



NATIONAL
CYBER
RESILIENCE
CENTRE
GROUP



THE NATIONAL CYBER INSIDER

NATIONAL CYBER RESILIENCE CENTRE GROUP

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

Building National Resilience Securing the UK's most critical infrastructure



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



resilience too in the face of an ever-evolving threatscape, with dependence upon increasingly complex supply chains, all the while meeting stringent regulatory requirements.

We see three core aspects of resiliency that CNI and public sector organisations need to think about:

- 1. Resilience through monitoring:** tracking the shifting threat landscape, proactively adding appropriate mitigation measures, so as to enhance overall resilience and ensuring alignment with changing regulations
- 2. Resilience through protecting the digital supply chain:** minimising the potential threat your digital supply chains pose to your estate
- 3. Resilience in threat response:** swiftly responding to and adapting from cyber threats

Resilient monitoring

Visibility over your network is paramount to ensuring you can keep abreast of the changing threat landscape and ensure resilience when the organisation comes under attack. While it's not a new technology, network segmentation is one of the most effective ways to ensure that your organisation has optimal visibility over the type and scope of cyber threats. Paired with third-party threat intelligence data, it can give CNIs and public sector bodies potent internal and external visibility of the potential threats facing their digital estates.

Adopting this type of segmentation will also help organisations remain compliant with upcoming legislation proposed by DSIT in April this year, which will bring in changes to NIS regulations, as well as enhanced regulatory powers to support them. Working towards continual alignment with helpful tools like the NCSC's Cyber Assessment Framework

will be crucial for ensuring compliance with these changing regulations.

Resilient supply chain

According to a 2022 security breaches survey, only about one in ten businesses review the risks posed by their immediate suppliers (13%). It's understandable - most businesses, whether they're public or private sector, have highly complex and interconnected supply chains, and gaining visibility and understanding into how these work and where the weak links persist is immensely difficult. Cyber criminals are well aware of this, and some of the worst public sector attacks of recent years have resulted from cyber attacks against third-party suppliers.

A Zero Trust approach to security is essential for ensuring supply chain security. Imagine the Zero Trust model like an extremely vigilant security guard - methodically and repeatedly checking your credentials before allowing you access to the office building where you work, even if they recognise you, then duplicating that process to verify your identity continuously. Implemented correctly, this architecture works seamlessly for users, reduces the attack surface, limiting the potential blast radius of cyber attacks, and simplifies infrastructure requirements.

Resilient response

When most people think of cyber resilience, this is the part that they have in their minds: how to withstand attacks, recover from them, and adapt for the future.



Cyber resilient organisations should understand that, even with the best preparations, they can't prevent every attack. While still maintaining preventative measures, IT security teams need to adopt programmes and technologies to help mitigate attacks quickly and effectively limit any damage. Here, network segmentation really comes into its own - if your external firewall is breached, segmentation ensures that attackers will find it very difficult to move laterally across your network to create further damage.

Recovering from an attack quickly is just as important, especially for CNI organisations. Getting systems up and running as quickly as possible following an attack or outage is key. Working with a provider that is able to offer high-availability edge computing resources close to where they're needed should be a primary element of any organisation's recovery plan.

Adapting processes and protocols following an attack is often neglected, but at a significant cost. Security teams should lead internal reviews to analyse how the threat came about, the response,

and adjust security programs and IT practices to further enhance cyber resilience. Having high-quality network observability is key here, as it enables the organisation to do a thorough post-mortem on the incident and so better prepare for future threats.

Looking ahead to a more resilient future

Public sector organisations are increasingly in the crosshairs of cyber criminals, facing sophisticated threats that can disrupt operations and compromise sensitive data. As an ambassador for the NCRCG, at Akamai, we understand the critical need for robust cyber defences to safeguard the UK's critical national infrastructure. We believe that resilience is more than the immediate response to an attack. Resilience needs to be an always-on effort, encompassing monitoring, supply chain risk analysis, and advanced response and mitigation techniques. Embedding this culture into the UK's CNI organisations will be critical to maintaining the levels of public services that UK citizens rightly expect from their government.

