Whitepaper

People as the Frontline Defence:

Building Public Sector Cyber Resilience Through Workforce Development

OffSec™
The Path to a Secure Future™

Table of Contents

Executive Summary

Zero-trust architecture and AI-powered security tools dominate public sector cybersecurity discussions, yet the most critical security asset is overlooked: the workforce.

The human impact is real. Recent cyberattacks, such as the 2024 one on London hospitals, act as a wake-up call for the public sector. The incident resulted in delays to 10,104 appointments and 1,700 operations at King's College Hospital NHS Foundation Trust and Guy's and St Thomas' NHS Foundation Trust.[1] These numbers represent more than just data - they reflect real people and disrupted lives. Behind every statistic is a story.

A common theme runs throughout. 95% of all cybersecurity incidents involve human error.[2] Technology alone cannot solve this challenge. Often, public sector organisations focus on the process and technology, but overlook the people pillar. This blind spot is a vulnerability that disrupts lives, wastes money, and erodes public trust.

With the UK public sector 6.17 million staff strong, there's an unprecedented opportunity. Upskilling the workforce can transform this vulnerability into the sector's strongest defence. Leaders must encourage ownership from the board level to the frontline.

It's about breadth and depth. Cyber leaders need the right specialist skills in their teams to proactively identify weaknesses and stay ahead of bad actors. Yet tickbox training is not enough. Leaders must go beyond compliance and create a positive security culture. Continuous real-world skills development is crucial to keep pace with emerging threats in an increasingly hostile world.

Now is the time to invest in people as the frontline defence.

The Real Cost of Inaction

For the first time in UK history, a person's death has been directly linked to a cyberattack.[3] King's College Hospital NHS Foundation Trust confirmed one patient died during the ransomware attack in June 2024. A long wait for a blood test result due to the incident was identified as a contributing factor. This watershed moment is a stark reminder that cybersecurity is now a matter of life and death.

40% of ransomware attacks target the public sector, according to the National Audit Office.[4] With more than one in five public sector organisations reporting critical skills gaps, the question is whether your workforce is ready.

A series of recent high-profile cases, like The British Library, The Electoral Commission, and major London hospitals, serve as cautionary tales. These incidents illustrate the true costs of inaction.

Operational impasse

Cyberattacks can cause widespread disruption to staff and the public. The Electoral Commission, for example, was still reporting operational issues three years after an attack.[5]

Recovery costs

The cost of recovery should not be underestimated. The British Library was forced to spend up to £7 million, 40% of its reserves, on rebuilding digital services.[6]

Reputational impact

This is often a hidden cost of a breach. At a time when public trust is low, public sector organisations cannot afford the damaging impact of a cyberattack. Negative media attention can erode confidence and result in political criticism.

The business case is compelling. With the average ransomware demand costing a staggering £3.2 million, upskilling the workforce is an investment in prevention.[7] The impact on human lives and public trust is immeasurable.

Three Drivers for Change

Cybersecurity is an urgent priority for the public sector. Now is the time to prepare and bolster defences. Key policy drivers include:

The Cybersecurity Assessment Framework

This framework advocates a whole lifecycle approach, from managing risk, protecting against attacks, detecting threats, and minimising the impact. Principle B6 highlights the need for trained security specialists as central to an organisation's security posture.

The Government Cyber Security Strategy 2022 - 2030

This strategy calls for the public sector's critical functions to be significantly hardened to minimise the impact of cyber risk. It suggests the need for people, processes, and tech to work together. A cyber secure culture is not a nice to have, but a non-negotiable.

Legislative Backing

The government's upcoming Cyber Security Bill will mandate robust cybersecurity measures, making workforce development and supply chain protection a compliance requirement, not just best practice.

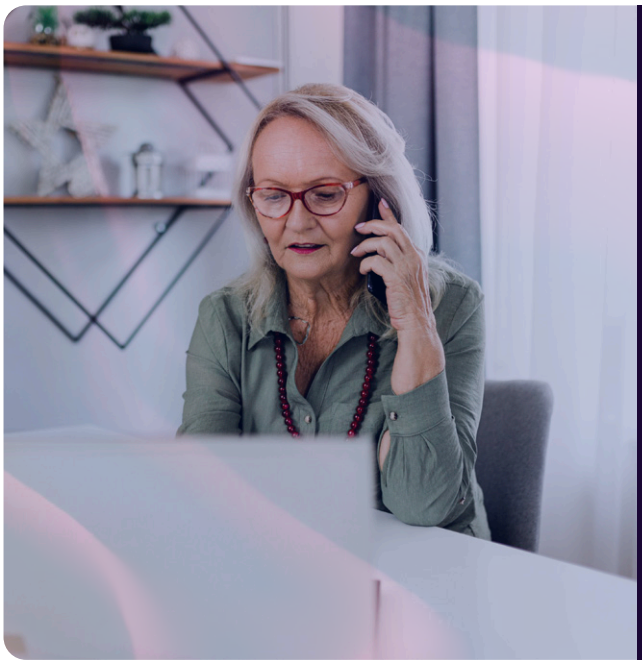
Sector-specific Challenges

While cybersecurity is a priority across the board, each sector faces its own unique challenges.

