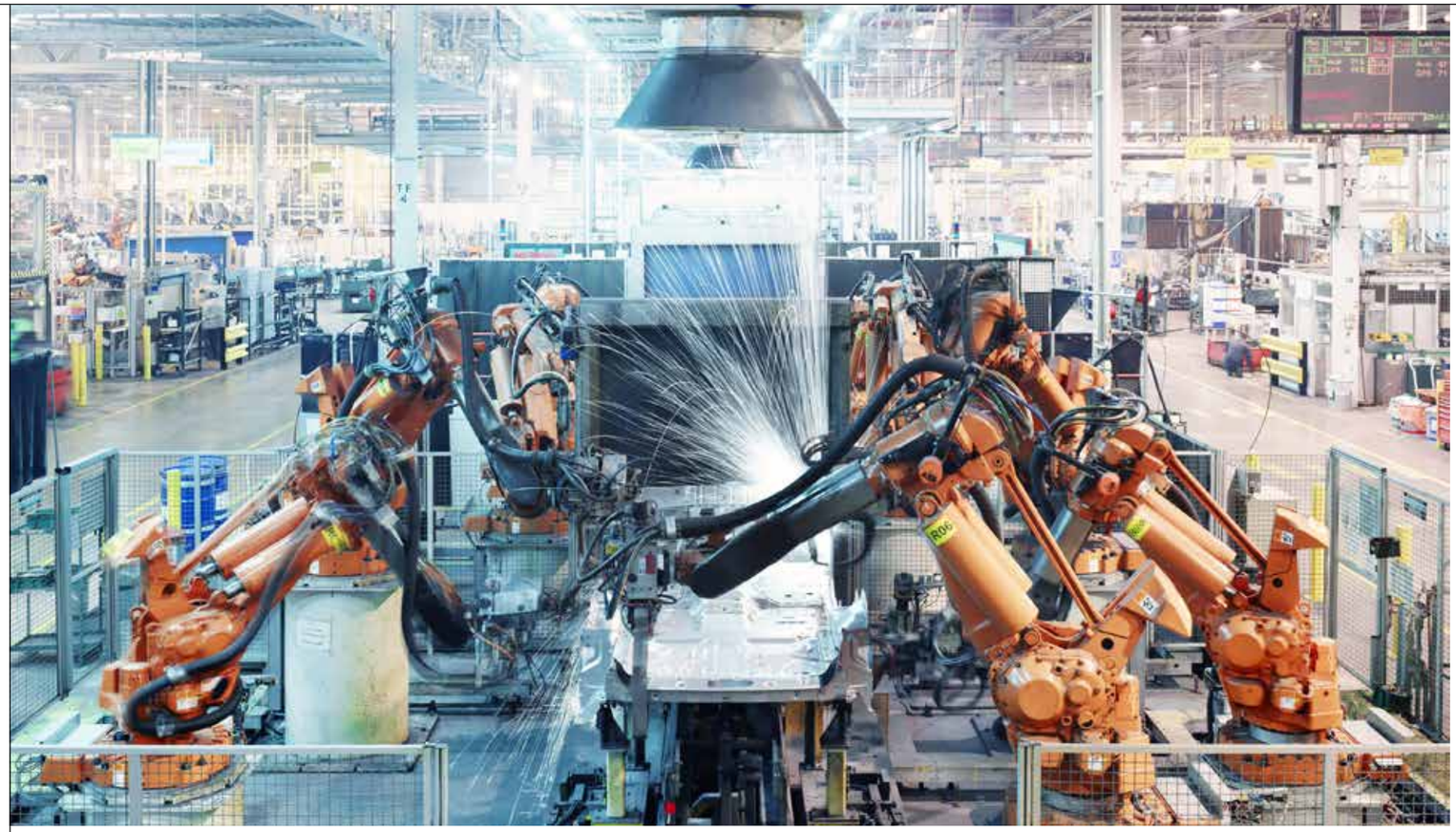

Picture credit: Land Rover MENA

BEYOND BOX-TICKING?

Dan Jones *shines a light on the government's new resilience-focused action plan responding to the rising cyber threat*

The government has published its new £210-million cyber action plan that sets out how it plans to tackle the growth in online threats. Spearheaded by a new Cyber Unit, the Government Cyber Action Plan (GCAP) is designed to: "rapidly improve cyber defences and digital resilience across government departments and the wider public sector, so people can trust that their data and services are protected".

For security leaders across the UK and internationally, GCAP represents more than a funding announcement – it signals a structural shift in how governments intend to manage cyber risk at scale.