To find out more. www.akamai.com

Inside this edition...

What is the CRC Network?

Learn about the CRC Network and how this police-led, business-focused initiative collaborates with NCRCG, National Ambassadors and the Cyber PATH programme to deliver greater cyber resilience for our SME businesses and charitable organisations.

PAGE 2

Cyber talent crisis isn't about headcount



A new global study from SANS and GIAC finds that the cyber security workforce crisis may be more misunderstood than ever.

PAGE 5

National Ambassador Chainalysis provides valuable training opportunity



Read about the valuable five-week blockchain training course provided exclusively to Cyber PATH students.

PAGE 6

Cyber PATH alumni is still making an impact

How the 2023 Cyber Student of the Year is encouraging women into cyber careers?



PAGE 6

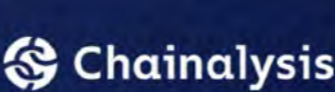
Shaping Cyber's Future: From the frontlines of innovation to inclusive leadership



Read more from Natalie Billingham, Senior Vice President of Sales and Managing Director for EMEA at Akamai.

PAGE 8

NATIONAL AMBASSADORS





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

At NCRCG, we provide insight at a macro level, 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.

Are you identifying the weakest links in your supply chain?

In this edition of The SME Guardian, we highlight some of the businesses who have joined the CRC Network's community and what they are doing to help themselves and others combat the increasing problem of cybercrime. You will also learn about how the CRC Network, through its Cyber PATH programme, is addressing the cyber talent pipeline crisis, by creating real-work experiences for the country's brightest students. Which also means affordable access to entry level risk discovery services for your small business or third sector organisation.

How our National Ambassadors are supporting the SME community

Join us in building your business's cyber resilience



Get it right the first time

At the heart of the construction industry is the need to build resilient infrastructure. This is no different when it comes to your business's cyber resilience. We're here to help you build a strong foundation for your business's cyber resilience, so you can get it right the first time.

Join us in building your business's cyber resilience

At the heart of the construction industry is the need to build resilient infrastructure. This is no different when it comes to your business's cyber resilience. We're here to help you build a strong foundation for your business's cyber resilience, so you can get it right the first time.

Join us in enhancing your cyber resilience



At the heart of the construction industry is the need to build resilient infrastructure. This is no different when it comes to your business's cyber resilience. We're here to help you build a strong foundation for your business's cyber resilience, so you can get it right the first time.

Joining your business's cyber resilience

At the heart of the construction industry is the need to build resilient infrastructure. This is no different when it comes to your business's cyber resilience. We're here to help you build a strong foundation for your business's cyber resilience, so you can get it right the first time.

Joining your business's cyber resilience

At the heart of the construction industry is the need to build resilient infrastructure. This is no different when it comes to your business's cyber resilience. We're here to help you build a strong foundation for your business's cyber resilience, so you can get it right the first time.

Give your business's cyber resilience a police-backed boost



Join the Cyber Resilience Centre in your region and ready your business against today's key threats

The National Cyber Resilience Centre (NCRC) is a national centre for excellence in cyber resilience, working with the UK's leading organisations to help them build a strong foundation for their business's cyber resilience. We're here to help you build a strong foundation for your business's cyber resilience, so you can get it right the first time.

Joining your business's cyber resilience

At the heart of the construction industry is the need to build resilient infrastructure. This is no different when it comes to your business's cyber resilience. We're here to help you build a strong foundation for your business's cyber resilience, so you can get it right the first time.

