently effective security outcomes. Put simply, the more forces invest time and effort in the SyAP process, the more cybersecure they will become.

In the fire and rescue sector, the NFCC has adopted the [National Cyber Security Centre's Cyber Assessment Framework \(CAF\)](#) to assess cyber resilience. At the time of our inspection, the use of the CAF within the fire and rescue service wasn't mandatory. And external validation was limited as there is no fire and rescue sector equivalent of the PDS. We found that the adoption of CAF and the quality of assessment varied significantly between services.

Organisational prioritisation and capability in each service therefore have a decisive role in determining its resilience. We found that these national arrangements were helpful. But, on their own, they aren't enough to provide robust cybersecurity resilience across the fire and rescue sector.

In both sectors, we found that the absence of mandatory national frameworks and inconsistent application of national guidance or standards meant there was significant variation in cybersecurity maturity levels. National bodies in both sectors offer support, but they don't yet provide a complete or consistent foundation for resilience.

There is significant variation in policing and fire and rescue cybersecurity capacity and capability

We also found that there was significant variation in how each sector approached cybersecurity and their respective capacity and capability to deal with the risks presented.

Policing benefits from several national bodies and programmes that don't exist in the same form in the fire and rescue sector. We interviewed many people in policing who described the real value of its shared investment in the PDS. And the added value and support gained from its range of cybersecurity service and products. Many highlighted the benefits of the PDS [National Management Centre](#). Specifically, its capabilities to identify, detect, prevent and respond to [cyberattacks](#) through the critical incident management process 'Defend as one' (set out in pillar 2 of the '[Government Cyber Security Strategy: 2022 to 2030](#)').

Other interviewees were extremely positive about the value of having national cybersecurity accreditation and assurance frameworks. They also spoke about the benefits of a SyAP self-assessment process which PDS cyber compliance specialists independently graded and supported at a local level.

During our inspection, we spoke to chief information security officers (senior executives responsible for an organisation's vision, strategy and programmes to protect and secure information assets and technologies) and senior information risk owners (senior executives responsible for overseeing corporate information and cybersecurity risks). Many who held these roles in policing were extremely positive about the cybersecurity focus and improvements established through the NPCC Police Information Assurance Board. They were also optimistic about the PDS's development of a new cybersecurity specialist learning and development programme.

These bodies provide structural advantages not consistently available to the fire and rescue service, and which are only now emerging as concepts or opportunities in that sector.

Policing can still improve its cybersecurity arrangements

Despite the strengths in police cybersecurity capacity and capability, we found that national arrangements still didn't provide:

- consistent visibility across all ICT systems;
- a central understanding of all local cybersecurity capabilities, including what ICT tools forces use to identify, monitor, detect or prevent risk;
- independent cybersecurity assurance for all third-party ICT suppliers;
- a mandatory baseline defining the minimum cybersecurity controls all police forces must implement;
- full end-to-end monitoring and detection across all ICT systems;
- consistent processes across policing on cyberattacks or near misses;
- consistent structured debriefs for all levels of cyberattacks, near misses or cybersecurity breaches;
- structured cybersecurity learning and development tailored to the whole workforce; or
- comprehensive national cybersecurity testing and exercising programmes.

National fire and rescue arrangements leave the sector without consistent protection

Fire and rescue services benefit from support from the Ministry of Housing, Communities and Local Government, the NFCC, [warning advice and reporting points](#), and local authority networks. These bodies:

- share threat intelligence and alerts;
- produce guidance and good practice materials;
- help peer discussion and collaboration;
- raise awareness of cybersecurity risks; and
- provide basic cybersecurity awareness training and learning resources.

However, the CAF framework and an annual cybersecurity assurance process aren't mandatory across the fire and rescue service. The NFCC can't make all services comply with the cybersecurity assurance process. Nor can it make each chief fire officer invest in implementing the CAF.

The NFCC doesn't centrally co-ordinate third-party supplier assurance or national monitoring or detection capability for the sector. The fire and rescue service doesn't have enforced technical baselines for identity, endpoint or network controls. Instead, the sector is guided by voluntary standards produced by the Fire Standards Board, and by the NFCC '[Digital, Data and Technology strategy](#)'. While these provide useful direction and align with other recognised frameworks, they aren't enforceable. As a result, adoption is inconsistent and services apply these variably.

Overall, the absence of mandatory national requirements means that the fire and rescue sector's cybersecurity resilience remains heavily dependent on local capability, capacity and leadership. This results in significant variation in maturity, leaving the sector without a consistent or assured baseline of protection.

Assurance of third-party ICT suppliers needs to be stronger

We found that both sectors struggled to make sure that partnership or third-party supplier ICT arrangements were cybersecure. Procurement and contracts for ICT provision were widespread and heavily relied upon. But we found that the general information security requirements in contracts were weak, particularly in relation to cybersecurity and assurance provisions.

In [chapter 5 of this report, 'Third-party ICT suppliers'](#), we mention how policing, through the PDS, has developed and implemented a [Third-Party Assurance for Policing \(TPAP\) model](#). This is a set of standards that police forces should adopt when procuring or contracting any third-party ICT system or product. It includes standards for forces to use to assess supplier compliance against SyAP.

This is a step in the right direction. But more needs to be done if policing is to have a more robust professional contracts process; one with a centralised and co-ordinated approach to managing the cybersecurity requirements of all partnership and third-party ICT contracts across policing. The TPAP model is a good starting point for all forces to adopt. However, the white paper on police reform, '[From local to national: a new model for policing](#)', also provides an ideal opportunity to improve and better co-ordinate the strategic approach to this issue.

Without some fundamental changes, policing will continue to duplicate effort and manage the heightened risks associated with the third-party ICT supply chain inconsistently and ineffectively.

In the fire and rescue sector, the third-party ICT provision and assurance landscape is completely fragmented. No national supplier assurance scheme equivalent to policing's TPAP exists. National guidance and fire standards are in place but aren't mandatory or supported by external validation. We found variation across services in supplier cybersecurity resilience. In some services, reliance on county councils or shared service arrangements further reduced local visibility and control of ICT systems.

Some senior leaders in the sector told us they lacked the specialist cybersecurity knowledge needed to test suppliers' claims and thought that national guidance was generic.

Supply chain cybersecurity incidents are frequent and can have severe consequences. But supplier assurance continues to largely depend on local capability and prioritisation. Without stronger national co-ordination, clearer accountability and consistent implementation of standards, this issue presents a serious risk to the fire and rescue sector.

Cybersecurity guidance and implementation present challenges

Across both sectors, national bodies publish cybersecurity guidance. This includes policy templates, risk frameworks, technical and data protection guidance, threat intelligence and incident reporting protocols.

However, we found that this guidance wasn't always well understood and adoption varied by organisation. Some guidance documents weren't clear enough and didn't offer practical examples tailored to the operational context. Some interviewees told us they were so busy that they struggled to apply guidance in practice.

Several fire and rescue sector leaders told us that, while national guidance was useful, services didn't always have the capacity or resources to implement it consistently. Leaders in one service we inspected highlighted the absence of mandatory cybersecurity standards, a national supplier risk framework or modernised funding models. They said this made it difficult for services to make sure everyone accepted and understood guidance.

Both sectors need to translate national cybersecurity guidance into effective local practices and build the capacity required to meet these expectations consistently.

At the time of our inspection, cybersecurity resilience depended too heavily on local capability, resulting in variation that placed public safety and service continuity at risk. To change this, both sectors need to strengthen national standards and guidance, improve co-ordination between national bodies and local forces and services and set clear lines of accountability in forces and services.

