nationalcrcgroup.co.uk

THE
NATIONAL CYBER INSIDER

NATIONAL CYBER RESILIENCE CENTRE GROUP

POLICE-LED, BUSINESS-FOCUSED SUPPORT FOR SMALL BUSINESSES AND THIRD SECTOR ORGANISATIONS

Convergence crisis:

Why cyber resilience must evolve as cyberattacks become more organised

By **Richard Meeus**, Director of Security Technology and Strategy for EMEA, Akamai

Last year, discussions on cyber resilience focused on closing the gap between increasing threats and existing defences. However, although this gap still exists, the nature of the threat has changed.

In the UK, the scale of the challenge is becoming increasingly apparent. The National Cyber Security Centre (NCSC) reports that it handled 204 nationally significant cyber incidents in the past year, an average of four per week, up sharply from 89 the previous year. Nearly half of these incidents could have seriously impacted essential services such as healthcare, energy, transport and local government systems, highlighting the mounting pressure on national infrastructure.

This shift is not just about scale; it is also about how attacks are designed and executed. As cybercriminals adopt more coordinated and repeatable methods, traditional, siloed security approaches are becoming less effective. The challenge is no longer just defending individual systems, but also understanding how attacks move across them, often remaining undetected until disruption occurs.

Akamai's latest State of the Internet (SOTI) Security Report, on apps, APIs, and DDoS reveals that we are facing a convergence crisis. Rather than testing one technique after another sequentially, attackers are now combining application attacks, API abuse and DDoS campaigns into coordinated, parallel operations.

From isolated threats to coordinated campaigns

Traditionally, organisations approached web application security API protection and DDoS mitigation as separate disciplines. However, the SOTI report shows that, as attackers are now using blended attacks, defences need to be more aligned.

APIs, in particular, have emerged as the primary attack surface. As organisations accelerate their digital transformation and adopt AI-driven services, APIs have become the connective tissue of modern infrastructure – and a critical point of exposure.

Recent data illustrates the scale of the issue:

- 87% of organisations have experienced security incidents related to APIs.
- The number of API attacks has more than doubled in the past year, highlighting the rapid expansion of this attack surface.
- Layer 7 DDoS attacks targeting API and web services have increased by over 100% in the last two years, which indicates a significant and rapid escalation of this threat.

These attacks now follow a defined chain involving entry through APIs, spread across applications, and culminating in DDoS-driven disruption. This reflects the industrialisation of cybercrime, which is becoming increasingly automated through AI and is therefore efficient and scalable.

Adapting to a converged threat landscape: building resilience

This shift requires a new approach to resilience across the UK's cyber ecosystem. Traditional methods that rely on distinct controls for applications, APIs and network security are inadequate. Resilience must now operate across these areas, reflecting how threats actually emerge and escalate.

1. **Unified visibility**: Modern attacks exploit gaps between systems. Organisations should implement integrated monitoring of applications, APIs and networks. This enables the early detection of API abuse and the disruption of coordinated campaigns, providing a clearer view of national cyber risk.
2. **API-first security**: APIs drive innovation and risk, particularly as AI adoption increases. Many organisations lack a complete inventory of their APIs, leaving endpoints unknown and exposed. Continuous discovery, authentication, authorisation and behavioural monitoring are therefore essential as APIs increasingly serve as entry points for attacks.
3. **Adaptive mitigation**: Industrialised attacks can escalate quickly. Mitigation must therefore operate at scale, providing automated responses, handling high volumes of traffic and offering multi-vector protection. Disruption to critical services can have an immediate societal and economic impact. As the NCSC notes, ensuring service availability is as important as preventing compromise.

A collective response to an industrialised threat

As attack methods converge, the response must evolve too. Addressing these challenges requires coordination between the government, law enforcement agencies, industry and academia. This coordination must cover everything from understanding adversary behaviour and shaping policy to delivering operational capability and advancing research. The UK's Cyber Security (Responsibility of Operators of Essential Services and Transparency) Bill, also known as the CSR Bill, reinforces this approach by placing clear duties on organisations to manage systemic risk and share relevant insights. In this context, collaboration is both strategic and essential to building a resilient national cyber ecosystem.

Building resilience for what comes next

The industrialisation of cyberattacks is not a short-term trend. It reflects a broader change in the way that adversaries operate, and this change will continue as automation and AI reduce the barriers to entry. Recent nationally significant incidents demonstrate that this shift is already impacting essential services and economic stability. Resilience must now be continuous, integrated and collaborative across applications, APIs and networks, and be supported by cross-sector partnerships.

Organisations can take practical steps today to improve their cyber security, such as securing APIs with consistent authentication and authorisation, monitoring for unusual activity and ensuring that their DDoS mitigation and incident response plans are up to date and have been tested. At the same time, traditional cyber hygiene measures should not be overlooked, as they remain fundamental to reducing exposure and strengthening the ability to detect, respond to, and recover from incidents.

Those who adapt most effectively will move beyond fragmented controls to coordinated approaches. The priority is clear: evolve alongside the threat. Strengthening coordination, improving visibility and aligning security practices across organisations is central to maintaining the security and continuity of the services on which society depends.

Inside this edition...

Groundbreaking Supply Chain Insights from the National Ambassador Programme

Most enterprise organisations accept that supply chain resilience is a primary concern when considering cyber security; however, reaching SMEs in the supply chain is more complex than many people realise.

Firstly, it's a new challenge, one that requires them to communicate with the companies in their supply chain. This may seem straightforward; however, large organisations don't typically contact their suppliers en masse, and if they did, it's unlikely the contacts they hold would be the person who handles cyber resilience.

Working with our National Ambassadors, NCRCG offers a range of solutions to help large organisations run supply chain campaigns tailored to their operating model.

In this edition of the National Cyber Insider, you can read examples of recent supply chain campaigns we've run with Nationwide (Page 4) and Sir Robert McAlpine (Page 5). You can also see examples of our bespoke, innovative approach to customer campaigns with L'Oréal (Page 5) and NatWest Group (Page 8), and how we are tackling entire sectors, as featured in our recent Care Sector outreach (Page 6).

The supply chain challenge is not caused by an unwillingness to tackle the problem; well-intentioned guidance is too general and will usually fail inside large organisations. Success is derived from understanding the challenge and adopting an agile, creative approach for each organisation. We know how to connect Security, Marketing, Legal, and HR Departments, and when we achieve this, it is the key to mobilising SME cyber resilience engagement at scale.

NCRCG has the experience, expertise and resources to bridge the gaps that currently prevent effective communication internally, and with the relevant people in SME supply chain.

National Ambassadors

Helping businesses to become more secure through the sharing of relevant information, training and guidance

The Cyber Resilience Centre Network (CRC Network) comprises nine centres across England and Wales and was set up as a collaboration among the police, government, private sector and academia to help strengthen cyber resilience across the nation's small and medium-sized enterprise (SME) community in support of the government's National Cyber Strategy.

The network is delivered by the **National Cyber Resilience Centre Group** (NCRCG), which is a not-for-profit organisation funded and supported by the Home Office, policing and private sector partners. It provides a platform to coordinate a strong defence against cybercrime and, by doing so, makes the UK a more attractive place to work in and invest in.
Through NCRCG and the CRC Network, we have a vehicle to lead the charge in strengthening our nation's cyber resilience. The model ensures law enforcement can learn from the insights and experiences of leading organisations across the UK economy, including in the public, private, and third sectors.

Our **National Ambassador** programme provides an opportunity for the UK's largest companies to collaborate with senior law enforcement officials and the government to inform national developments on cyber resilience and reduce the risk posed by cybercriminals to their supply chains, customer bases, and the wider SME community.

Integral to the national reach are nine regional Cyber Resilience Centres (CRCs), established across England and Wales and led by policing, to provide a range of fully funded, high-quality cyber resilience services to smaller organisations in their locality.

Each Centre works closely with local universities to handpick a unique and talented cadre of students who work alongside senior security practitioners and supervisors to deliver a range of cyber resilience services to SMEs and third-sector organisations. This service is delivered via our **Cyber PATH** programme, which provides funded solutions to SMEs and real-life work experience to students to encourage them to explore cyber as a rewarding career choice.