AVIVA

Joining your business's cyber resilience

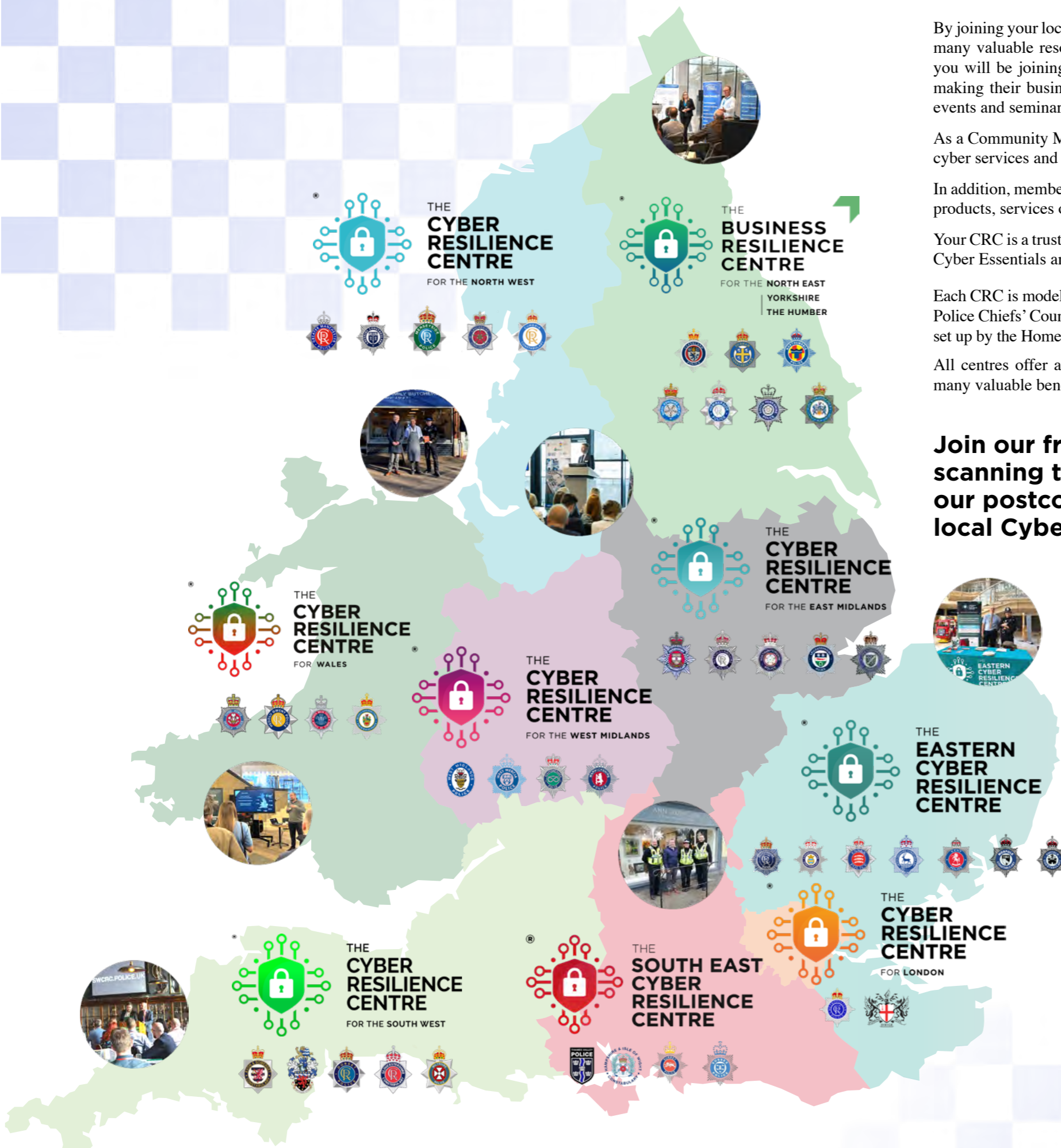
At the heart of the construction industry is the need to build resilient infrastructure. This is no different when it comes to your business's cyber resilience. We're here to help you build a strong foundation for your business's cyber resilience, so you can get it right the first time.

Joining your business's cyber resilience

At the heart of the construction industry is the need to build resilient infrastructure. This is no different when it comes to your business's cyber resilience. We're here to help you build a strong foundation for your business's cyber resilience, so you can get it right the first time.



Joining a Cyber Resilience Centre is a simple process



By joining your local publicly funded Cyber Resilience Centre, you will be able to access many valuable resources, advice, training and support for all things cyber. Moreover, you will be joining a network of like-minded business owners who are committed to making their businesses more cyber resilient in the future. The centres regularly host events and seminars and share local, national and international cyber threats and trends.

