COHESITY

Resilience and Resistance: The Future of Public Sector IT

COHESITY

EXECUTIVE SUMMARY

These are critical times for the delivery of change via digital services for the UK's public sector. However, because Public Sector IT covers so many different requirements and concerns, there is no 'One size fits all approach'.

Education, with its younger users, external stakeholders, such as parents, suppliers and under-fire Education professionals, is focused on insider threats.

Meanwhile, the **Emergency Services**, with its reliance on specialised Operational Technology (OT) and role in Critical National Infrastructure (CNI), is more concerned about supply chain threats.

Local Government, with its very public facing posture, is most concerned with phishing, vishing and social engineering, with 44% of its IT workers citing it as a top concern.

National Government concerns are much more long term, with 39% of IT workers worried about the shortage of skilled cybersecurity personnel.

These very different challenges mean, despite moves to collaborate across departments and regions, teams and boroughs, there remains a need to customize IT solutions to departmental or local requirements.

Perhaps because of recent high-profile ransomware attacks, the focus of public sector IT leaders has been on their ability to recover. However, they also recognise they now need to work more on detection and prevention. Ultimately to achieve genuine cyber resilience, detection, prevention and recovery in the UK must be world-class, but is that realistic?

Given the ongoing and well-publicised budget restrictions, the UK's Public Sector IT professionals recognise they need to consolidate infrastructure, share IT services where possible and strictly prioritize spend. While these are not new strategies, they do help to maximize the return on IT investments and ensure future resilience.

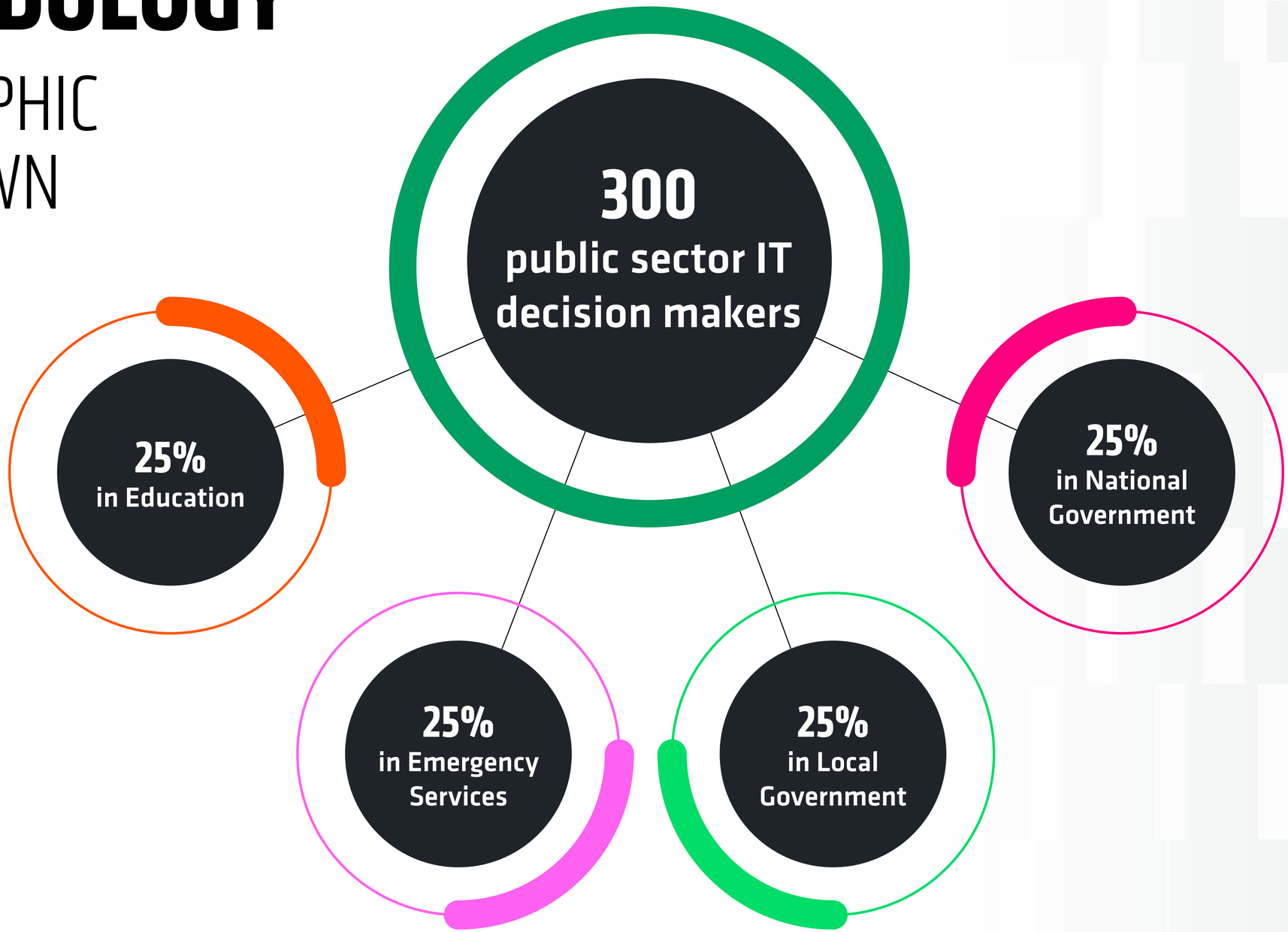
Despite this, Internal resistance to change is a significant barrier slowing the modernization of the Public Sector's many legacy IT systems.