At NCRCG, we provide insight, consolidating information and analytics from across the CRC Network to enable the adoption of best practices across the country. However, each Centre retains regional leadership to ensure that national guidance and assistance gets closer to those who really need it.

Situating MSPs in the Modern Supply Chain

CyberSmart

Written by **Jamie Akhtar**, Co-Founder and CEO at CyberSmart.

Supply chain cyber risk is a defining security challenge of modern business. Research suggests that the average small and medium-sized business (SMB) in Europe has nine times more suppliers than employees, with a median of 800 suppliers. As for larger enterprises, the supply chain can be made up of thousands of organisations of varying sizes. With such complex connectivity between organisations of all sizes, it's clear that supply chain risk is no longer a theoretical concern, rather one that business leaders must deal with head on.

While we've made progress in recognising that risk is shared across ecosystems, we still haven't fully reckoned with the role of one of its most critical components: Managed Service Providers (MSPs).

The Changing Role of the MSP
MSPs have evolved far beyond their traditional remit. They are no longer just providers of IT support, instead they are embedded operators within the digital infrastructure of thousands of organisations. The 2025 CyberSmart MSP Report found that 60% of customers now expect them to manage their cyber security and IT infrastructure, which is a big responsibility. As trusted partners, they manage endpoints, control identity layers, deploy security tooling and increasingly act as outsourced security teams for time and resource strapped SMEs.

Managed compliance is becoming the next evolution of managed security. IT providers have moved from break-fix to managed services to managed security, and are now entering the era of compliance as a service.

In many cases, MSPs have a significant level of access to customer organisations. That level of access fundamentally changes the risk equation.

Attackers understand the value of targeting an MSP. Rather than targeting individual organisations, they are increasingly looking upstream as a way to achieve scale. A single compromise can cascade across an entire client base. It's efficient, repeatable and, with a sharp rise of AI-enabled attack techniques, becoming even easier to execute.

Supply chain security only works if responsibility is clearly assigned and proportionate to risk, not just broadly shared.

Regulatory Gaps and The Cyber Security and Resilience Bill
Whilst MSPs sit at the centre of the ecosystem, from a regulatory and standards perspective, they remain under-defined.

The UK's Cyber Security and Resilience Bill, however, represents a positive step forward, particularly in its recognition that cyber risk extends beyond individual organisations and into the wider supply chain. MSPs that employ at least 50 people and have a turnover exceeding €10 million will be regulated, placing approximately 1,100 MSPs within its scope (for context, the UK is home to 12,867 MSPs, according to DSIT, as of 2025). What does this mean for those MSPs?

If an MSP falls into scope, it must be registered with the Information Commissioner's Office (ICO). The MSP must have appropriate and proportionate security measures in place to mitigate risk and any incidents must be reported to the ICO.

However, it still lacks specificity when it comes to MSPs at large. They are implicitly included, but not explicitly addressed as a distinct and high-impact category. MSPs are not just another supplier. Their level of privilege, access and operational responsibility sets them apart. Treating them as part of a broad supplier base risks missing the systemic impact they can have, both positive and negative.

Shifting Expectations and Accountability
Whilst frameworks like Cyber Essentials, ISO 27001 and various best-practice guidelines are valuable, they are not designed specifically for MSPs. They don't fully account for the multi-tenant environments MSPs operate in, the scale at which they deploy changes or the downstream risk they carry on behalf of their clients.

What's emerging, therefore, is a growing case for something more tailored, like a dedicated standard or certification framework for MSPs.

Not as an additional compliance burden, but as a necessary evolution of how we manage systemic cyber risk. CyberSmart's 2025 MSP Report found that customers (or potential customers) are already scrutinising the security of MSPs they partner (or are considering partnering) with. In fact, 77% of MSP leaders globally said scrutiny of their businesses' security capabilities has increased, suggesting that MSP customers are more aware than ever of the importance of good cyber credentials in a potential partner. A dedicated framework would make this unofficial good practice and due diligence on the part of the end customer more official, shifting the burden of responsibility and accountability from end user to MSP and standardising good cyber hygiene.

A well-designed MSP framework would set a clear baseline for security controls, operational processes and incident response expectations. It would recognise the unique role MSPs play and provide a mechanism for validating that they are operating at an appropriate level of maturity.

For customers, particularly SMEs, it would bring much-needed transparency. Selecting an MSP would no longer be a leap of faith based on marketing claims, but a decision grounded in verifiable security standards. This is especially important for SMEs that don't have the time, knowledge or resources to carry out this research themselves.

For MSPs, it would help professionalise the sector further. Those already investing in robust security practices would be able to differentiate, while the broader market would be lifted through clearer expectations. If MSPs are regulated, will customers choose those that are over those that are not? Put it this way: If you had to choose from two high street banks, one that was regulated and one that was not - which would you pick? Regulation could have significant implications for the market - accelerate consolidations and a "race to the top" to meet the thresholds. Alternatively, and more likely, smaller MSPs will still voluntarily comply and demonstrate it through CAF assurance.

And for policymakers, it would offer a scalable way to strengthen national cyber resilience without placing unrealistic demands on individual businesses.

MSPs as Critical Infrastructure
We need to stop treating MSPs as an edge case in supply chain discussions and start recognising them as critical infrastructure in their own right. That means bringing them into the centre of regulatory frameworks, not leaving them implied within broader categories.

It also means acknowledging that the threat landscape is shifting faster than our governance models. 44% of MSP leaders note that emerging AI threats are the biggest threat to the MSP they work for. The unknown of these attacks raises the stakes significantly. However, MSPs have always been at the forefront of change, with a strong history of supporting customers through uncertain times. These professionals have scale and expertise unmatched by SME IT teams, and, with increasing digital complexity, they are well placed to help those organisations without security and technical skills to navigate change.

Ultimately, improving supply chain security is about recognising the industries and areas that matter most. MSPs are a critical cornerstone of many supply chains and leaving them behind when it comes to regulation poses significant security risk.

If we want to build a more resilient digital economy, we need to ensure that the organisations with the greatest reach and influence are held to the highest and most appropriate standards. Anything less leaves a gap that attackers will continue to exploit.

MSPs are often seen as the weakest link, let's make them the strongest line of defence.

Dedicated to local communities:

How Rachel Lloyd-Moseley is taking the message to SMEs in local communities

Sir Robert McALPINE

National Ambassador organisations are playing their part in assisting the CRC Network to reach SMEs, whether by reaching out to their customers or those in their supply chain; however, some are going much further to highlight the work of their regional CRCs in the communities where they work or live. They are actively encouraging and supporting employees to use their 'volunteer days' to raise awareness about cyber threats and signpost them to their local Cyber Resilience Centre.

Rachel Lloyd-Moseley, Head of Procurement - Nuclear at Sir Robert McAlpine, recently addressed local businesses at a networking event in her home town in the West Midlands. Having worked with the National Cyber Resilience Centre Group (NCRCG) to launch a supply campaign for Sir Robert McAlpine, Rachel was inspired to help local companies, charities, schools and community groups by presenting to them about the ever-increasing cyber threats facing all businesses. The evening was a resounding success, with many local companies signing up with their Cyber Resilience Centre.

Speaking about the experience, Rachel said: "I'm delighted with the engagement at the event and the genuine interest shown by all on the night. And it's not only the response from the business owners, I was approached by many people also seeking similar presentations for their community groups. Among them are a community centre, wishing to arrange Security Awareness Training for 113 volunteers, the local school and several charities.

"It is gratifying to be able to help small organisations, many of whom don't have internal resources to address cyber issues. These small business owners are time-poor and need to be focused on running their businesses. In many cases, they are not aware that their business could be a target of a cyber attack. Even those who are aware of the threats struggle to find trusted support.

The town's Mayor and the councillors attending the event expressed their gratitude to Rachel for her enlightening presentation; the Mayor also expressed his intent to share the meeting details with his counterparts in surrounding areas. So, from a small-town meeting, the word is spreading not just in Rachel's community but also in neighbouring towns and regions!