As a Community Member, you will be able to take advantage of the range of affordable cyber services and training programmes provided via the Cyber PATH programme.

In addition, membership allows you to learn how to procure private sector cyber security products, services or resources.

Your CRC is a trusted resource and also a straightforward place to find IASME-approved Cyber Essentials and Cyber Essentials Plus Certifiers in your region.

Each CRC is modelled on a successful structured collaboration acclaimed by the National Police Chiefs' Council (NPCC). They form a nationwide network of not-for-profit centres set up by the Home Office.

All centres offer a range of membership options; membership is FREE and includes many valuable benefits.

Join our free community by scanning the QR code and using our postcode tool to find your local Cyber Resilience Centre.



The Cyber Resilience Centre Network has a shared sole aim of helping SMEs increase their cyber awareness and resilience.

There is a 3 in 5 chance that a small business will fail within six months of experiencing a cyber attack and we don't want any businesses to be part of this statistic.

Joining this publicly funded service is **FREE** and includes:

- A free 30 minute review** with the centre's Head of Cyber and Innovation on your current cyber set up.
- Access to free resources**, tools and guidance designed to help your business start its cyber security journey including resources from the National Cyber Security Centre.
- A Cyber Toolkit** - Resources designed to encourage essential cyber security discussions between the company and their technical experts.
- 10 Steps to Cyber Security** - The steps enable businesses to break down the task of protecting their cyber security, by looking at 10 key components.
- A Cyber Attack Drill Toolkit** - A suite of exercises based around real world scenarios designed to allow businesses to test their response and approach to each given scenario.
- A monthly newsletter** full of tips, tricks, and resources to help you tackle current cyber threats and trends.



CYBER PATH™
POLICE & ACADEMIA
TALENT HORIZONS

An elite talent pipeline, Cyber PATH welcomes the brightest students who want to help shore up the nation’s defences with law enforcement against cybercrime and develop the essential skills, knowledge and experience they need to succeed in the workplace upon graduation in a live, commercial setting.

Introduction to Cyber PATH


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 affordable 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

<p>SECURITY AWARENESS TRAINING</p>  <p>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.</p>	<p>INTERNAL VULNERABILITY ASSESSMENT</p>  <p>Identifies any weaknesses in your internal networks and systems, such as insecure WiFi networks and access controls, or opportunities to steal sensitive data.</p>	<p>REMOTE VULNERABILITY ASSESSMENT</p>  <p>Identifies any weaknesses in the way your organisation connects to the internet.</p>
<p>FIRST STEP WEB ASSESSMENT</p>  <p>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.</p>	<p>INDIVIDUAL INTERNET DISCOVERY</p>  <p>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 cyber criminals to target your business.</p>	<p>SECURITY POLICY REVIEW</p>  <p>An in-depth review of how your current security policy is written and implemented.</p>
<p>CORPORATE INTERNET DISCOVERY</p>  <p>A comprehensive review of publicly available information about your business using internet search and social media tools. It is primarily focused on identifying any information that could be used by cyber criminals to craft an attack.</p>	<p>WEB APP VULNERABILITY ASSESSMENT</p>  <p>A complete assessment of your website to highlight any vulnerabilities and their potential risk to your business.</p>	<p>CYBER BUSINESS CONTINUITY REVIEW</p>  <p>A thorough review of your business continuity plan and overall resilience to cyber attack.</p>



LAUNCH YOUR BUSINESS INTO THE STRATOSPHERE OF CYBER RESILIENCE WITH CYBER PATH



CYBER PATH™
POLICE & ACADEMIA
TALENT HORIZONS



New SANS Report Finds Cyber Talent Crisis Isn't About Headcount. It's About Skills.

A new global study from SANS and GIAC finds that the cyber security workforce crisis may be more misunderstood than ever.

In a sharp break from headlines focused on unfilled roles, the 2025 Cyber Security Workforce Research Report reveals that 52 percent of cyber security leaders say the real issue is not the number of people but a lack of the right people with the right skills.

The study, based on insights from nearly 3,400 cyber security and HR managers, shows a clear shift in mindset. Organisations are no longer prioritising headcount growth. Instead, they are investing in skills development, internal training, and more strategic collaboration between cyber security and HR teams.