NHS:
Where Lives Hang in the Balance

While the shift from analogue to digital will accelerate transformation, it also multiplies vulnerabilities. The ransomware attack on blood services at major London Hospitals offered a sobering reminder. Cybersecurity is not just an IT concern, but critical to patient safety.

This presents a catalyst for change. In response to growing threats, NHS England has ramped up efforts, investing £4.3 million to enhance cybersecurity across the health service.[8] With 60% of staff calling for more cybersecurity training, there's an appetite and a need for workforce development to bolster defences.[9]



Local Government:
Democracy Under Siege

Almost half of UK councils hover on the edge of bankruptcy. Yet investing in cybersecurity is essential for survival. The 2020 Redcar and Cleveland Borough Council attack consumed £11.3 million in recovery costs.[10] The truth is that most councils cannot afford a ransomware incident.

Legacy tech and a lack of digital maturity represent a significant burden. Investing in the workforce presents an opportunity to empower staff at all levels to protect systems. With local government reorganisation, there are opportunities to think differently about cross-council collaboration and share learning to amplify impact.

Central Government:
The Uncomfortable Truth

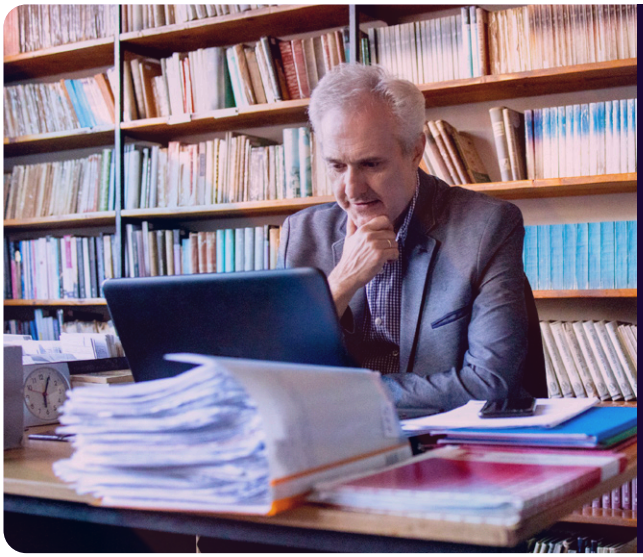
Despite bold commitments, the government faces an uncomfortable truth. National Audit Office findings suggest it's off track and has not met its goal of significantly hardening its defences by 2025.[11] 58 critical IT systems harbour significant vulnerabilities. Radical change is needed.

The new Government Digital Service presents opportunities to fundamentally reimagine services through digital transformation, with workforce development as a cornerstone.

Defence:
The Invisible Battlefield

As geopolitical tensions escalate, defence is more important than ever. UK government investment has reached the highest levels since the Cold War.[12]

Yet the nature of warfare is changing. The UK is in constant confrontation with hostile nation states in cyberspace, creating a new invisible battlefield. The *Strategic Defence Review* calls for a shift to a more proactive posture, strengthening the sector's offensive capabilities.



Education:
Shaping Tomorrow's Digital Citizens

Educational institutions hold vast amounts of sensitive data about students and families while operating with limited cybersecurity resources. The statistics are alarming: 91% of higher education institutions and 85% of further education colleges experienced a breach or attack in the last 12 months.[13]

The sector has an opportunity and a responsibility to nurture a cybersecurity talent pipeline for the future, as outlined in *The Cyber Growth Action Plan*.

Blue Light and Justice:
Cybersecurity on the Front Lines

Emergency services increasingly rely on digital systems for critical operations. Cyberattacks pose risks to public safety, making resilience essential for community protection.

In the justice system, attacks can undermine legal proceedings and damage trust. The *Ministry of Justice Security Strategy* suggests the need to create a positive security culture, extending training and awareness to all levels.[14]

Housing:
The Foundation of Digital Trust

With the government's pledge to 'get Britain building', housing associations face rapid growth and digitalisation. The Connexus incident in the West Midlands demonstrates increasing vulnerability.

Housing associations hold sensitive personal and financial data about tenants, often including some of society's most vulnerable individuals. New technologies like smart sensors and the Internet of Things introduce fresh attack vectors that only a cyber-aware workforce can effectively manage.

The Evolving Threat Landscape

Public sector organisations need to keep pace with a rapidly changing and increasingly hostile threat landscape:

Increased reliance on tech
Digital transformation across the public sector has a dark side - it increases reliance on tech. Incidents like the CrowdStrike IT outages show the potential for widespread disruption in a hyperconnected world. Emerging technologies like generative AI, the Internet of Things, and quantum computing all bring new vulnerabilities.