In a letter written by Ian Murray MP, Minister of State for Digital Government and Data, to the chair of the Science, Innovation and Technology Committee, Mr Murray explained how GCAP represents a: "critical step to fix our digital foundations, whilst also tackling the specific challenges highlighted by the State of Digital Government Review and the National Audit Office". The minister acknowledged that public sector resilience had: "not kept pace" with evolving threats and that the level of risk: "remains unacceptably high", citing last year's Legal Aid Agency incident as a stark reminder of the real-world impact cyberattacks can have on essential services.

He also characterised the plan as a: "radical shift" in approach, with stronger central direction, clearer minimum standards and explicit accountability for managing cyber risk. Recent high-profile incidents have shown how quickly cyber disruption can spiral out of control, impacting more than the initial target. Jaguar Land Rover was forced to stop production following a cyberattack on a key supplier, having knock-on effects that impacted it's supply chain and workforce

Jaguar Land Rover was forced to stop production following a cyberattack on a key supplier

Crucially, departments will be held to standards equivalent to those applied to Critical National Infrastructure (CNI) under the forthcoming Cyber Security and Resilience Bill (CSRB). If delivered effectively, this alignment with CNI standards could prove transformative, embedding cyber resilience as a core operational discipline rather than a compliance obligation.

GCAP is a response to the increasingly volatile and technology-dependent world in which we live, where online threats can originate from geopolitical tensions, organised gangs or simply because someone clicked on something by mistake. In its most recent annual review, the National Cyber Security Centre (NCSC) revealed that it had dealt with 204 'nationally significant' cyberattacks against the UK in the 12 months to August 2025, up from 89 in the previous year. A large number of incidents it handled were linked to what it called Advanced Persistent Threat (APT) actors, which include nation-states or highly capable criminal groups.

Dr Richard Horne, Chief Executive of the NCSC, said that cyber security is now a: "matter of business survival and national resilience," before adding: "With nearly half the incidents handled by the NCSC deemed to be nationally significant, and a 50 percent rise in highly significant attacks on last year, our collective exposure to serious impacts is growing at an alarming pace."

That "collective exposure" is highlighted in the Government's own 2025 Cyber Security Breaches Survey, which found that while most organisations have basic protections in place, more advanced practices are thin on the ground. It found that while rudimentary cyber hygiene may be widespread, formal incident response planning, supply chain risk assessment and board-level oversight are less common among small and medium-sized firms.

And it is this that GCAP is seeking to address and move organisations from tick-box compliance to real-world preparedness. That shift – from periodic assurance to continuous operational resilience – is arguably the most important element of the plan. In practical terms, that means organisations gaining real-time visibility of their assets, including endpoints, internal systems, internet-facing infrastructure, cloud environments and even forgotten or misconfigured services. As the events of recent years have told us: it doesn't matter how small the gap is, if it's out there someone will find it and exploit it.

This is why external attack surface management (EASM) is so important, especially in something as large and sprawling as the public sector. And since many organisations do not realise how much they have exposed – or how quickly that footprint changes – EASM helps them answer the question: what could a would-be attacker find if they scanned us right now?

Of course, if visibility is to be done continuously, so too must efforts to resolve problems. That means levelling up patching and configuration fixes through automation, something which should reduce the delay between detection and action. However, automation in isolation is not enough. The scale and complexity of modern government IT estates demand a move towards Autonomous IT – an operational model in which systems continuously identify risk, prioritise remediation and take corrective action with minimal human intervention.

Since it's important to assess performance, key performance indicators (KPIs) such as mean time to detect (MTTD) and mean time to respond (MTTR) need to be collected, not to sit on a shelf to gather dust, but to be used to assess performance.

GCAP could have wide-reaching benefits that extend far beyond the public sector. The UK Government buys huge amounts of technology and digital services. If it demands stronger security controls, tougher reporting rules and clearer accountability, then suppliers must meet those standards to win or keep contracts.

DESPITE ALL THE TALK ABOUT RISK MITIGATION, IT'S EASY TO FORGET THE HUMAN SIDE OF A BREACH

The ripple effect of the changes in legislation should not be overlooked. Historically, when government tightens operational standards, markets recalibrate. Suppliers innovate, security baselines rise and resilience expectations become embedded across sectors. GCAP has the potential to catalyse that same uplift effect. In 2024, for example, a ransomware attack on Synnovis – a key pathology services provider for multiple NHS trusts – disrupted diagnostic testing and patient care across parts of the health service. Those responsible published data files they had stolen in the attack, prompting Synnovis to obtain a legal injunction to prevent people from using or further publishing the data.