“My personal perspective is that we don't actually have a talent shortage in cyber security,” said Helen Patton, former CISO and cyber security leader at Cisco. *“The real issue lies in understanding the skill*

sets that are needed for the kinds of roles you have and finding the people who have those skill sets.”

The shift is not just philosophical. This year's data confirms that technical capability has overtaken work experience and academic degrees as the most valued hiring qualification. Certifications now rank second, with hiring managers placing increasing value on validated, job-ready skills rather than resumes padded with credentials.

“A couple of years ago, it was 70 percent technical expertise and 30 percent attitude,” said Aus Alzubaidi, CISO at MBC Group. *“Today, we're approaching 25–75, where most of the profile is based on attitude. Adaptability and eagerness to learn are now non-negotiable.”*

Workplace culture and flexibility also emerged as central themes in both hiring and retention. According to the study, 34 percent of organisations say working well within a team is the most important cultural value in a cyber security hire. Remote

work, development programmes, and clearly defined career paths are now being recognised as competitive differentiators.

“We frame soft skills as power skills because, in cyber security, we're here to build teams,” added Lynn Dohm, Executive Director of WiCyS. *“Some of the best talent we've recruited came from accounting, education, and other unexpected places.”*

The study also shows early signs that regulations like NIS2 and DORA are already shaping hiring practices. Nearly half of European organisations say their workforce strategies are now being influenced by privacy, compliance, and risk management mandates.

This comprehensive report, based on global survey responses from HR and Cyber security Managers, offers valuable insights on how these two work roles can collaborate effectively to build, develop, and retain high-performing cyber security teams.



Download the full report and delve deeper into insights around:

- How the cyber security skills gap is evolving and what it means for your organisation
- The critical role of cyber security training and certifications in team development and retention
- Effective collaboration strategies for HR and Cyber security Managers in the hiring process
- Adapting to changing workplace values and how they impact hiring and retention
- 8+ case studies from industry leaders like United Airlines, Cisco, IBM, Airbus, Middle East Broadcast Corporation, and more.

Visit the SANS stand (B10) to find out more and download the full report:
<https://www.sans.org/u/1AZF>

IFA really does see the value of advice

The Cyber PATH team and the regional centres are always delighted to receive positive feedback after they deliver one of their services to a local business, and that was certainly the case with fmifa (Financial Management - Independent Financial Advice), the long-established and highly respected firm of independent financial advisors based in Penn, Buckinghamshire. However, in reality, it's not really a surprising reaction from a company whose values and mission are so closely aligned with that of the CRC Network!

As a financial management company, they have a well-earned reputation for providing reliable advice based on the knowledge, expertise and experience of their team. While their advice is primarily focused on financial planning, they occasionally highlight what they know about emerging threats, particularly around financial scams and online fraud; it's something their clients have come to value and appreciate, mainly because it's coming from a source they know and trust.

Because they are in a trusted position, they naturally do everything possible to fact-check any cyber advice they pass on to clients. So, they were particularly intrigued when one of their team received a recommendation to look at the work of the South East Cyber Resilience Centre, a police-led, business-focused organisation dedicated to improving cyber resilience among the



SME community. Like fmifa, the centre offers truly independent guidance and training, and so the relationship began.

As a business that is conscious of its responsibility to protect client data, fmifa decided to commission the centre to provide some training for all of the staff. Regardless of their previous diligent approach to cyber, like their clients, they appreciate the value of advice, especially when an expert and independent source provides it. After talking through the options with a member of the Cyber PATH team, they booked Security Awareness Training.

The training was provided by Ehsan Mehrdad, a Cyber PATH student under the guidance of Detective Inspector Chris White, who is Head of Cyber & Innovation at the South East Cyber Resilience Centre. The training was delivered in two identical sessions so that the fmifa team could all attend one or the other without any disruption to the day-to-day operation of the business.

fmifa was delighted with the delivery of the training and the time taken by the Cyber PATH team to break the message down into layperson's terms; again, it aligns very well with their ongoing efforts to speak to their clients in non-financial jargon!