Speaking about Rachel's contribution, NCRCG's Chief Experience Officer, Joanna Goddard, said: "Rachel has demonstrated her passion for helping the business community by taking our message into local communities. We are delighted to support the work she is doing, and we're grateful for her ongoing contribution and advocacy both at a national and local level. I'm also delighted that other National Ambassador organisations have now also adopted this model to make greater impact to help smaller organisations where staff have connections."

CRC Network Summit 2026

SHAPING A SECURE DIGITAL FUTURE

The CRC Network Summit 2026 took place at The Oval in London on the 29th January. The Summit is an opportunity to bring government, law enforcement, and the private sector together to discuss and collaborate on improving the cyber resilience across our SME and third-sector communities.

A wide range of delegates, including those from the Home Office, City of London Police, NCSC, DSIT, IASME, and the Welsh Government, joined teams from the Regional CRCs, Cyber PATH and NCRCG for an insightful and engaging day of presentations, discussions and workshops.

Dan Jarvis MBE MP | Minister for Security

The Summit opened with an inspiring video message from **Dan Jarvis** MBE MP, Minister for Security, that set a positive and ambitious tone for the day. Deputy Commissioner, City of London Police, **Nik Adams** then welcomed the 140 attendees, setting out his hopes and aspirations for the day ahead. Throughout the day, the audience enjoyed and engaged with a range of speakers and discussion panels, with insightful and thought-provoking contributions from the presenters and the delegates.

The highlight of the day was the compelling keynote address by Rob Elsey, Group Chief Digital and Information Officer at Co-op. Rob delivered a talk about the Co-op's recent cyber incident, which was an enthralling, inspiring, and transparent account of the entire event. The audience was particularly interested in and impressed by the attention paid to his team's well-being, not only during the incident but also afterwards as they recovered from what was a serious and extremely challenging situation.

On completion of the day's packed schedule, the delegates enjoyed some networking time, during which they shared thoughts and inspiration and explored possible collaborations, many of which are now coming to the fore.

Rob Elsey | Group Chief Digital and Information Officer at Co-op

Tijs Broeke | Chair, NCRCG, and Chair, Police Authority Board

Nik Adams | Deputy Commissioner, City of London Police

Richard Meeus | Akamai
David Cox | Mastercard
Mandy Haeburn-Little | BRIM
Gordon Adam | Mastercard

Rachel Lloyd-Moseley | Sir Robert McAlpine
Sharren Kennedy | NatWest Group
Mandy Haeburn-Little | BRIM
Wayne Selk | GTIA
Sharon Gould | Nationwide

Cyber Resilience Centres (CRCs) across England and Wales work closely with local universities to handpick a unique and talented cadre of students, who work alongside senior cyber security practitioners and police officers to deliver high-quality, tailored and fully funded cyber resilience services to smaller organisations.

SMEs are looking to reinforce their cyber resilience but aren't always sure where to begin. So, rather than overwhelming them with advice and recommendations inappropriate to their size and resource, Cyber PATH students find and explain solutions to complex challenges in ways that are straightforward and accessible.

Students are trained and prepared to deliver any of the nine services that the Centres offer (predominantly to small businesses, charities, and other organisations).

Cyber services tailored to the needs of SMEs

SECURITY AWARENESS TRAINING
Provides employees with a basic but effective understanding of their cyber environment and the confidence to recognise and draw attention to any potential security issues. It is delivered in small, succinct modules using real-world examples.

INTERNAL VULNERABILITY ASSESSMENT
Identifies any weaknesses in your internal networks and systems, such as insecure WiFi networks and access controls, or opportunities to steal sensitive data.

EXTERNAL VULNERABILITY ASSESSMENT
Identifies any weaknesses in the way your organisation connects to the internet.

FIRST STEP WEB ASSESSMENT
An initial assessment of your website to highlight its most pressing vulnerabilities. It is considered a light-touch review in comparison to the fuller Web App Vulnerability Assessment offered.

INTERNET DISCOVERY
A comprehensive review of publicly available information about a potential or existing employee using internet search and social media tools. It is primarily focused on identifying any information that could be used by cybercriminals to target your business.

SECURITY POLICY REVIEW
An in-depth review of how your current security policy is written and implemented.

MICROSOFT 365 SERVICE
Reviews your Microsoft 365 configuration to identify any flaws and weaknesses in your organisation's set up.

WEB APP VULNERABILITY ASSESSMENT
A complete assessment of your website to highlight any vulnerabilities and their potential risk to your business.

CYBER BUSINESS CONTINUITY REVIEW
A thorough review of your business continuity plan and overall resilience to cyber attack.

Nationwide's supply chain campaign makes its mark with Chipping Norton creative agency

It's great to come across organisations that appreciate the ongoing need to make staff aware of cyber threats. Creative agency, mark-making* is one of these companies. What makes it even more encouraging is that mark-making* is already Cyber Essentials certified, but they are clearly not resting on their laurels!

Founded in 1995, the company is well-respected for its creative output, which is reflected in its impressive client portfolio, primarily, but not exclusively, in the financial sector. It is also a company with strong values and purpose, demonstrated by its B Corp status. Indeed, they are rightly proud of just how well they scored in the Overall Impact assessment with a score of 121.3, exceeding the B Corp benchmark by over 40 points, proving that they really do go the extra mile to ensure that they're using their business as a force for good.

We caught up with Russ Holt, Head of Production at mark-making*, to find out more about their recent experience of our Cyber PATH service, and we were delighted to find a link with one of our valued National Ambassadors, Nationwide, who are also one of their valued clients.

One of the reasons Nationwide is engaged in the National Ambassador programme is to derisk

their SME supply chain. Working in collaboration with NCRCG and IASME, Nationwide recently ran a campaign to encourage companies in their supply chain to become Cyber Essentials or Cyber Essentials+ certified. They were also offering funding support to their supply chain partners who wanted to explore certification. mark-making* was already Cyber Essentials certified, but that didn't deter them from taking free membership of their regional Cyber Resilience Centre, as highlighted in the Nationwide campaign. As a result, they joined the Cyber Resilience Centre for the South East.

On joining, Russ had with the Centre Director, to find out more about the services and support available to SMEs through the Centre. Russ was quick to identify a service that is crucial to all businesses, Staff Awareness Training. Regardless of their Cyber Essentials certification, Russ accepts the need to make staff aware of the ever-changing cyber-threats and scams. The training was then provided in person at the mark-making* premises, led by Savva Pistolas, and the whole team appreciated the presentation style and the real-life examples used to demonstrate the topics.

Speaking about the Cyber PATH training experience, Russ Holt said: "The training was highly beneficial to all of the team; indeed, it was a real awakening to hear some of the facts and examples of the threats faced by SMEs daily.

"Even though we are Cyber Essentials certified, Nationwide's campaign prompted us to join the Cyber Resilience Centre for the South East, because they can offer ongoing guidance, support and relevant up-to-date threat intel.

"It also made perfect sense to us that cyber security is everyone's responsibility. Therefore, we have a duty to ensure that all of the team knows the threats. So, opting to accept the Staff Awareness Training offered by Patrick at the South East CRC was an easy decision.

"All in all, it was a very worthwhile exercise, and we will certainly be looking at some of the other Cyber PATH services to bolster our cyber resilience in the future."

Patrick Milford, CRC Network Lead, also commented: "It's great to see companies adopt a continuous learning approach to cyber. mark-making* sets an excellent example for others; even though they already have Cyber Essentials certification, they appreciate the need to continually inform and make their staff aware of the threats.

"It's also great to see that Nationwide's national supply chain campaign is working and, as a result, SMEs are becoming more resilient."

Sir Robert McAlpine: Leading the way in securing construction supply chains

Sir Robert McAlpine recognises the challenges faced by all businesses in today's online world, none more so than among the SMEs in our supply chain that we depend on daily. That's why we chose to join the National Cyber Resilience Centre Group (NCRCG) as National Ambassadors. Our collaboration with NCRCG enables us to protect our supply chain more effectively, making our business more resilient in the process.