In contrast, AI is already widely adopted for some tasks and is seen particularly as a way to accelerate the frequency of data integrity testing to ease anxiety about cyber threats - but does AI test recovery processes in the most appropriate way?

As promising as the new technology and its attendant uses are, all processes must be rehearsed by the 'human' aspects involved, because those interactions are what matter most when attacks inevitably and increasingly happen.

METHODOLOGY

DEMOGRAPHIC BREAKDOWN



PUBLIC SECTOR CONCERNS

COHESITY

CYBER CONCERNS DIFFER SHARPLY ACROSS PUBLIC SECTORS

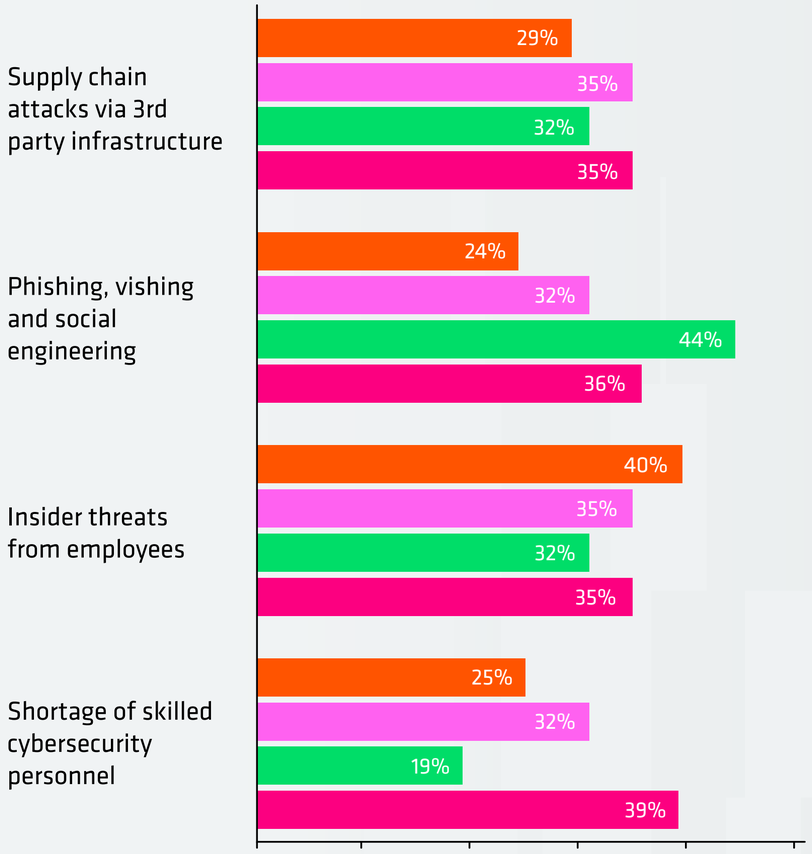
When it comes to cybersecurity priorities, the UK Public Sector is anything but unified. Every IT team faces distinct pressures shaped by its users, systems, and operating environments. Public-facing organisations, with their daily exposure to citizens, tend to emphasise protection against external threats, while others focus on internal weaknesses.

In Education, 40% tag insider threats as a top concern, perhaps a reflection of both the younger, more transient user base and the larger attack surface this provides. Emergency Services, meanwhile, with their reliance on highly specialised operational tech, are more concerned with supply chain vulnerabilities - a top concern for 35% of them.

44% of Local Government leaders focus most on phishing and vishing, where attackers exploit human behaviour as the entry point to a vast array of under-pressure services. At the National Government level the challenges are longer term and 39% see persistent cyber skills shortages as the biggest threat, slowing innovation and leaving critical services exposed.

Those already using AI are notably less concerned about cyber threats. However, concerns over legacy tech actually increase, from 24%-30%, among those using AI tools. This divergence shows there is no single roadmap to resilience, only tailored responses.

Top cybersecurity concerns - next 18 months



Concerns around the shortage of experienced skilled IT staff drop from 45% to 24% among those who use AI in their roles

- Education
- Emergency services
- Local Government
- National Government

CYBER CONFIDENT - MOSTLY

STRONG IN RECOVERY, WEAK IN DETECTION

There are signs Public Sector IT resilience is rising to meet escalating cyber threats. The best outcome is, of course, to prevent cyber attacks. Failing that, detection and recovery need to be as fast as feasible.

When asked about their confidence in detecting, preventing, and recovering from ransomware attacks, a clear pattern emerged: Public Sector teams are most confident in their ability to recover from cyber attacks, but less assured about detecting and preventing incidents in the first place.