Geopolitical instability
The UK is the third most targeted country globally after the US and Ukraine.[15] The public sector's critical infrastructure and high-profile make it vulnerable to cyberattacks from hostile state actors, such as China, Russia, and Iran.

The scale and severity of attacks
The public sector faces an unprecedented volume of attacks, increasing the chance that the next one will be a catastrophic incident. The ICO reported that 21% of incidents managed by NCSC in the year to September 2024 were deemed to be nationally significant.[16]

Newly sophisticated threats
The rise of ransomware-as-a-service and generative AI is removing barriers to entry for potential bad actors. Deep fakes and executive impersonation make it harder than ever for the workforce to detect attacks.

The weakest link
A high reliance on legacy infrastructure makes the public sector vulnerable. Shadow IT and workarounds also create security issues. These legacy systems often cannot support the latest security tools, making human vigilance essential for threat detection.

Supply chain vulnerabilities
Complex supply chains increase the attack surface, creating multiple entry points. Third-party vendors and contractors often have less robust security controls while having privileged access to public sector networks.

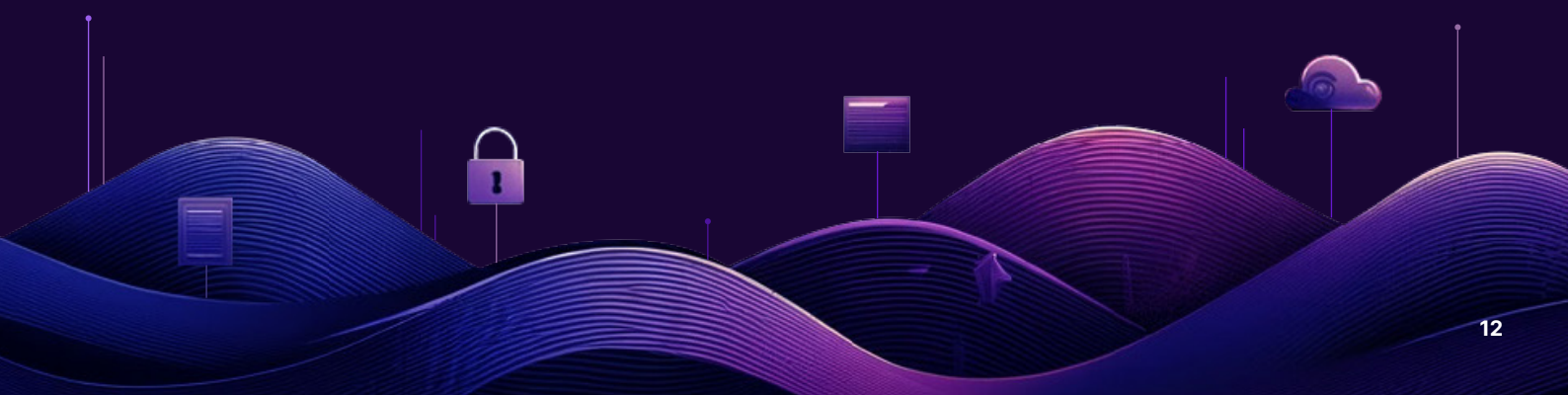
Yet the most insidious challenge is a blind spot. Organisations often overly focus on process and tech at the expense of considering people. This represents a vulnerability - and an opportunity - for the public sector.

With more than one in five public sector organisations reporting gaps in advanced cyber capabilities, the skills gap represents a national security risk.

The rapid growth of cyber threats creates new challenges, but traditional recruitment approaches fall short in the public sector context. Skills gaps are often more pronounced, as it's hard to compete with private sector pay. Outsourcing is challenging and expensive.

Forward-thinking organisations are shifting their focus from recruiting external talent to developing internal capabilities. The benefits are compelling. Home-grown talent understand your specific systems and risks inside out. In the event of a breach, internal teams can deliver faster incident response times and be cost-effective compared to contractor rates.

For visionary leaders, there's an opportunity to think creatively, for example, by creating IT to cybersecurity pathways and retaining talent through development.



The Human Factor

95% of cyberattacks succeed because of human error.

The human factor represents a challenge and an opportunity for the public sector. Tech and process are only part of the solution. Leaders mustn't underestimate the human aspect. It's essential to understand how people actually work and understand their pain points. When there are pressure points, staff are more likely to develop workarounds or make mistakes, creating vulnerabilities.

The public sector must invest in the overlooked pillar of people as a defence. This will demand three cultural shifts:

1. **From blame to a learning culture:** Counterintuitively, leaders need to create spaces where people can fail in order to succeed. A feeling of psychological safety will help staff come forward and learn from mistakes.

2. **Cybersecurity is everyone's business** Viewing cybersecurity as the preserve of Digital Data and Technology teams only creates vulnerabilities. The wider leadership team must take ownership and ensure all staff are supported in building a foundational awareness, bolstering defences.