We appreciate that SMEs are particularly at risk, not because of any shortcomings on their part, but instead because they are traditionally time-poor and lack the in-house cyber security expertise that larger organisations have in place today. With this in mind, we are striving to support our supply chain by highlighting that guidance is available. NCRCG supports the nine regional Centres (CRCs) which are operated by police with funded help for small organisations. The CRC Network is designed to support SMEs with helpful guidance, staff training, and other valuable services tailored to smaller organisations.

As a National Ambassador for NCRCG, we have developed campaigns to encourage our supply chain to join a regional Centre and embark on their journey towards improved cyber resilience. The campaigns are designed to make the sign-up process as simple as possible for SMEs. Once they have joined a Centre, business owners can speak one-to-one with policing at their regional CRC. Sir Robert McAlpine is confident that they are receiving trusted support from a government-backed, police-led initiative.

So far, we have seen an exceptional uptake among our supply chain, with many businesses throughout the country signing up to their local CRC. The feedback from those companies has also been highly positive, with many expressing their appreciation for the introduction, the ease with which they can engage, and the support they are receiving from their CRC. Not only have many started to benefit from better awareness of cyber threats, but they have also received valuable Staff Awareness Training and regular recommendations and guidance, specially created by the NCSC for SMEs.

Sir Robert McAlpine's commitment to cyber resilience extends beyond supporting the construction supply chain; we are equally keen to support all SMEs in the communities where we operate. For this reason, we are using the campaign structure to enable local businesses of all types to join their local CRC. Staff at Sir Robert McAlpine are using Volunteer Days to take the message into the community by addressing local business networking and community groups and signposting them to our specially created CRC sign-up page, which directs businesses to their nearest participating centre.

Andy Black, Chief Digital & Technology Officer at Sir Robert McAlpine, commenting on the National Ambassador programme, said:

"We are delighted to be working closely with NCRCG to assist us in protecting our suppliers. Cyber threats are one of the biggest challenges facing our sector, and many others, and we appreciate the need to support small and medium-sized businesses that don't have the internal resources larger companies have. We fully accept that we are only as strong as our weakest link, so it's crucial that we do what we can to help them become more resilient.

"Working with NCRCG has simplified the task for us. They are a police-led, government-funded organisation with the tools and infrastructure to enable us to support our supply chain. We trust the guidance and one-to-one support they offer, and we are delighted to have their help in reaching our suppliers."

Rachel Lloyd-Moseley, Head of Procurement - Nuclear at Sir Robert McAlpine, added:

"The support we have received from NCRCG has been impactful and instrumental in raising awareness among those in our supply chain. They have provided a solution that gives us great confidence that we are directing our suppliers to guidance that they can trust, and that will better protect them against the increasing number of cyber threats.

"The NCRCG and CRC Network are not only helping our suppliers, but they also enable us to offer the same protection to all businesses in the communities where we work. Cyber threats affect everyone today. At Sir Robert McAlpine, we have a duty to do what we can to assist those we work with, and our fellow construction companies, and NCRCG are helping us daily to assist SMEs throughout the country."

AN OFFER FROM SIR ROBERT McALPINE

As part of their commitment to securing SMEs, Sir Robert McAlpine is happy to share their dedicated supply chain campaign landing page to make it easy for any organisation to sign up for free membership with the nearest participating Cyber Resilience Centre. Simply scan the QR Code below, complete the short form and you will be redirected to the relevant CRC depending on your postcode.

SCAN NOW

L'Oréal highlights the beauty of a bespoke approach

National Ambassador, L'Oréal is keen to see SMEs in its supply chain and customer base become more resilient, and NCRCG has been working with their Northern Europe CISO and his team to determine the best way to reach its target audiences.

He was quick to recognise that reaching their salon customers would require the assistance of their marketing and communications teams, and he was grateful for NCRCG to collaborate directly with them to explore workable solutions to raise awareness among the thousands of salon customers in the UK.

Traditional National Ambassador campaigns have been via email promotions directing SMEs to a landing page that redirects them to their nearest participating regional CRC. However, it was felt that there were better, more impactful ways to reach this particular audience.

The vast majority of salons are owner managed, open extended hours, at least six days per week. Many use social media platforms extensively to promote their businesses and take bookings. So, email driven campaigns didn't seem to be the best approach.

NCRCG hosted several exploratory meetings with the L'Oréal marketing teams to fully understand their business and how they traditionally interact with their customers. Indeed, as a leading brand, they provide extensive support for their salons, including their learning platform, where they regularly create video training and knowledge-sharing content specifically designed for their salon customers.

This is a hugely engaged platform used by their customer salons. NCRCG recommended that a more effective and impactful way to reach these business owners would be through video masterclasses delivered via the established highly popular learning platform.

We presented the findings and proposed solutions of our research to the marketing teams, those who look after customer comms as well as corporate comms, which included sanctions by legal teams, as well as for technical content with the CISO team. All teams were impressed with the depth of our expertise in navigating and liaising internally in enterprise organisations, research, and the knowledge we had acquired through meticulous investigation. All agreed that the customer campaigns should be delivered via the learning platform.

From there, we have worked with Cyber PATH's Talent Manager, Sophie Powell, and former Cyber PATH student also current team member at East CRC, Sapphire Little, to develop bespoke masterclass content tailored to salon owners.

The presentations were recorded in-house and presented to L'Oréal for content approval. Then, we commissioned a professional video production company to create the final masterclass videos in line with L'Oréal's branding and video style, and presented by Cyber PATH.

NCRCG will also work with L'Oréal's business relationship managers to brief them on the many benefits of joining a regional police Cyber Resilience Centre and make them aware of the content that is available on the learning platform before this is launched to the customer salons.

We believe we have identified a solution that integrates well with L'Oréal's customer engagement approach and clearly demonstrates NCRCG's willingness to collaborate with each National Ambassador to deliver a bespoke solution. We know there is no one-size-fits-all answer, so we strive to identify the best way to reach your audience and have the expertise to do so.

We are also working with L'Oréal's procurement team to identify how we can assist them in making their supply chain more cyber resilient. Again, we will explore how they work and communicate with their suppliers, and we will develop solutions that match their operations.

Our collaboration with L'Oréal so far has involved meetings across several countries and has included input from communication, marketing, cyber and legal teams. It is a testament to the L'Oréal brand that it places such significant importance on cyber resilience, and trust NCRCG to deliver campaigns for both its suppliers and its customers. It also highlights the beauty of being flexible and offering bespoke solutions that meet the precise needs of the business.

THE CYBER RESILIENCE CENTRE NETWORK

Strengthening our national resilience

Each of the nine Cyber Resilience Centres (CRCs) works closely with its local universities to handpick a unique and talented cadre of students who work alongside senior cyber security practitioners and police officers to deliver high-quality and tailored cyber resilience services to smaller organisations.

Cybercrime is fluid; it keeps changing and advancing as technology evolves. That is why we are bringing in the brightest and the best young people from academia to develop a second-to-none talent pipeline both for policing and the private sector.

The CRC Network have a platform to lead the charge to strengthen our national cyber resilience and ultimately benefit the UK economy, protect our national assets, and make the UK a more attractive place to work in, invest in and deal with.

We know our nation's smaller organisations are looking to reinforce their cyber resilience but aren't always sure where to begin.

So, rather than overwhelming them with advice and recommendations inappropriate to their size and resource, our students are finding and explaining solutions to complex challenges in ways that are straightforward and accessible.

In doing so, they are developing their understanding of how smaller organisations operate, the pressures they face and what is required to build cyber resilience against threats specific to their locality. At the same time, each student is gaining the essential skills, knowledge, and on-the-job training they need to succeed in the workplace.

Manufacturing business almost had to throw in the towel

THE CYBER RESILIENCE CENTRE FOR WALES

The Cyber Resilience Centre for Wales has been working with a company to prevent a recurrence of a near-catastrophic event. A medium-sized manufacturing company operating under a hybrid working model experienced a significant cyber incident that severely impacted both its IT infrastructure and production capability.