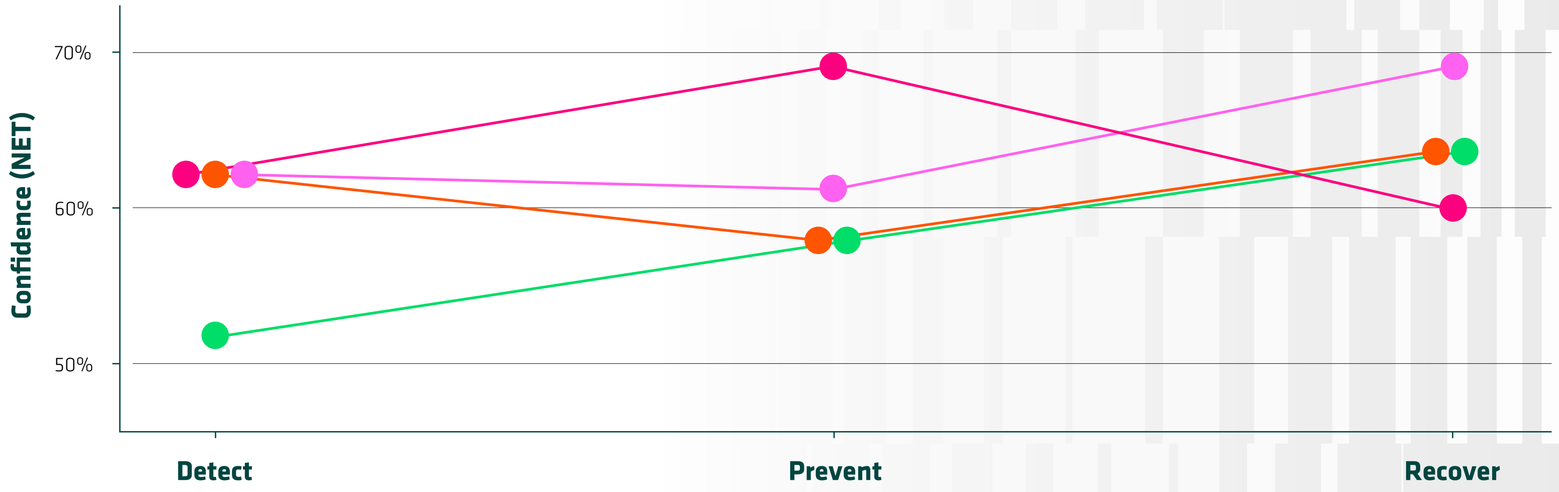
Overall 60% of respondents expressed confidence across their ability to detect, prevent and recover from cyber attacks. That's an encouraging sign that the sector is taking cyber resilience seriously. However, the picture is far from uniform. A sizable 40% reported low confidence, underscoring the persistent gap between ambition and capability.

Recovery is where confidence is highest. Many Government IT leaders are used to bouncing back quickly from attacks with proven incident response processes. Yet this confidence in recovery highlights a paradox: most are better at treating the symptoms than the causes. This leaves detection and prevention risks under-resourced.

Diving deeper, Local Government consistently lags behind other sectors with a breakdown of confident/not confident of 52%/48%. While the National Government and Education have made strides in standardising recovery processes, local councils remain more exposed to disruption, with fewer resources and stretched IT teams adding to the challenge.

Public Sector IT can rightly be proud of its resilience, it needs to strengthen detection and prevention to stop attacks before they cause damage and create budget-sapping costs.

How confident are you in your organisation's current ability to Detect/prevent/Recover from Ransomware attacks?



FREQUENCY OF STRESS TESTING

COHESITY

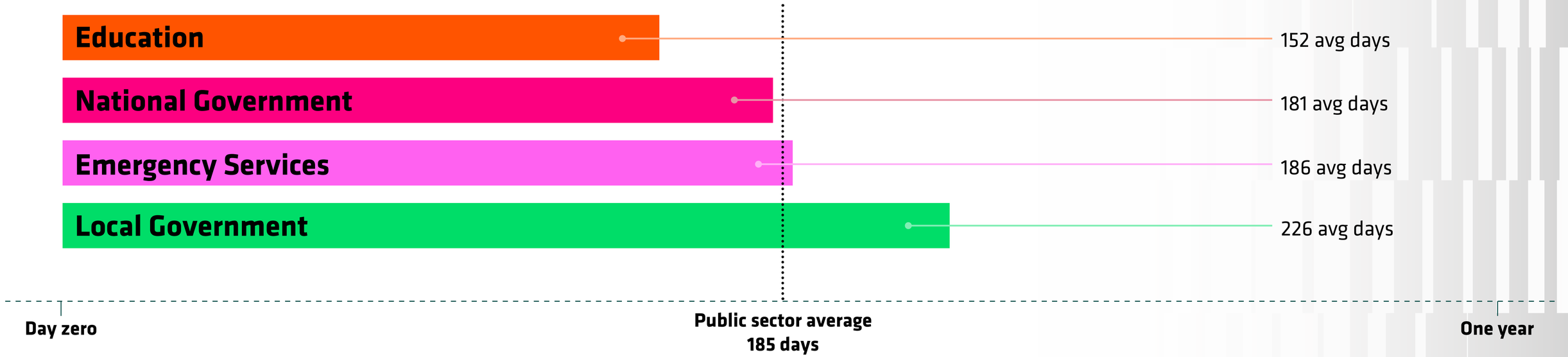
TESTING TIMES FOR PUBLIC SECTOR IT

Confident responses to cyber attacks rely on pre-testing defences. Encouragingly, the Public Sector is keeping pace with, and in some cases exceeding, the commercial sector average for stress-testing recovery plans. Our survey shows Public Sector teams conducting full-scale incident response tests at least every year, with many pushing further with testing on average every 186 days.

Education leads the way, running recovery tests roughly every five months, giving its IT teams a higher level of readiness than many private sector counterparts. National Government and Emergency Services hit the average of six months, but Local Government lags behind, stretching closer to seven months between tests - a gap which leaves critical services exposed.

AI acts as an accelerator. Respondents using AI tools test more frequently although the linkage is not definitive and does not suggest an overreliance on AI in testing. Practical real-world, or table top, testing helps engagement of consideration of priorities but nothing ensures cyber maturity better than repeated, multi-departmental, full disaster recovery testing practices.

How frequently does your organisation conduct full-scale tests of its data recovery plans?