The whole fmifa team was particularly impressed with the professionalism of Ehsan, who “presented exceptionally well, in a relaxed manner”.

However, beyond Ehsan's style and knowledge, they were particularly impressed with how the Cyber PATH programme enables students to gain paid real-work experience. As a company that is genuinely invested in the local community and that accepts its social responsibility, they truly appreciated how their use of the Cyber PATH service is helping to make students more workplace-ready. Speaking about Cyber PATH and the Security Awareness Training, fmifa Managing Partner Philip Harper said:

“We were delighted with the training sessions delivered by Ehsan; his presentation was excellent, and he hit the right notes.

“As a business, we know the value of expert advice, and we feel this is what we received; and even though we are cyber aware, we still learned a great deal in an easily digestible manner. Every member of our team took something away from the training, so that made it a success for us.

“We were delighted to provide a university student with the opportunity to experience a professional workplace. In return, we benefited from their up-to-

date knowledge and training. I highly recommend Cyber PATH to any organisation.”

Indeed, the team at fmifa were so confident in the quality of advice they received that they are now sharing it with their clients via their popular client newsletters!

We are pleased with the outcome of our initial engagement with fmifa; we're also delighted they are now exploring some of the other Cyber PATH services to further bolster their cyber presence. We look forward to working with them again in the near future.

“We were delighted with the training sessions delivered by Ehsan; his presentation was excellent, and he hit the right notes.

Shakespeare Birthplace Trust embraces cyber resilience



West Midlands CRC and Cyber PATH were delighted to recently work with the Shakespeare Birthplace Trust to deliver Security Awareness Training across the whole organisation, including volunteers, staff and trustees.

The Shakespeare Birthplace Trust was formed in 1847 following the purchase of Shakespeare's Birthplace as a national memorial. It is the independent charity that cares for some of the world's greatest Shakespeare heritage in his home town of Stratford-upon-Avon. It is the global centre for learning about and experiencing the works, life and times of the world's best-known writer.



provide via Cyber PATH.

It comprises five Shakespeare family homes, internationally designated museum collections, award-winning learning programmes and digital

channels, providing imaginative, immersive and interactive opportunities for people of all ages and backgrounds to get up close and personal with Shakespeare.

At the heart of all things Shakespeare, the Trust holds the world's most extensive Shakespeare-related library, museum and archives open to the public, with over 1 million documents, 55,000 books and 12,000 museum objects. They also care for the Royal Shakespeare Company's archive of theatre records, as well as an extensive local history archive of Stratford-upon-Avon and South Warwickshire, with records dating back to the twelfth century.

With so many facets to the Shakespeare Birthplace Trust, you will appreciate the requirement for a great deal of staff and, crucially, a high number of volunteers. The trustees correctly identified the need to make all personnel more cyber aware, something we at West Midlands CRC were delighted to

Commenting on the Security Awareness Training service, Mark Watts, Head of Business Change & Delivery, said: *“It has been a great experience*

working with the Cyber Resilience Centre for the West Midlands and Cyber PATH. Through Cyber PATH, they have provided expert cyber security awareness training sessions that were pitched at the right level for our organisation and filled with useful and actionable information. Their training has resonated with all levels of our organisation, including volunteers, staff and our trustees.

“Colleagues have praised their trainers for demystifying topics and providing easy-to-adopt behaviours to keep people safe online at work and home. Other comments have focused on how highly knowledgeable, personable, and friendly the trainers were, making attendees feel comfortable and able to ask questions.

“Cyber PATH made time to understand our organisation and tailored our training accordingly. They covered different types of security vulnerabilities, including social engineering, strong passwords and their importance, Spear Phishing, Vishing, Email Phishing and Smishing, Social Engineering, Device Management and Ransomware.

“Each was expertly broken down into simple messaging that directed people on what to look for and how to act.

“We would highly recommend both their training programme and their expert trainers.”

We were delighted to work with such a high-profile organisation and to see how they embraced the training in order to understand the threats charities and the business sector face in today's world.