An employee working from home on a company laptop wanted to live-stream a boxing match; unfortunately, he did so on his work device. When setting up in preparation for the fight, he was instructed to download specific software via the link provided to him to join the broadcast. After following the instructions, he was able to enjoy the bout.

Unfortunately, when he returned to his office and connected to the company network, malware was installed on the system. The result was far-reaching. There was a loss of critical data, including production schedules, order information and client records.

Furthermore, they experienced significant operational downtime due to infected computers and manufacturing equipment; 80% of the system had to be taken offline, halting production because it could not communicate with automated machinery.

Beyond the operational impact, the incident resulted in significant financial and reputational damage because of lost production and delays in customer fulfilment.

With guidance from the Cyber Resilience Centre for Wales, the business identified several key actions to prevent a recurrence:

Staff Cyber Awareness Training: Regular training sessions to help employees recognise unsafe websites, phishing attempts, and the dangers of streaming or downloading unverified content.

Anti-Malware and Endpoint Protection:
Deployment of robust anti-malware and endpoint detection solutions to monitor and automatically block malicious activity.

Network Segmentation:
Separating the operational technology (OT) network from the IT environment to prevent malware from spreading between production systems and office devices.

Device Monitoring and Access Control:
Implementing mandatory security scans for all devices before connecting to internal systems.

Engagement with the Wales CRC:
Ongoing collaboration with the Centre to conduct cyber health checks, review internal policies, and promote improved cyber hygiene practices.

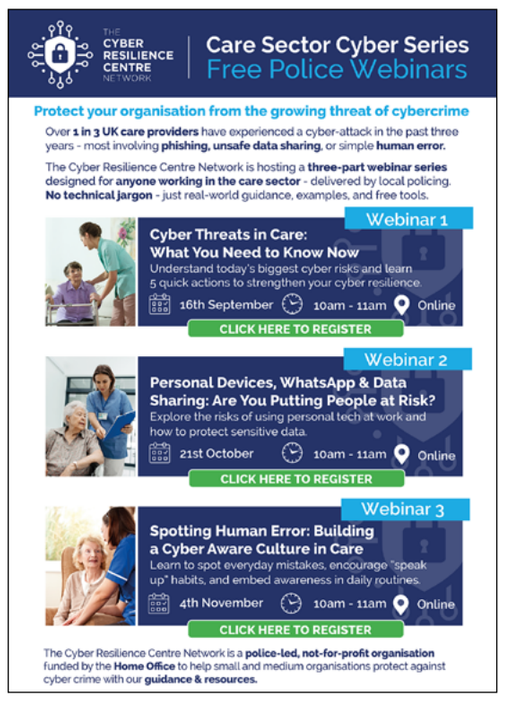
Unfortunately, the incident occurred before engagement with the CRC. Still, it highlights the critical need to make staff aware of the risks and fully understand the vulnerabilities in your operation. Membership of a CRC would have signposted the company to Cyber PATH Security Awareness Training, Vulnerability Assessments and Policy Assessments. Fortunately, it wasn't a knockout blow, and, with the CRC's help, the company is recovering from the incident.

Reaching SMEs, sector by sector: Care Sector focus

We recently piloted a sector-specific approach. Our initial activity was to target the Care Sector with a series of specially prepared webinars offering relevant guidance for organisations in the sector.

The CRC for the East worked with us utilising a team member's OSINT skills to support the research and its delivery.

Supported by Paul Lopez, Director at The Cyber Resilience Centre for the East, Sapphire Little has coordinated the campaign with considerable success. The three-webinar series received **1634** registrations, resulting in **1257** new members in the care sector joining a regional CRC.



Care England promoted the webinars internally, and while they were successful and extremely well received, they were not as well attended as the original series run by the CRC Network.

CARE ENGLAND
The voice of care

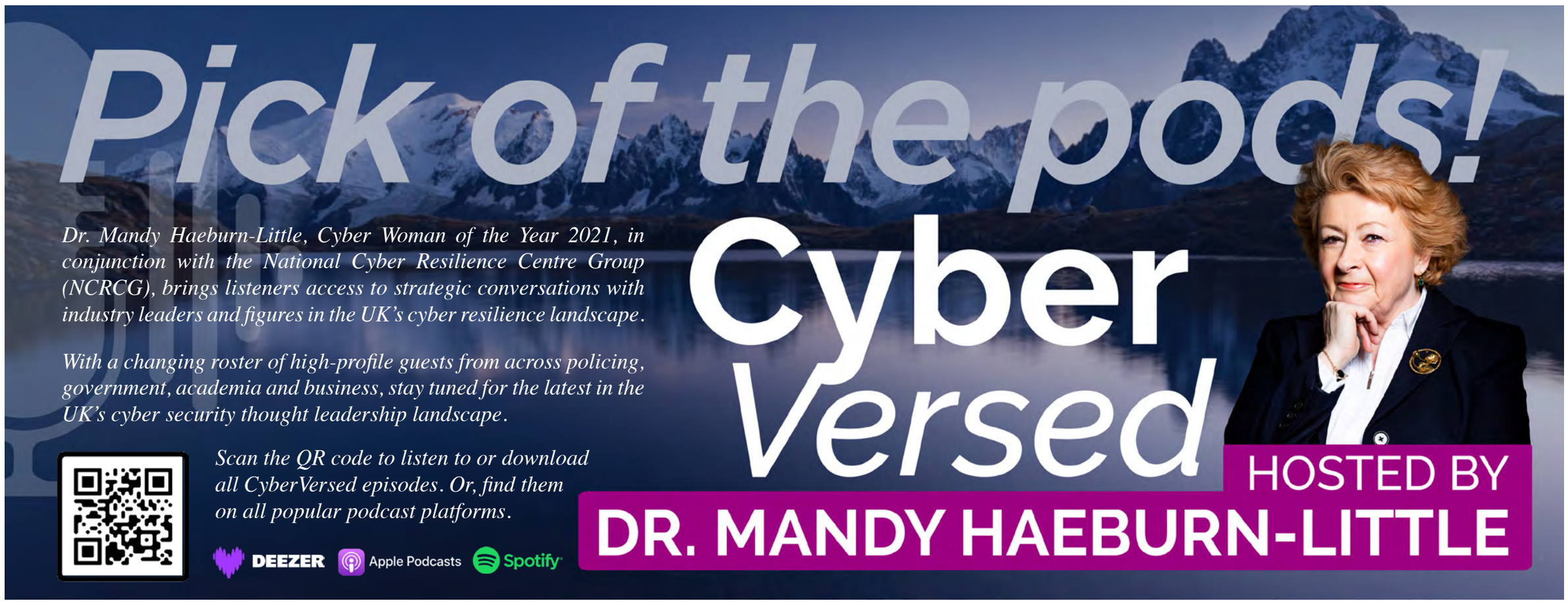
Following a review of the exercise with Care England, we were invited to run another series of webinars for The Care Provider Alliance in association with Care England.
The Care Provider Alliance (CPA) brings together the ten main national associations representing independent and voluntary adult social care providers in England. They represent the entire sector, providing a coordinated response to the major issues affecting it.

The Care Provider ALLIANCE

This time, we were invited to promote the event through the CRC Network's outreach channels, using the same process we deployed for the CRC Network Cyber Series. These webinars took place during late February and early march. Once again, the uptake in businesses in the Care Sector was exceptional.

We know that the process works well, so we have recently developed a CRC Network Sector-Specific Campaign Guide. The step-by-step document outlines the process and provides clear guidance to enable NCRCG to replicate the planning, promotion and delivery of future campaigns in other sectors in collaboration with other CRCs. We are currently reviewing priority sectors and we will launch similar campaigns either through the CRC Network or in collaboration with relevant governing bodies.