IT MODERNISATION CHALLENGES

COHESITY

RESISTANCE TO CHANGE

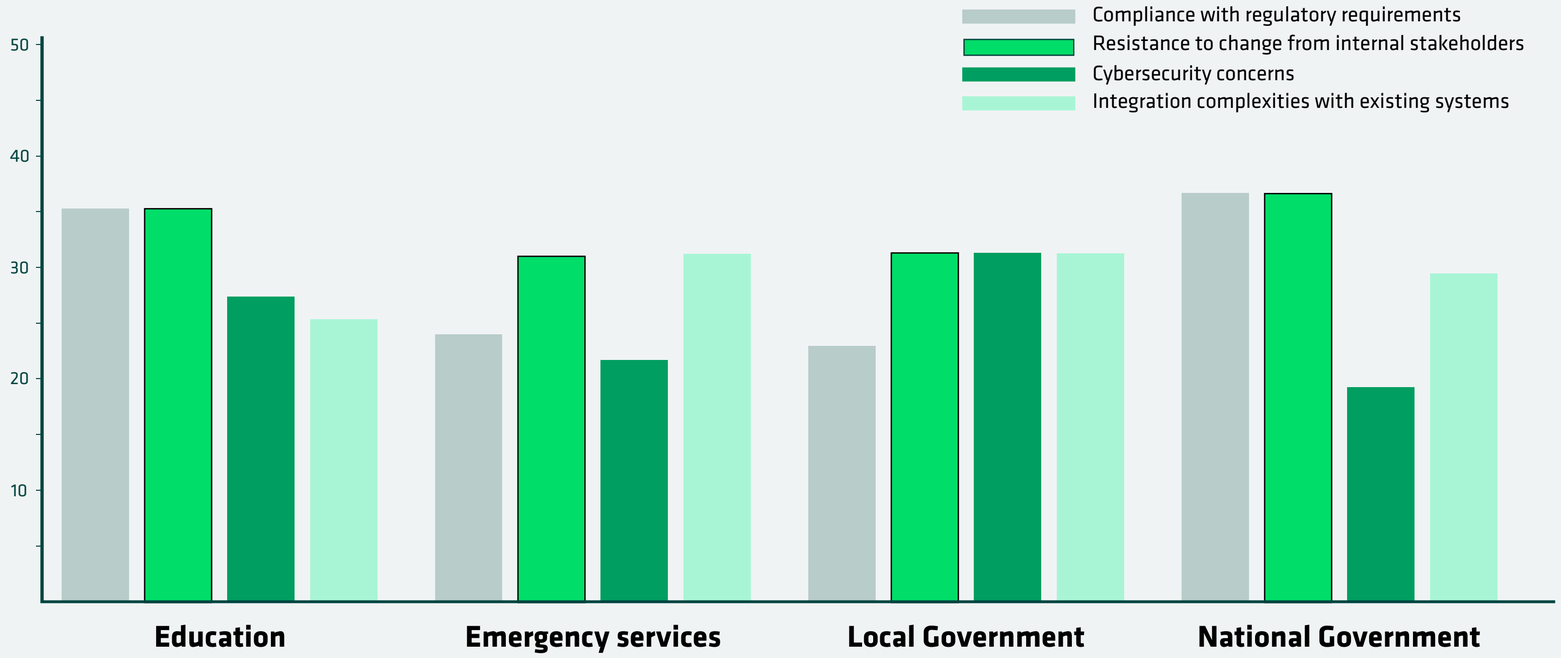
Modernising legacy IT systems remains the most pressing challenge for public sector leaders. Education and National Government IT teams struggle most with compliance requirements at 35% and 36% respectively. Local Government cites **cybersecurity concerns** at 31%, and 41% of Emergency Services workers cite integration complexities.

One challenge cuts across all sectors: **resistance to change from internal stakeholders**. Ranked the second-biggest obstacle in every sector, cultural inertia continues to slow progress more than almost any technical issue. For IT leaders, building resilience is about winning the confidence and cooperation of those who rely on them.

Those already using AI in their roles are even more likely to highlight resistance to change as their top concern, moving from fifth place issue for late AI adopters, to top concern among those using AI today. In fact, **resistance to change** is the only concern to increase among AI users compared to non-AI users, from 29% to 34%, showing while AI promises efficiency and automation, it also challenges existing IT working practices and heightens internal anxieties.

Ultimately, overcoming resistance requires more than technology upgrades. It demands strong communication, clear strategies, and a cultural shift towards embracing innovation. It remains the only surefire way to deliver repeated practice of multi-departmental, cyber attack response processes. Until then legacy systems remain an anchor dragging on public sector IT modernisation.

What are the biggest data related obstacles to modernising your legacy IT systems?



PARTNER PRIORITIES

PUBLIC SECTOR CHECKLIST SHOWS VENDORS MUST ADAPT

When choosing data management partners, Public Sector IT leaders express clear priorities. They need highly-compliant providers who demonstrate long-term financial stability and offer a roadmap that grows with their future needs.