3. **From a reactive to a proactive mindset** Too often, efforts focus on responding to threats and defending data. A shift is needed to a more offensive approach where staff anticipate and address vulnerabilities, strengthening cyber resilience.

The Supply Chain Imperative

Complex supply chains multiply the attack surface for public sector organisations. This was illustrated by the London hospitals cyberattack, where a ransomware group gained access through the third-party provider, Synnovis.

An internal focus is not enough. The gold standard ISO-27001 requires broader responsibility for managing third-party risk.

This includes:

Setting standards and minimum training requirements for suppliers

Regular assessments of third-party security practices

Incident response coordination across the supply chain

Commissioners must take action to address security gaps in suppliers before they become their problem.

Core Cyber Capabilities

Leaders must ensure their in-house cyber teams have the capabilities to prevent, manage and recover from a cyberattack. This requires strategic thinking about the skills needed to thrive in a rapidly evolving threat environment.

The Government Security Profession Career Framework provides structured guidance on nurturing cyber capabilities to create a strong team. Key capabilities include:[17]

Cybersecurity audit and assurance
This includes auditing the implementation of security controls and checking that the organisation is meeting compliance requirements. Attention to detail is key - this function is often the last line in defence.

Cybersecurity governance and risk management
This role works closely with senior stakeholders to assess risk and provide proportionate advice on business decisions. They often act as a bridge between digital and operations.

Digital forensics
Forensics is about capturing, analysing and reporting on evidence in line with legal guidelines. A meticulous approach is required to identify breaches of policy, regulations, or the law.

Incident response
This role handles incidents like cyberattacks, minimising disruption and ensuring robust learning to prevent a similar thing from happening again. Clear communication is key, including updating stakeholders across the business.

Monitoring
This is about gathering and analysing security event data, addressing malicious activity and escalating incidents. This broad view of the organisation enables the identification of new threat patterns.

Secure systems architecture and design
Secure by design is gaining momentum in the public sector. This role involves building IT systems with security in mind while delivering system requirements, blending technical and risk management skills.

Security testing
Also known as Penetration testing, this is about adopting an adversary mindset and attempting to penetrate existing defences. These insights help to address vulnerabilities and strengthen the security posture.

Vulnerability management
This role involves triaging vulnerabilities based on the risk posed to the organisation. Problem-solving is crucial. It's all about identifying mitigating actions and advising the business on practical implementation.

The Critical Skills Mix

Cybersecurity leaders need to step back and see the big picture of their team's skill mix. Understanding strengths and areas for development is crucial for building organisational resilience.

Teams must have these three capabilities covered:

Red team

This offensive approach involves using attacker techniques to identify vulnerabilities in organisational defences, helping organisations prepare before it's too late.

Blue team

This emphasises defensive operations, including monitoring, incident response, and threat hunting. These teams detect and respond to actual attacks.