THE CYBER RESILIENCE CENTRE FOR THE EAST



Topics discussed include:

- The inspiration and purpose of the West Midlands Cyber Hub
- Why the Hub is an important addition to the entire cyber ecosystem in the region
- How it is becoming a place for collaboration and innovation
- Millennium Point and what makes it the ideal locaction for the Hub
- How the Hub is already proving to be a benefit to the Cyber PATH students
- The future goal to champion Women in Cyber and Neurodiversity in Cyber
- The focus on engaging young people with the Hub

Duration: 25 mins

Topics discussed include:

- Nik's ambitions for the CRC Network
- What his role feels like as the first Deputy Commissioner to have Cyber and Fraud within his remit
- The commitment shown by the National Ambassadors
- The Annual CRC Network Summit in London
- Rob Elsey Chief Digital Information Officer at the Co-op's presentation
- Police Reform
- The new police headquarters and how they aim to integrate policing with the private sector

Duration: 33 mins

Topics discussed include:

- The current threats in Cyber and Fraud, and how the two are converging
- How Chainalysis is using blockchain intelligence to move from a reactive to a more proactive approach
- How blockchain data is helping increase connectivity among partners worldwide
- Explanation of what blockchain is and how it operates
- Popular cryptocurrencies and how they have changed in recent times
- Money laundering techniques
- The increasing sophistication of law enforcement and the courts
- Duration: 38 mins

Topics discussed include:

- Why the CRCs and MSPs are better equipped to help SMEs when they work together
- Patrick's new role and how it assists enabling the CRC Network to support the SME community at scale
- Why strengthening MSP relationships is a primary focus for the entire CRC Network
- The importance of trust
- The National Engagement Strategy
- Why SMEs must enquire about an MSP's processes

Duration: 32 mins

Topics discussed include:

- Nick's background and how he arrived at Police CyberAlarm
- An overview of the new Police CyberAlarm offering
- Working with third-party organisations to raise awareness
- Law enforcement can build an accurate picture of the current and ever-changing threat landscape, enabling them to issue targeted alerts to specific businesses about threats that may affect them
- Examples of how Police CyberAlarm has assisted a range of organisations

Duration: 19 mins

Securing the Future:

Why Closing Cyber's Mid-Career Exodus is a Security Imperative

Spokesperson: **Natalie Billingham**, EMEA Managing Director and SVP of Sales, Akamai Technologies

Securing the Future: Why Closing Cyber's Mid-Career Exodus is a Security Imperative

The cybersecurity industry is facing a hidden crisis. We are losing highly skilled women at a time when their expertise is needed most. This mid-career exodus drains talent and actively weakens our collective ability to defend the digital world.

As we gather at CyberUK 2026, the focus is often on innovation and resilience. However, in an increasingly complex digital landscape, our ability to keep pace depends not only on technical advances, but also on the individuals who shape our defence strategies. Effectively tackling today's cybersecurity challenges requires teams and leaders who are as diverse as the threats they face.

Last year, we emphasised the importance of creating space for more voices in cybersecurity. This year, our latest research, "The Mid-Career Exodus", published by Akamai's FLAME initiative, reveals a troubling truth: although we excel at attracting women to the field, retaining them is a significant challenge. This issue represents more than just a talent pipeline problem; it poses a tangible security vulnerability.

The UK's cybersecurity workforce remains uneven. According to the UK government's Cybersecurity Skills Study, women make up just 17% of cybersecurity professionals, and almost half of organisations report skills shortages. Our FLAME research reveals a significant talent drain: 87% of women leave the tech sector altogether within ten years, often at mid to senior level. In doing so, they take their invaluable expertise with them.

We surveyed 192 women specialising in cybersecurity, and the findings are striking. Women are drawn to the mission. In fact, 75% find it satisfying to tackle meaningful security challenges, and 80% value access to continuous learning and professional certifications. However, despite this engagement, many struggle with the irregular and stressful nature of cybersecurity work, which often leads to mid-career exits.

Key factors include:

- **Disruption to work-life balance**: 40% of respondents cited security incidents and on-call requirements as influencing factors in their decision to leave or consider leaving.
- **Isolation and stress**: 31% reported stress from constant threat monitoring and 28% felt isolated as women in a male-dominated field.
- **Leadership gap**: 35% of respondents cited a lack of female role models in senior security positions.

These insights reinforce the idea that retention is not just about recruitment, but also about fostering an environment in which women can flourish throughout their careers.

As Zoe Mackenzie, President of WiCyS UK & Ireland Affiliate, noted in the report: "We lose women from cybersecurity at the exact moment their expertise becomes most valuable. This isn't a pipeline problem; it's a leadership one".

The good news is that the door is not closed. Nearly four in ten women who have left the tech industry would consider returning under the right conditions. The solutions are practical and measurable and often focus on structural changes rather than individual interventions.

In the cybersecurity sector, this means addressing the operational challenges that affect women in the field.

- **Flexible work and pay**: Implement genuine flexibility in how, when and where work is done, coupled with competitive pay and clear career progression pathways.
- **Inclusive Leadership**: Promote visible female leadership and cultivate a culture that values recognition for prevention as well as response.

By establishing mentoring programmes, collaborative learning initiatives and talent retention frameworks, organisations can play a pivotal role in implementing these changes in partnership with industry leaders. Together, we can ensure that women are able to enter the field of cybersecurity, thrive in it, take on leadership roles and shape its future.

Losing skilled women from cybersecurity undermines our collective ability to protect the digital world. The mid-career exodus is not inevitable; it is a consequence of the choices made by companies and leaders. By committing to tangible organisational changes, we can reverse this trend and build a cybersecurity industry in which women not only enter, but also remain and take on leadership roles, thereby strengthening our collective defence.

Collaborative Defence in Practice:

How CGI's NCRCG National Ambassador Role Supports the CYBERUK 2026 Agenda

As CYBERUK 2026 brings the UK's cyber community to Glasgow, CGI's work with the National Cyber Resilience Centre Group (NCRCG) shows why the next phase of cyber defence will be won through trusted partnerships, practical action and shared responsibility.

As CYBERUK 2026 opens, it does so at a time when UK's cyber debate moves beyond awareness to execution. Hosted by the NCSC with the theme, 'The next decade: Accelerating our cyber defence', this event brings together leaders and technical professionals from government, industry and academia. In that context, CGI's role as a founding National Ambassador to the NCRCG is especially relevant because it shows what collaborative defence looks like in practice, not just in principle.

That distinction matters. The UK's cyber challenge is no longer simply to understand threats; it is to organise faster, broader and more coordinated responses across supply chains, public services and critical infrastructure. CYBERUK 2026's four core tracks - Resilience, Technology, Threat and Ecosystem - all point to the same conclusion: effective cyber defence now depends on trusted relationships, shared intelligence and the ability to turn insight into action at pace.

"Collaboration is no longer optional—it's the core of cyber defence," said Alex Woodward, Senior VP at CGI Cyber Practice, ahead of the conference. "Our role across our alliances such as NCRCG and others, is to embed real-world insights from complex sectors such as energy, government, and financial services into a shared resilience framework aligned with the CyberUK agenda."

The NCRCG is a not-for-profit partnership linking policing, government, business, and academia to improve cyber resilience for UK SMEs. Through nine regional centres in England and Wales, it provides practical, fully funded support to smaller organisations and their supply chains, helping strengthen national resilience.

CGI's Ambassador role gives it a practical way to contribute to that national effort. As a founding Ambassador, CGI works alongside law enforcement, government and fellow Ambassador organisations to share insight, inform resilience initiatives and help reduce cyber risk across supply chains and customer bases. That fits naturally with CGI's wider cyber practice in the UK, where experience across regulated industries, critical national infrastructure and government can help inform the broader resilience conversation.

The Ambassador role creates a route for lessons learned in operational environments to flow back into the wider ecosystem. Maxine Bulmer, Cybersecurity Director Consulting Delivery, CGI's National Ambassador for the NCRCG, has been closely involved in that engagement, helping connect industry expertise with NCRCG programmes and conversations across the community. The value lies in the exchange: organisations do not simply contribute advice, they help shape a more consistent and practical national voice on cyber resilience.