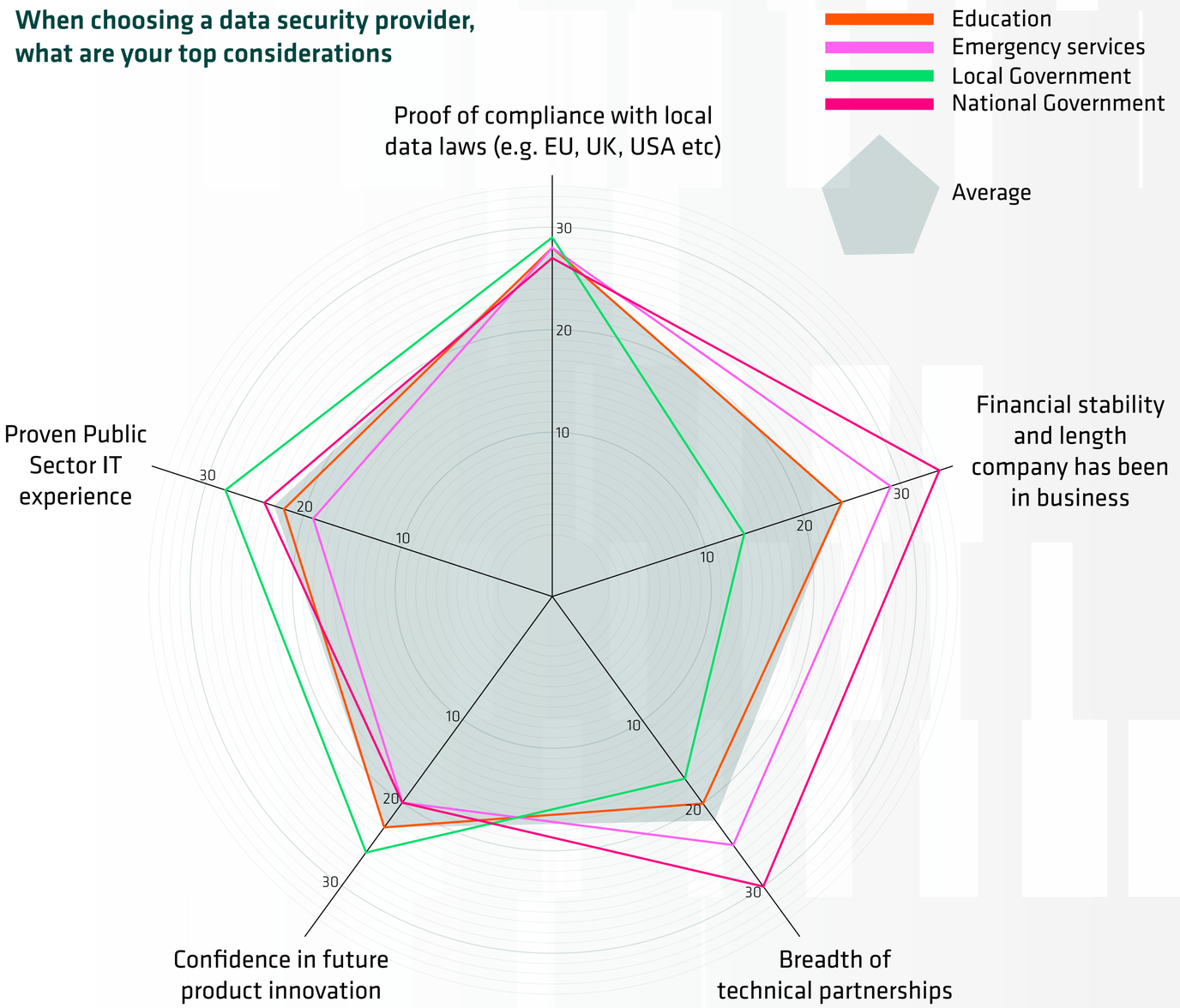
For Education and Local Government, compliance is the standout concern. With sensitive citizen and student data at stake, confidence a vendor can meet strict regulatory requirements is non-negotiable.

National Government and Emergency Services are both most concerned with the financial stability and length of time a partner has been in business. Here the similarities end, with 26% of Emergency Services respondents seeking platform-agnostic solutions as their secondary criteria, and 29% of National Government prizing breadth of technical partnerships.

Technology providers' Public Sector track record, often considered a key differentiator, now ranks lower. Instead, IT leaders value a consultative approach that supports them in navigating ongoing budget pressures and shifting security demands, paired with a vision for future innovation that keeps them ahead of the curve.

Public Sector buyers want partners who combine reliability with adaptability. The message is clear: flashy promises matter less than evidence of stability, compliance, the ability to innovate, adapt and genuinely evolve alongside the organisations they serve.