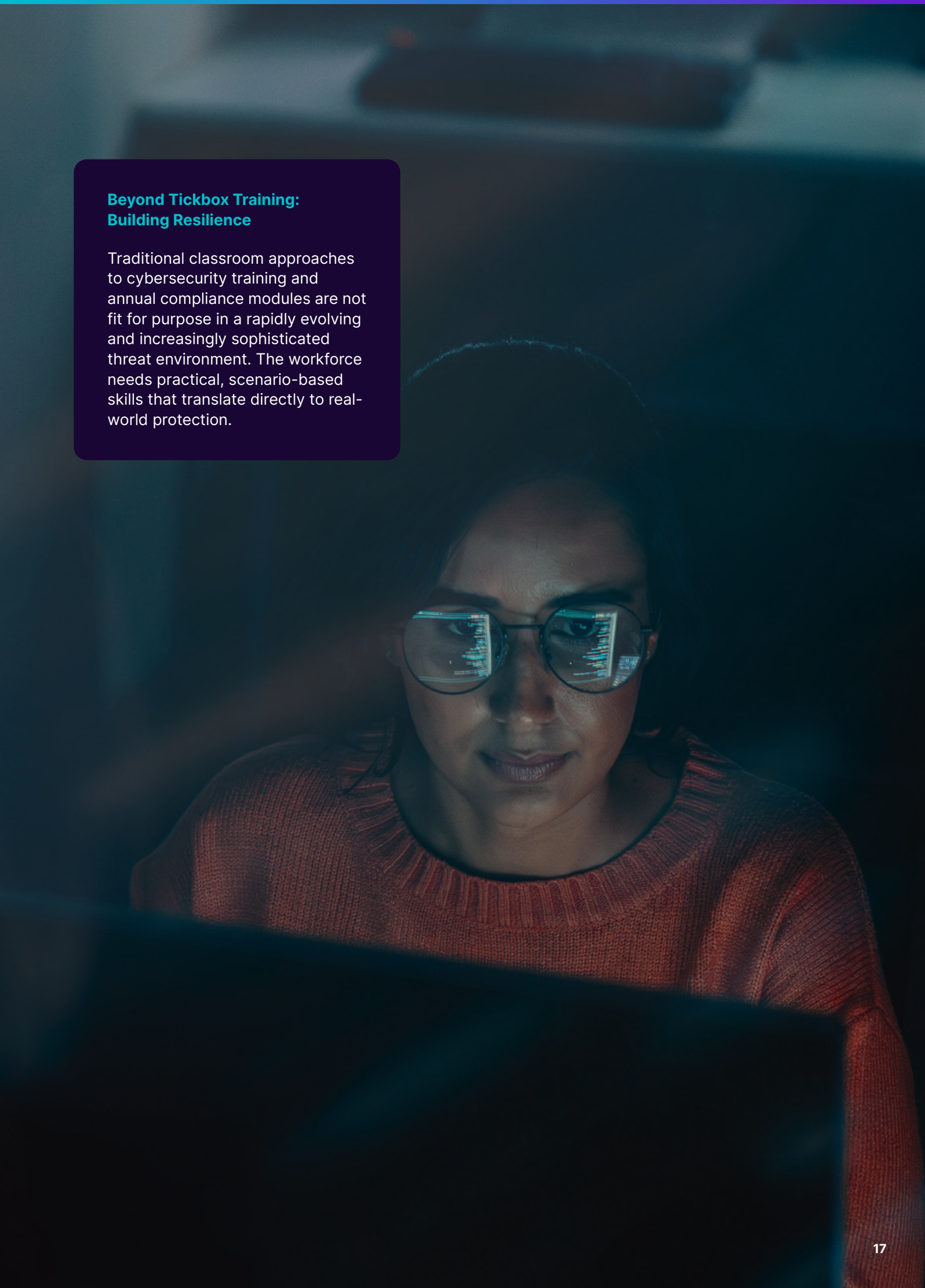
Yellow team

This is about building IT systems so they are secure by design, ensuring new developments include robust security protocols.

Purple team

Cross-collaboration between red and blue teams helps share learning and improve the overall security posture.

Public sector organisations often lack red team capabilities, limiting their ability to test defences against realistic attack scenarios. Addressing this gap through workforce development can transform organisational security posture.



Beyond Tickbox Training: Building Resilience

Traditional classroom approaches to cybersecurity training and annual compliance modules are not fit for purpose in a rapidly evolving and increasingly sophisticated threat environment. The workforce needs practical, scenario-based skills that translate directly to real-world protection.

The 7 Essential Workforce Development Strategies

Immersion	Scenario-based training labs enable cyber teams to hone real-world skills. Immersion in a simulated environment can help shift staff from theory to practical application.
Gamification	Balancing robust content with fun is crucial to incentivise and motivate teams. Pitting your red team against your blue team in a safe environment can create healthy competition and give your department the edge.
Tracking progress	Progress markers can incentivise staff to make time for continuous development. For leaders, these indicators help them better understand the skills mix and gaps within the team.
Continuous learning	One-off training cannot keep pace with evolving threats. Cyber professionals need ongoing learning and development to adapt to emerging attack vectors and adversary tactics.
Adversarial thinking	Teams must reframe their mindset to think like an adversary. This proactive offensive approach is often overlooked in the public sector. It's all about pinpointing vulnerabilities and addressing them before it's too late.
Cross-functional collaboration	Sharing across different teams within the organisation can create richer experiences and strengthen relationships across boundaries. Including operational teams can build understanding of real-world working practices and address vulnerabilities.
Individualised learning experiences	In addition to shared learning, individualised learning can help participants deepen their skills. This could include a combination of approaches, like self-study, online courses, conferences, and more.

Implementing these strategies delivers quantifiable benefits:

- **Faster detection:** Reduced time from breach to detection.
- **Quicker response:** Accelerated incident containment and recovery.
- **Increased confidence:** Staff feel empowered to flag potential threats.
- **Cultural change:** Security becomes embedded in daily operations, not an afterthought.

Investing in the workforce has the potential to make people the public sector's greatest asset and strongest defence.