That is why this partnership speaks directly to the CYBERUK 2026 agenda. The conference theme is about acceleration, but acceleration in cyber defence does not come from technology alone. It comes from shortening the distance between policy and delivery, between national guidance and local adoption, and between individual organisational experience and collective preparedness. NCRCG's network - and CGI's role within it - helps close those gaps.

For business and public sector leaders alike, that has a practical implication. Resilience can no longer stop at the edge of a single organisation; it has to extend into suppliers, partners and regional economies. Large enterprises are only as resilient as the smaller organisations they depend on, which is why NCRCG's regional model - amplified by Ambassador organisations such as CGI - offers something genuinely useful: a way to connect national priorities with local adoption at scale.

The strongest outcome from CYBERUK 2026 will not be another statement of intent. It will include examples of organisations working together in ways that measurably improve resilience across the UK economy. CGI's partnership with the NCRCG is credible because it is rooted in that kind of practical contribution: supporting SMEs, strengthening supply chains, developing future talent and creating stronger links between industry, policing and government. In a threat environment that rewards speed, trust and coordination, that is not just aligned with the CYBERUK agenda - it is what the next decade of cyber defence should look like.

Written by **Kunle Anjorin**, Director of Cybersecurity within CGI UK's Cyber Practice. He leads the delivery within the Energy, Utilities, Media and Telecoms sector.

Building Cyber Resilience at Scale:

How GTIA and the NCRCG Are Supporting the UK's Cyber Security and Resilience Act

Wayne Selk is Vice President, Head of Cybersecurity Programs at Global Technology Industry Association (GTIA).

As cyber threats continue to grow in frequency, sophistication, and economic impact, small and medium enterprises (SMEs) and small micro organisations (SMOs) across the UK remain disproportionately at risk. Limited resources, lack of specialist expertise, and growing regulatory pressure combine to create a challenging environment, one that the UK's forthcoming Cyber Security and Resilience Bill is designed to address. The challenge now lies in helping businesses not only understand the Act, but also build practical, sustainable cyber resilience in line with its intent.

The Problem: Risk Without Readiness

While large enterprises often have dedicated security teams and compliance frameworks, SMEs and SMOs depend heavily on managed service providers (MSPs) and IT service providers (ITSPs) to secure their environments. This creates a cascading risk scenario: if an ITSP lacks mature cyber security controls, those gaps are effectively inherited by dozens, or hundreds, of downstream clients. At the same time, many small businesses continue to see cyber security as a technical issue rather than a core business risk, resulting in underinvestment and low engagement until an incident occurs.

The Cyber Security and Resilience Bill seeks to raise the baseline, but legislation alone cannot create resilience. What is needed is coordinated education, practical guidance, and trusted frameworks that translate policy objectives into day-to-day operational improvements, particularly for businesses that do not know where to start.

A Collaborative Response: GTIA and the NCRCG

To bridge this gap, the Global Technology Industry Association (GTIA), acting in its role as an Ambassador to the National Cyber Resilience Center Group (NCRCG), is working closely with regional Cyber Resilience Centers (CRCs) across the UK to develop a national strategy aimed squarely at SMEs, SMOs, and the ITSPs that support them.

GTIA's approach recognizes that cyber resilience must be built at multiple levels simultaneously. On one track, the focus is on empowering small businesses to better understand cyber risk in the context of their own operations, revenue, and reputation. On another, equal emphasis is placed on strengthening the cyber security posture of IT service providers themselves, ensuring they do not unintentionally become risk multipliers within the digital supply chain.

What the Solution Looks Like

Central to this strategy is an education-led model delivered through the UK's regional Cyber Resilience Centers. Since the beginning of 2026, SMEs and SMOs are now be able to access structured cyber security training through their local CRC, designed to align cyber security principles with real-world business risk. The goal is not compliance theatre, but informed decision making, helping organisations understand what protections matter most and why.

Complementing this, GTIA is working with its UK ITSP members to raise the security baseline within the managed services community itself. This effort is anchored by the GTIA Cybersecurity Trustmark, a framework that goes beyond Cyber Essentials and Cyber Essentials Plus by establishing a foundational security program at the ITSP level. Rather than pushing risk downstream to clients, ITSPs adopting the Trustmark are expected to manage and mitigate risk within their own operating environment first.

This dual-track approach, educating end customers while professionalising service providers, creates a reinforcing cycle of resilience across the ecosystem.

How Other ITSPs Can Benefit

For IT service providers, engagement with GTIA and the CRC Network offers more than regulatory alignment. The Cybersecurity Trustmark provides a structured path to operational maturity that can be tailored across different industry verticals, each with its own compliance and risk profile. This is particularly valuable for MSPs serving healthcare, finance, and regulated professional services, where client expectations are rapidly increasing.

Global Technology Industry Association

Participation also enhances trust. As customers become more security-aware under the Cyber Security and Resilience Bill, ITSPs able to demonstrate adherence to a recognised, industry-led framework will be better positioned to differentiate themselves in a crowded market.

What's Next

Looking ahead, the strategy developed by GTIA and the NCRCG is designed to scale. As CRC-delivered training rolls out across regions, lessons learned will inform continuous improvement in both educational content and ITSP security practices. Over time, this creates a feedback loop where regulatory intent, industry capability, and small-business resilience reinforce one another.

The Impact on UK Businesses

The long-term impact of this collaboration is significant. For SMEs and SMOs, it means access to trusted, local resources that demystify cyber security and make the Cyber Security and Resilience Bill achievable rather than intimidating. For ITSPs, it means clearer expectations, stronger operational foundations, and reduced systemic risk. And for the UK economy as a whole, it means a more resilient small-business sector aligned with the objectives of the Cyber Security and Resilience Bill, strengthening security not just through rules, but through education, trust, and shared responsibility.

NatWest Group adopt a highly targeted approach

NatWest Group recognised that for their customer campaigns, a highly targeted approach would work best, so we created separate landing pages for each identifiable business category. This approach enables us to craft specific messages and graphics relevant to the intended audience.

The first campaign has been launched to 1500+ charity sector organisations that are NatWest Group customers; other campaigns will follow soon.

NatWest Group use a variety of methods to promote the campaign, including email with PDF attachments. However, we know from experience that these campaigns require additional signposting and promotion. We identified that relationship managers and other customer-facing personnel should receive bespoke CRC briefings to ensure they are confident when talking to customers about the campaign's value and joining a CRC.

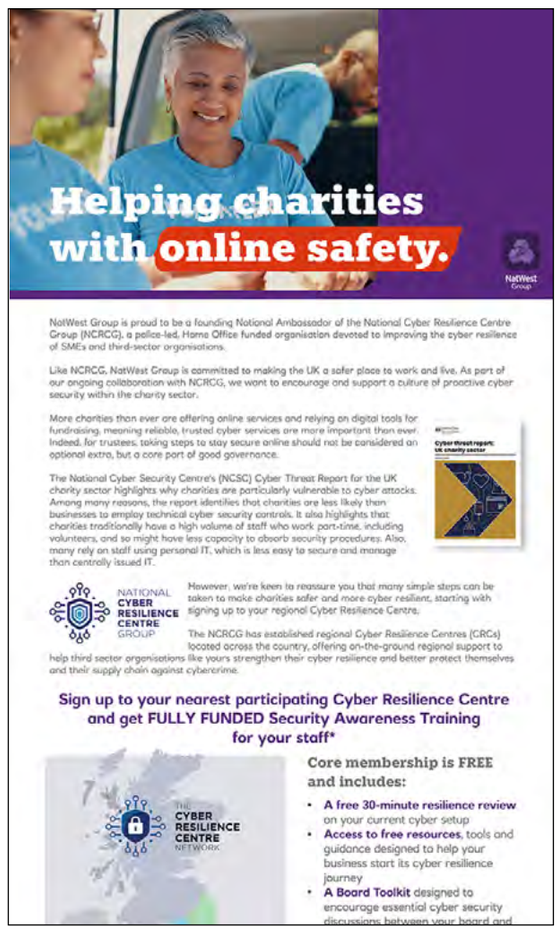
NCRCG organised a series of briefing events delivered online by police officers working in the regional CRCs. The staff briefing was a significant undertaking, but one we believe is extremely worthwhile because these people have day-to-day relationships with business customers. We have begun with the objective of reaching 10,000 managers. The spin-off benefit is that they are better equipped to communicate with all their customers across all sectors.