When choosing a data security provider, what are your top considerations



ARTIFICIAL INTELLIGENCE - NATURAL CONCERNS

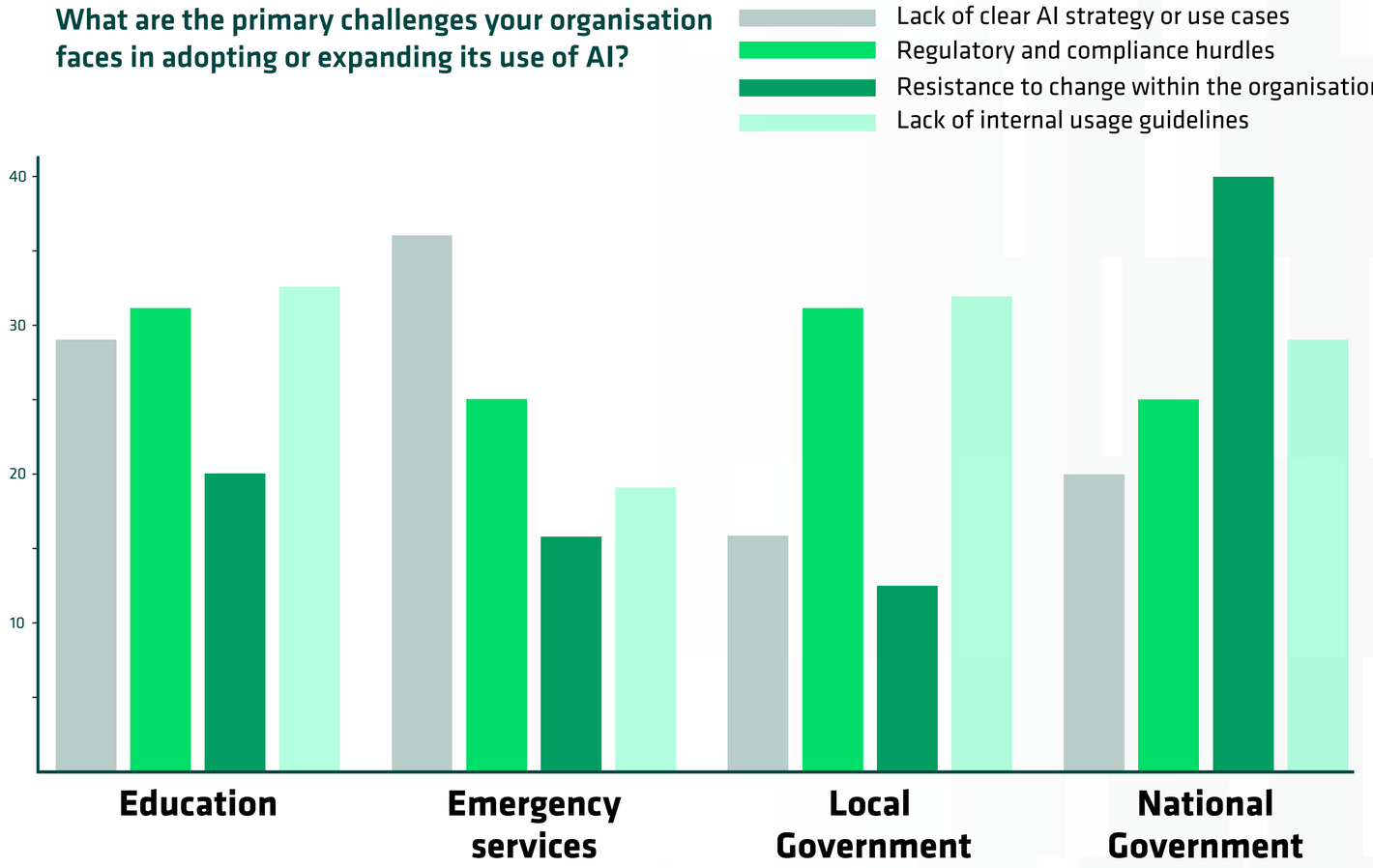
COHESITY

For a growing majority of workers, AI adoption is already used in day-to-day operations. In this survey, 79% of the respondents use it in their day to day roles. But the journey to further adoption looks very different depending on whether organisations are already using it, and which sector they work in.

Among those not yet using AI, concerns loom larger. These include uncertainty about whether it will be used "properly," anxiety over compliance, and a lack of internal clarity on strategy. Yet once AI is actually deployed, those worries diminish significantly, replaced by more practical discussions about scaling and optimising its use. The evidence suggests that experience builds confidence, even in a risk-conscious environment like the public sector.

Challenges vary widely across sectors. Education and Local Government highlight a lack of internal guidance, with 32% and 33% flagging it as a key challenge respectively. 36% of Emergency Services decision makers struggle with a lack of clear AI use cases, reflecting the specialised and high-stakes nature of their work. For the National Government, resistance to change is the biggest hurdle at 40%, underlining the cultural and organisational barriers to transformation.

What are the primary challenges your organisation faces in adopting or expanding its use of AI?



Education currently leads on adoption at 89% using it in their roles, while Local Government lags behind at only 73%. The uneven pace across the sector reflects the complexity of implementing AI - and the need for tailored strategies rather than one-size-fits-all solutions.

FRAMEWORK MAKES THE DREAM WORK

COHESITY

COMPLIANCE AND STABILITY TOP VENDOR CHECKLIST FOR PUBLIC SECTOR DATA PARTNERS

International, EU and UK national initiatives and cyber frameworks are beginning to reshape how Public Sector organisations approach cybersecurity - though not all with equal effect.

For more centralised systems, such as the Emergency Services, the Cyber Assessment Framework (CAF) has delivered real impact with 52% saying its resulted in less duplication of effort, streamlining cyber efforts in exactly the way it was designed to.

Similarly, Defend as One has proven valuable across departments, improving access to shared tools and resources and reinforcing the collective defence posture that public sector IT increasingly relies upon.

By contrast, Secure by Design has yet to make the same mark. While duplication of effort is the main advantage cited by all sectors, Its less-defined nature means perceptions vary widely, with some organisations struggling to translate the principle into tangible improvements. Still, as the approach matures, it may yet find its footing as part of a broader toolkit for resilience.