Case Study: The US Coast Guard Academy

Transforming cyber capabilities with real-world training

The Challenge: Bridging the Gap Between Theory and Practice

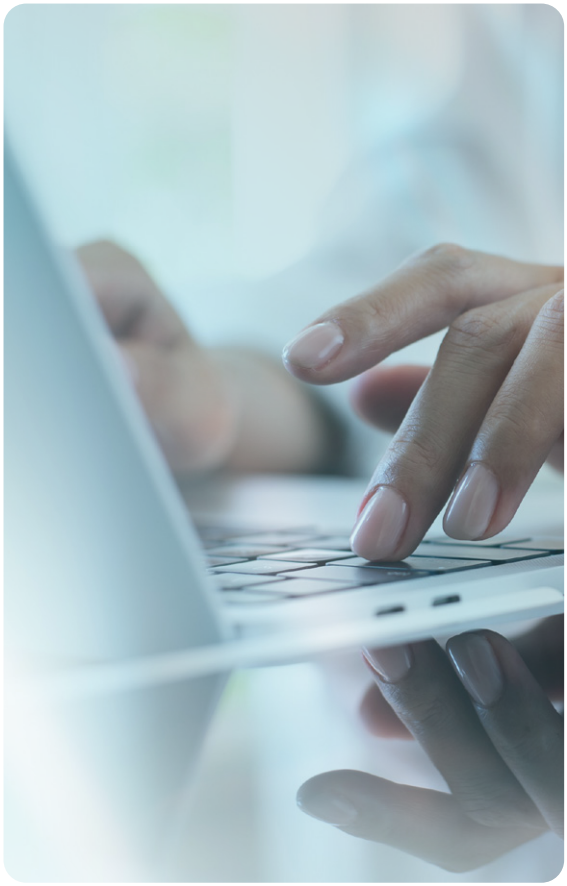
As an elite military training college, the US Coast Guard Academy educates future leaders to ensure the safety and security of the nation's waters. Introduced in 2018, the Cyber Systems Major recognises the growing importance of cybersecurity skills.

The goal is to prepare cadets for the real-world pressures of handling security incidents. Unlike academic subjects, memorising facts is not enough. The Academy needed to equip graduates with practical, industry-recognised skills while operating on a constrained budget.

The Approach: Certified Hands-on Training for Foundational Skills

The US Coast Guard Academy approached OffSec to deliver rigorous training through the SEC-100: CyberCore Security Essentials course, leading to the CyberCore Certified (OSCC SEC-100) certification. These industry-recognised credentials helped cadets apply knowledge in real-world scenarios, preparing them for professional practice.

OffSec supported the Academy to share learning across red and blue teams, helping cadets realise the need for a well-rounded skillset to succeed in cybersecurity.



The Results: Driving Performance and Strengthening Resilience

After the intensive OffSec training, the Academy achieved its best results in the National Cyber League competition.

Team Performance
Their team placed eighth out of 5000 teams, a huge improvement from the previous year.

Individual Excellence
Several cadets placed in the top twenty out of 9000 competitors.

Standards Setting
The OSCC certification provided clear benchmarks for foundational skills.

‘The hands-on nature of the training - particularly in the OSCC - forced us to really think on our feet and tackle problems we might never have encountered before. And honestly, that’s the kind of challenge that’s both nerve-wracking and exciting. It pushed us in ways we haven’t anticipated, especially when it came to things like problem-solving under time pressure.’

Max Eisenbeiser,
Training participant.

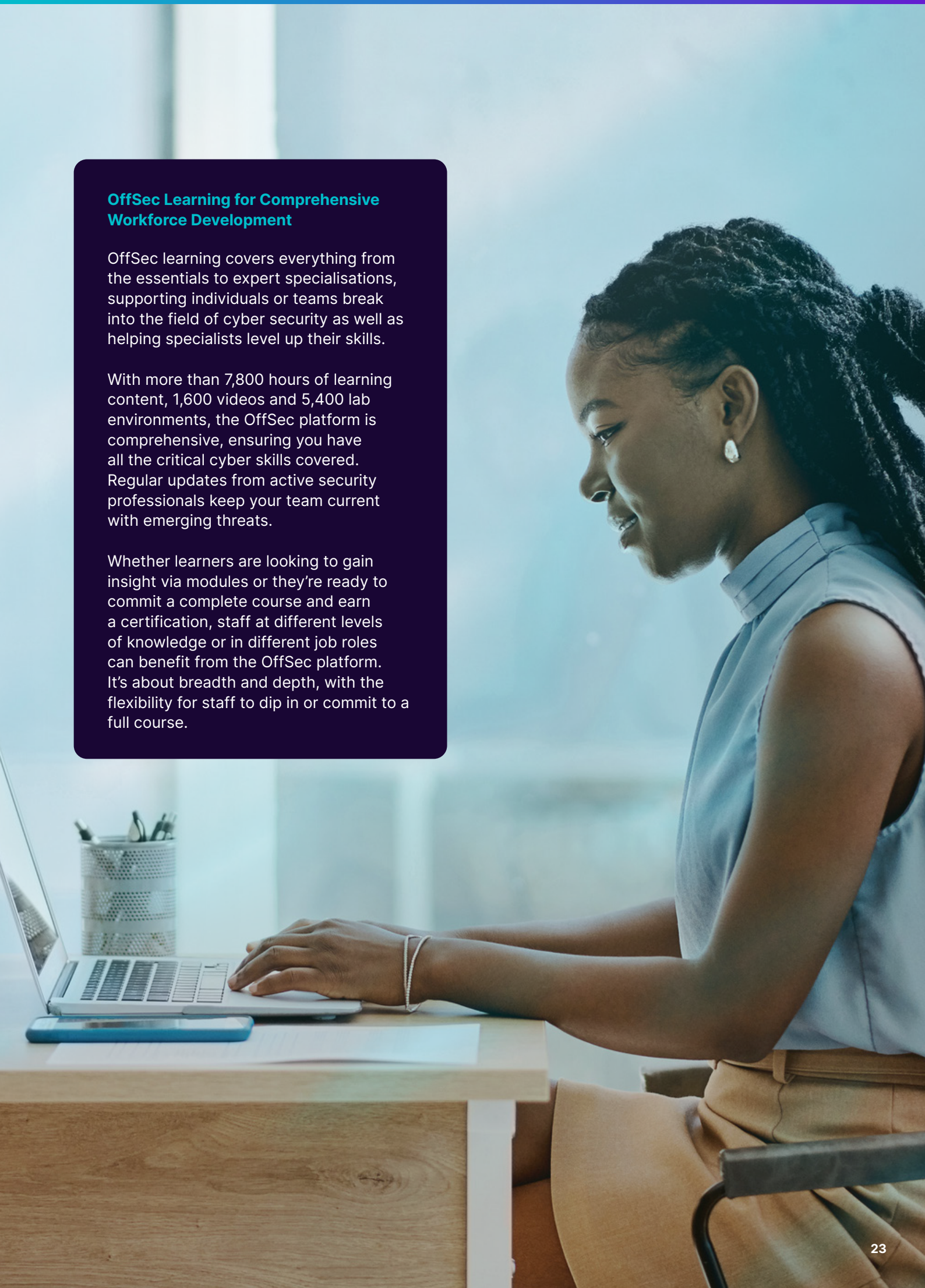
Bolster your Security Posture with OffSec