Directing respondents to a dedicated landing page enables us to track the campaign and report on the outcomes. Doing this helps us to refine future campaigns, but more importantly, it allows us to provide evidence of behavioural change among the SME community.

We will report the open and click-through rates for each landing page, as well as the number of organisations that signed up as a result of each campaign. We can also segment the data to show how many have signed up with each CRC.

Following on from the launch of the Charities campaign, NatWest Group is now working with NCRCG to initiate new campaigns. The first of these is highly focused and will target legal firms, specifically conveyancers. The intention is to follow a similar model, in which we brief staff and provide any support materials to help them reach the intended audience.

We are also working with NatWest Group to create and launch supply chain campaigns that will roll out soon.



AI, segmentation and the next phase of Zero Trust

Spokesperson: **Mike Havelock**, Regional Sales Manager EMEA at Akamai Technologies

The rapid adoption of artificial intelligence and the growing complexity of modern IT environments are transforming cyber resilience. For organisations in government, law enforcement, academia, and critical industries, this shift is redefining the practical requirements of Zero Trust.

A recent IDC InfoBrief titled 'Achieving Cyber Assessment Framework (CAF) Outcomes in the UK Public Sector' highlights these changes. It reveals an increased focus on AI-related risks, such as prompt injection, data exfiltration, and the misuse of AI-enabled services. At the same time, it emphasises the need for greater visibility, continuous monitoring and more proactive threat detection.

The CAF offers a structured approach to cyber resilience, focusing on outcomes such as threat intelligence, managing AI cyber risks, secure software development, security monitoring and threat hunting. Many organisations struggle not with understanding these priorities, but with implementing them effectively across distributed and interdependent environments.

This is an area in which Zero Trust must evolve. Traditional approaches, which tend to focus on identity and perimeter control, are no longer sufficient on their own. As IDC research makes clear, resilience depends on the ability to detect, contain and respond to threats within an environment, not just at its boundaries.

Segmentation is central to this shift. By dividing networks into granular zones and enforcing strict access controls between them, organisations can limit lateral movement and reduce the impact of a breach. This is particularly important in hybrid infrastructures, where users, applications and data are spread across on-premises systems, cloud platforms and third-party services.

However, scaling segmentation introduces its own challenges. Static policies and manual processes struggle to keep pace with dynamic workloads and rapidly evolving threats. Consequently, organisations are adopting AI-driven solutions to automate asset discovery, map system dependencies and detect anomalous behaviour in real time.

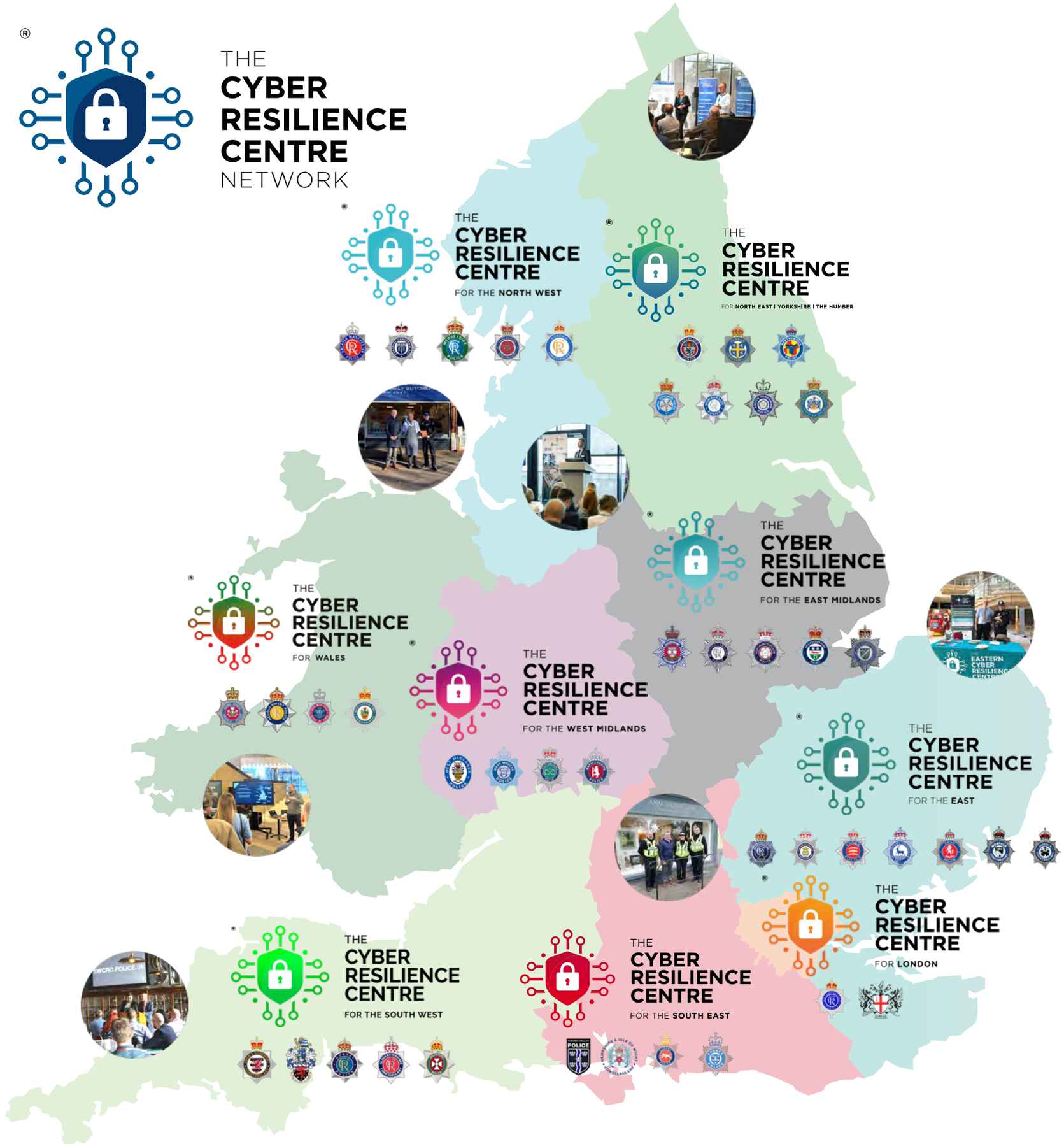
This direction closely aligns with the priorities set out in the IDC InfoBrief. Both strengthening threat intelligence and managing AI-related risks rely on in-depth insight into how systems and data interact. Similarly, effective security monitoring and threat hunting depend on the ability to observe and analyse activity across the entire environment rather than just a limited number of control points.

The growing use of AI also introduces new attack surfaces. APIs, machine learning models and AI-driven services can all be exploited if they are not properly understood and secured. Therefore, capabilities such as API discovery, AI-aware traffic inspection and DNS-layer controls are becoming essential as part of a broader, integrated security strategy, rather than as standalone measures.

These developments are particularly relevant for organisations within the Cyber Resilience Centre network. Many of these organisations operate across complex ecosystems that combine legacy infrastructure, cloud-native applications and extensive partner connections. In such environments, resilience depends on visibility and control: understanding what is happening across the network and responding quickly when risks emerge.

The direction of travel is clear. Cyber resilience is becoming more intelligence-led, continuous and outcome-driven, and is becoming increasingly aligned with frameworks such as the NCSC's CAF. AI will play a central role in this evolution, but only where it enhances understanding, supports decision-making, and enables practical risk reduction.

As Zero Trust continues to develop, AI-enhanced segmentation aligned to clearly defined resilience outcomes offers organisations a pragmatic way to strengthen their security posture in an increasingly complex threat landscape.



CYBER ESSENTIALS
CYBER ESSENTIALS PLUS

Cyber Essentials is a UK government recommended accreditation and helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security.

ncsc.gov.uk/cyberessentials