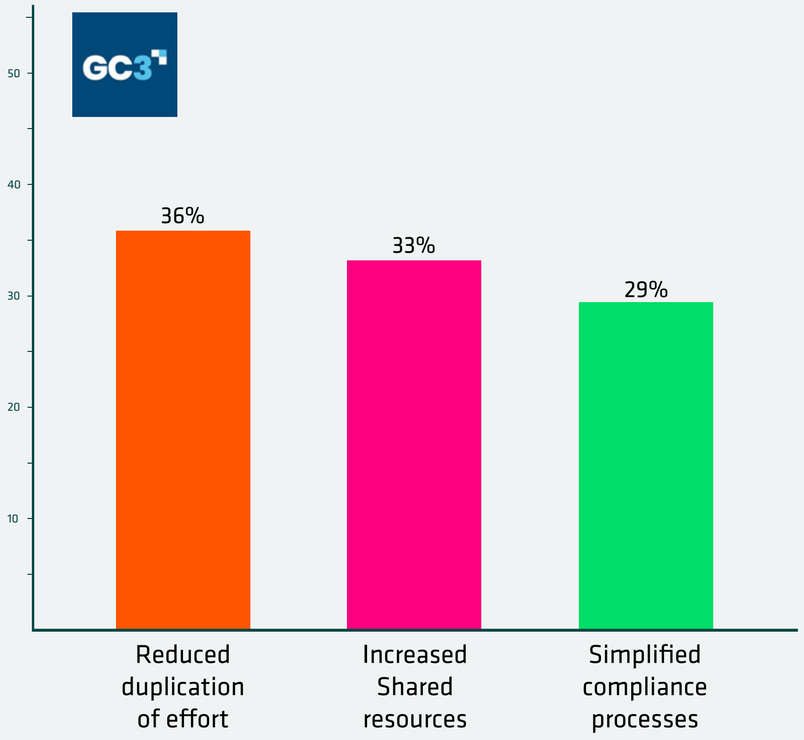
The clear lesson from these findings is that structured, well-embedded frameworks can make a meaningful difference. Where guidance is precise and adoption is collective, the public sector sees measurable gains in efficiency, resilience, and confidence.

FRAMEWORK MAKES THE DREAM WORK

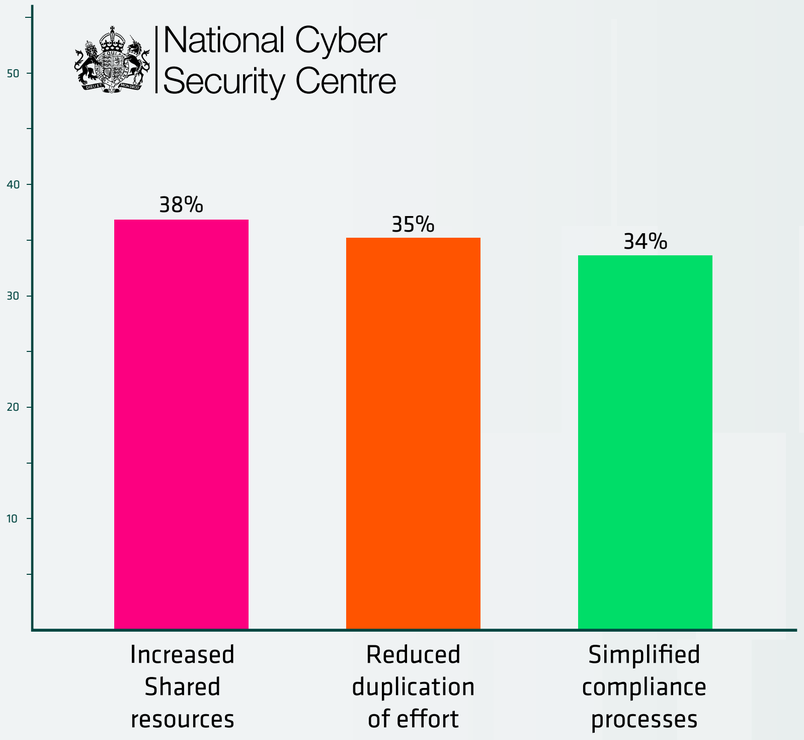
COHESITY

In what ways have the following initiatives impacted your organisation's ability to standardise cybersecurity practices?

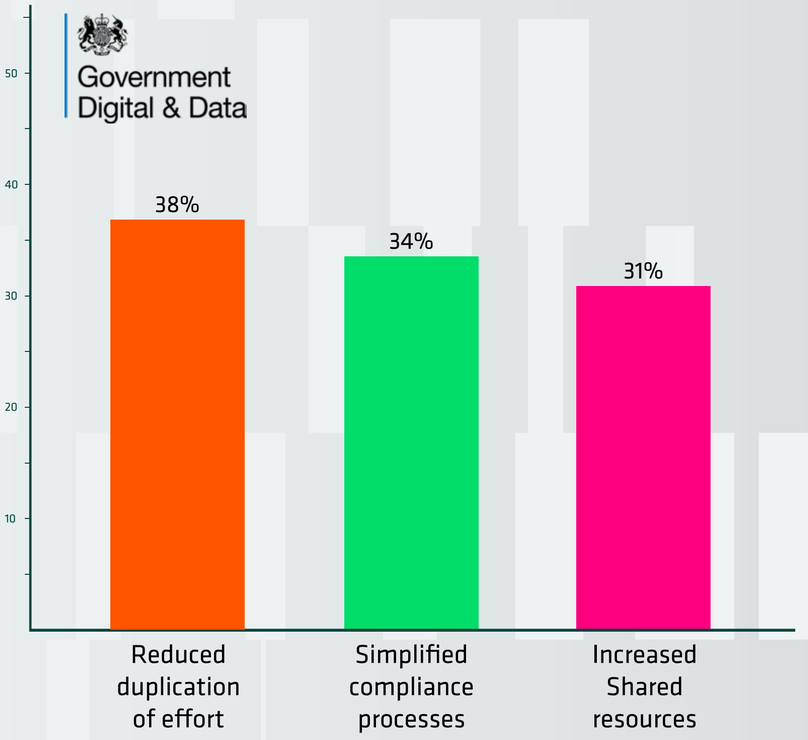
Defend as one



Cyber Assessment framework (CAF)



Secure by design



...AND TEAMWORK MAKES A DREAM WORK

Budget pressures are a constant reality for Public Sector IT teams, and how organisations respond to those budget pressures directly impacts the public that they serve.