Looking to address cyber skills gaps and secure resilience? OffSec is the leading provider of cyber workforce training, offering real-world, industry-leading courses, certifications, and skills improvement to the public sector.

OffSec learning gives cybersecurity teams the hands-on, real-world skills that build genuine capability, not just compliance. Unlike passive training modules, their development programmes are built around practical labs, adversary-style challenges, and scenario-based learning — so skills are proven, not just claimed.

'The Offsec platform has proven vital to the upskilling and development of the team, providing clear technical pathways/certifications, challenge labs and CTF exercises via a blended learning approach of instructor led videos, learning materials and exercises. The vast array of content which continues to be added to throughout the year aligning to new threats. Techniques and job roles, along with the continued platform development and enhancements from Offsec means that this has and will continue to be a core learning tool for the team moving forward.'

OffSec customer, UK government body



OffSec Learning for Comprehensive Workforce Development

OffSec learning covers everything from the essentials to expert specialisations, supporting individuals or teams break into the field of cyber security as well as helping specialists level up their skills.

With more than 7,800 hours of learning content, 1,600 videos and 5,400 lab environments, the OffSec platform is comprehensive, ensuring you have all the critical cyber skills covered. Regular updates from active security professionals keep your team current with emerging threats.

Whether learners are looking to gain insight via modules or they're ready to commit a complete course and earn a certification, staff at different levels of knowledge or in different job roles can benefit from the OffSec platform. It's about breadth and depth, with the flexibility for staff to dip in or commit to a full course.

Practical Learning to Strengthen Resilience

OffSec's cyber security learning can provide public sector cyber teams with practical, continuous, and threat-aligned cybersecurity training that supports national resilience, modern workforce capability, and secure digital services. Key benefits include:

1

Real-World, Hands-On Cyber Training

- **Immersive, lab-based learning mapped to MITRE ATT&CK and NCSC threat models.**
- **Covers attacker TTPs, including:**
  - Malware delivery & evasion.
  - Privilege escalation.
  - Network lateral movement.
  - Active Directory exploitation.
  - Cloud misconfigurations (Azure, AWS).
- **Outcome:** Public sector analysts and defenders can simulate, detect, and defend against real adversaries—from script kiddies to APTs.

2

Aligned with Government Frameworks and Standards

- **Supports upskilling in line with:**
  - Cyber Security Profession Capability Framework (CSPCF).
  - NIST/NCSC guidelines.
  - Government Security Function and Digital Data and Technology roles.
- **Modular content mapped to job functions: SOC analyst, incident responder, pentester, architect.**
- **Outcome:** Consistent, scalable development of cyber capability across the public sector and national security roles.

3

Progression to World-Class Certifications

- **Pathways to certifications such as:**
  - OSCP (used by numerous departments and agencies).
  - OSEP, OSWA, OSMR – for advanced or specialist cyber roles.
- **Recognition that meets or exceeds standards of top-tier government and public sector vetting and skills frameworks.**
- **Outcome:** Measurable, certifiable assurance of practitioner capability

4

Strengthens Cyber Talent Retention and Morale

- **Role-aligned learning keeps cyber professionals engaged and challenged.**
- **Fosters a culture of technical mastery and continuous learning within secure government environments.**
- **Outcome:** Helps reduce attrition and reliance on contractors by investing in in-house skills.

Ready to Transform Your Cyber Resilience?