These incidents highlight a simple reality that supply chain weakness can become systemic. Which helps to explain why raising resilience standards inside government inevitably means scrutinising the security posture of the organisations that support it. Indeed, as part of GCAP, the Government has unveiled a new Software Security Ambassador Scheme, which it hopes will drive adoption of the Software Security Code of Practice, a voluntary project designed to reduce software supply chain attacks and disruption.

We have seen this pattern before. GDPR – the EU's data protection regulation that sets strict rules for how organisations collect, process and safeguard personal data – has now become a global benchmark for data governance. In much the same way, many people think GCAP could play a similar role in ramping up operational cyber resilience. If that proves true, the UK could help set an international benchmark for operational cyber maturity, particularly in how governments manage third-party risk at scale.

But ambition must be matched by execution. Demand for cybersecurity and resilience skills across government is growing faster than the supply of available talent. Around half of businesses and more than half of government organisations report a basic cyber skills gap, leaving services vulnerable and forcing organisations to rely on costly outsourcing. In the public sector, long-standing issues around pay, career progression and limited leadership understanding of cyber risk have contributed to under investment and uneven security practices. The good news is GCAP seeks to address this through the creation of a dedicated Government Cyber Profession, while raising awareness of cyber risk at the leadership and board level.

While the intentions behind GCAP are to be applauded, it won't be fully rolled out until at least 2029. Meanwhile, threats continue to mount up with attackers exploiting known vulnerabilities within minutes of discovering a weakness. This is precisely where Autonomous IT models become critical. By reducing manual workload and embedding continuous control enforcement, it allows scarce expertise to focus on strategic risk, threat intelligence and high-value decision-making, rather than repetitive remediation tasks.

GCAP IS A RESPONSE TO THE VOLATILE AND TECHNOLOGY-DEPENDENT WORLD WE NOW LIVE IN

AI is being used to enhance phishing and social engineering, lowering the barrier to entry for cyber criminals and increasing scale. "Actors linked to China, Russia, Iran and the DPRK are using large language models (LLMs) to evade detection, support reconnaissance, process exfiltrated data, access systems through social engineering, and support vulnerability research and exploit development (VRED)," the NCSC has warned.

"In the last 18 months, security researchers have identified new techniques that exploit AI, including fully automated spear-phishing campaigns, hijacking cloud-based LLMs, automating post-breach attack stages and data exfiltration. The most significant AI-cyber development in the near-term will highly likely come from AI-assisted VRED, enabling access to systems through the discovery and exploitation of flaws in the underlying code or configuration," it said.

If nothing else, the threat posed by AI exposes the limits of those still hanging on to outdated manual security processes. Teams cannot investigate, prioritise and remediate at the same pace that automated tools can scan and exploit.

If government systems are high-value targets and adversaries can operate at speed and scale, defence must be able to do the same. That means automating patch deployment, enforcing policy continuously and correcting configuration drift before it becomes exposed.

As the NCSC rightly says: "keeping pace with AI-cyber developments will almost certainly be critical to cyber resilience for the decade to come".

For all the talk about digital resilience, scalable digital services, operational capability and risk mitigation, it's easy to forget the human side of a breach. In an open letter accompanying the NCSC's annual review, Shirine Khoury-Haq, CEO of the Co-op Group, reflected on the impact a high-profile cyberattack had on the business and her team.

"Dear business leaders and decision makers," she wrote. "I am writing this letter as a CEO whose business has just experienced a cyberattack, in the hope that by sharing some of our experiences and learnings, you can all feel better equipped in dealing with what is a mounting issue for us all.

"While you can plan meticulously, invest in the right tools and run countless exercises, nothing truly prepares you for the moment a real cyber event unfolds. The intensity, urgency and unpredictability of a live attack is unlike anything you can rehearse. That said, those drills are invaluable; they build muscle memory, sharpen instincts and expose vulnerabilities in your systems. At Co-op, our routine investment in security, the deliberate segregation of systems and frequent testing laid a strong foundation for our response to this cyberattack," she said.

That is what GCAP is meant to address. It offers an opportunity to redesign public sector cyber operations around continuous visibility, accountable performance metrics and Autonomous IT principles. There's no more urgent moment than this. It's time to shake up internal processes and invest in the right technology and infrastructure to ensure your organisation not only survives but thrives as a part of our national resilience ●

Dan Jones is Senior Security Advisor at Tanium.

GCAP is designed to: "rapidly improve cyber defences and digital resilience across government departments and the wider public sector"

Picture credit: Rob O'Connor