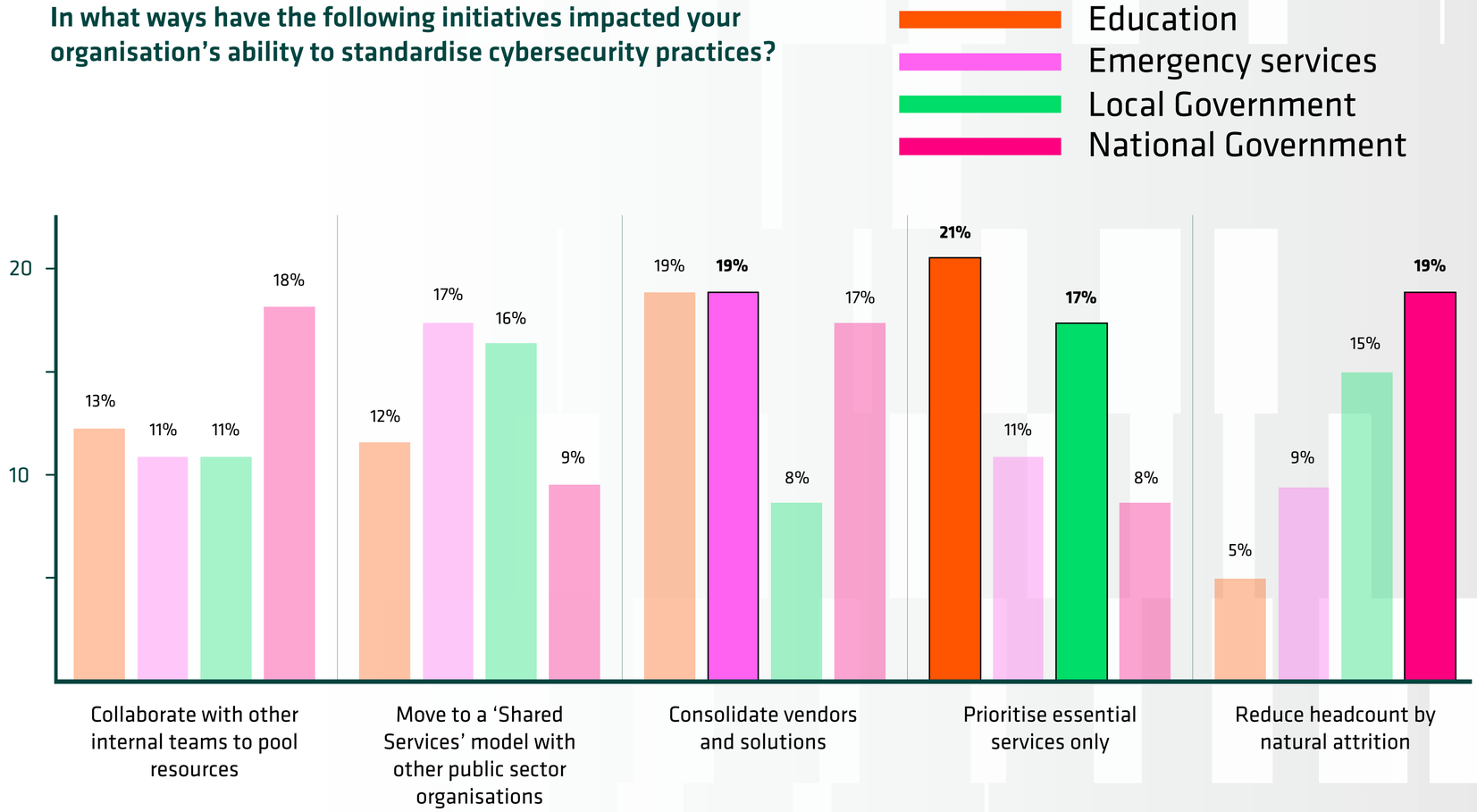
The closer an organisation is to citizens, the more likely it is to prioritise essential services only when funding is tight. Both Education and Local Government default to this most, cited by 21% and 17% of respondents respectively. This defensive stance reflects the frontline pressure to keep critical services running, even if it means delaying other projects.

Elsewhere, strategies vary. Consolidation of vendors and solutions emerges as a popular second choice across Education, Emergency Services, and National Government, at around 17% allowing leaders to stretch resources without sacrificing resilience. For National Government workers in particular, scale provides more flexibility: larger IT estates can absorb cuts by pooling resources or gradually reducing headcount through natural attrition.

Taken together, these responses highlight the pragmatism of Public Sector IT leaders. Faced with the ongoing challenge of "doing more with less," they favour collaboration, resource-sharing, and prioritisation over short-term fixes.

The result is Public Sector solutions which continue to safeguard critical services, while seeking more efficient infrastructure management despite budget constraints and cybersecurity threats.

In what ways have the following initiatives impacted your organisation's ability to standardise cybersecurity practices?



COHESITY

- Cohesity's **Destructive Cyberattack Resilience Maturity Model** is available to all organizations seeking to develop their resilience to destructive cyberattacks

- Get familiar with the five stages required to achieve cyber resilience by reaching out to us at **https://www.cohesity.com/contact/contact-sales/**