OffSec's workforce development solutions help you transform your biggest cybersecurity risk into your strongest defence. Discover how their learning solutions can help your team stay ahead of evolving threats today.

Book your discovery call now

The future of public sector cybersecurity isn't just about firewalls or stricter policies.

It's about people, the 6.17 million public servants who, when properly trained and empowered, become the strongest defence against increasingly sophisticated threats.

As AI and automation multiply the scale and sophistication of attacks, the human element becomes more critical. Advanced persistent threats, deep fake social engineering, and AI-generated phishing campaigns require human insight, intuition, and decision-making to detect and counter.

Investing in cyber skills can address workforce gaps, drive retention and strengthen cyber resilience. It's about going beyond tickbox training. Continuous, practical workforce development is essential. When supported to develop and thrive, people are the public sector's strongest defence.

References

1. Gov.uk. 'Cyber security breaches survey 2025.'
www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025

2. NHS England. 'Update on cyber incident.'
www.england.nhs.uk/london/2024/08/29/update-on-cyber-incident-clinical-impact-in-south-east-london-thursday-29-august/

3. Parliament UK. 'Cybersecurity in the UK.'
researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf

4. BBC. 'Ransomware attack contributed to patient's death.'
www.bbc.co.uk/news/articles/cp3ly4v2kp2o

5. National Audit Office. 'Government Cyber Resilience.'
www.nao.org.uk/wp-content/uploads/2025/01/government-cyber-resilience.pdf

6. Computing. 'Electoral Commission admits painful lesson.'
www.computing.co.uk/news/2025/security/electoral-commission-admits-painful-lesson-after-2021-hack?

7. The Financial Times. 'British Library to burn through reserves to recover from cyber attack.'
www.ft.com/content/4be5d468-0cc3-4881-a5fb-b5d0163de93e

8. Ibid 3.

9. HSJ. 'NHSE to monitor cyber vulnerabilities in NHS suppliers.'
www.hsj.co.uk/technology-and-innovation/nhse-to-monitor-cyber-vulnerabilities-in-nhs-suppliers/7037378.article

10. BT. 'Research reveals NHS cyber security perceptions.'
newsroom.bt.com/research-reveals-nhs-cyber-security-perceptions/

11. BBC. 'The inside story of a council held to ransom in cyber attack.'
www.bbc.co.uk/news/articles/cpw72pxrgdzo

12. Ibid 5.

13. Gov.uk. 'The Strategic Defence Review.'
www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad

14. Gov.uk. 'The Cyber Security Breaches Survey 2024.'
www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex

15. The Ministry of Justice. 'Cyber Security Strategy.'
assets.publishing.service.gov.uk/media/6581a6bffc07f3000d8d44b9/moj-cyber-security-strategy-2023-2028.pdf

16. The Independent. 'UK now ranks third in the world for cyber attacks.'
www.independent.co.uk/tech/security/cyber-attacks-uk-malware-nordvpn-b2802948.html

17. Gov.uk. 'Cyber laws to safeguard UK economy.'
www.gov.uk/government/news/new-cyber-laws-to-safeguard-uk-economy-secure-long-term-growth

18. Government Security. 'Government Security Profession Career Framework.'
www.security.gov.uk/government-security-profession-career-framework/cyber-roles/cyber-security-audit-and-

About OffSec

OffSec is the leading provider of continuous professional and workforce development, training, and education for cybersecurity practitioners.

OffSec's distinct pedagogy and practical, hands-on learning help organizations fill the infosec talent gap by training their teams on today's most critical skills. With the OffSec Learning Library featuring 6,000 hours of content, 1,500 videos, 2,500 exercises, and 900 hands-on labs, OffSec demonstrates its commitment to empowering individuals and organizations to fight cyber threats with indispensable cybersecurity skills and resources. OffSec also funds and maintains Kali Linux, the leading operating system for penetration testing, ethical hacking, and network security assessments.

About GovNews

GovNews specialise in facilitating innovative and engaging partnerships between the private and public sector. We have evolved to form a leading Public Sector news brand that is well established, trustworthy and identifiable for bringing positive news, views and insights that can deliver meaningful and long-lasting change.

Our content work embodies the transition and balance from conventional engagement, like corporate strategies, thought leadership and whitepapers, to the digital realm of video, social media, and online content. We supplement this work with both online and in-person engagements and events, integrating our long and well-established expertise in event production and UK Public Sector insights.

Our latest innovation, GovNews Community, is a unique platform exclusively designed for UK Public Sector professionals. This dynamic network offers a space where members can engage in discussions, access insightful content, watch informative videos, and actively participate in a thriving community. Much like a specialised social media platform, this hub facilitates seamless interaction, enabling members to connect, share ideas, and stay updated on industry trends. By fostering this online community, we empower UK Public Servants to collaborate, learn, and exchange knowledge, creating a vibrant and supportive environment that enhances their expertise and impact within the sector.

OffSec™ The Path to a Secure Future™ | GOV.NEWS