Speaking about the Cyber PATH services, Detective Inspector Michelle Ohren, Managing Director of West Midlands Cyber Resilience Centre, said: *“WMCRC are extremely proud of our Cyber PATH programme. It allows the next generation of cyber students to gain invaluable experience whilst ensuring quality training and practical guidance that everyone, even those with limited IT awareness, can undertake and embed into their daily practises.*

“This ensures that not only do they play their part in protecting their organisation, but they also become safer in their personal lives.

“It has been a privilege to work with The Shakespeare Birthplace Trust and support their staff and volunteers by delivering their cyber security training.”





National Cyber Security Centre

a part of GCHQ

www.ncsc.gov.uk



Explore the many useful resources created for SMEs



TOUGHEN UP

your business's online security with 2-step verification



Turn on 2-step verification now



Q&A: Securing Modern Apps in a Complex Threat Landscape



Modern applications are no longer monolithic—they're built as intricate symphonies of microservices, APIs, and dynamic app-to-app communications. Every interaction, while enabling innovation, can also introduce vulnerabilities. As applications become more mobile, distributed, and API-driven, securing them requires more than just perimeter defences. Visibility, control, and resilience must be built into the very fabric of application architecture.



In this Q&A, Charlie Gero, CTO and Vice President of the Security Technology Group at Akamai, discusses how organisations—especially within the UK public sector—can navigate today's evolving threat landscape. With rising geopolitical pressures, growing regulation, and digital government initiatives accelerating transformation, Charlie explores the practical steps security leaders must take to safeguard critical systems and services, without slowing innovation.

Q: What are the top security concerns for modern apps, especially in the public sector?

The attack surface is expanding rapidly—particularly

through APIs, microservices, and third-party integrations. In the UK public sector, data protection under UK GDPR and NCSC guidance adds another layer of pressure. Risks include insecure APIs, misconfigured services, and lack of visibility across data flows. Proactive, layered security architecture is essential.

Q: How can organisations gain better visibility and control in today's API-first environment?

You can't protect what you can't see. By implementing platforms that extend API protection to customers, service networks, and observability platforms, teams can control traffic between services, detect anomalies, enforce policies, and track data movement in real time - essential for both operational security and regulatory compliance.

Q: What's the secret to combining innovation with strong security?

Security should never be the brake on innovation—it should be the engine. By embedding DevSecOps practices and aligning with regulatory frameworks like the NCSC's Cyber Assessment Framework,

teams can ensure compliance while innovating faster. Integrate security early, automate often, and monitor continuously.

Q: Microservices and app-to-app communication expand capabilities—but also risk. How should teams respond?

Every connection between microservices is a potential vulnerability. Without unified security controls, attackers can exploit lateral movement within applications. Enforcing Zero Trust principles—strong identity validation, encryption, and strict access controls—helps secure every hop. It's about ensuring only authorised services can talk to each other.

Q: What strategies can improve resilience in the face of evolving threats?

Resilience is multi-layered. UK organisations should invest in threat modelling, real-time monitoring, and rapid incident response. Build infrastructure that supports automatic failover, risk-based patching, and business continuity. This is especially critical in sectors like healthcare, policing, and utilities.

Q: How can automation and AI help under-resourced teams?

Public sector teams often face budget and staffing constraints. That's where AI and automation become force multipliers. These technologies detect threats faster, reduce manual workloads, and help scale security operations without scaling headcount. It's essential for keeping pace with today's rapidly evolving threat landscape.

Q: What immediate steps should organisations take to boost app resilience in 2025?

First, focus on visibility, invest in security tools that give you API observability. Next, integrate security into DevOps to streamline compliance and reduce risk at every stage. Finally, prioritise automation and AI to scale security efforts without increasing headcount. These three pillars create a scalable, future-ready security foundation.

The public sector is under immense pressure to modernise while staying secure. From NHS digital platforms to cloud-powered government services, the risks are real—but so are the opportunities. As threats grow more sophisticated, the response must be smarter. Embedding security into the DNA of application development is the only way to keep pace. With visibility, automation, and a Zero Trust mindset, public sector organisations can secure the future—without sacrificing speed or service.

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.

Cyber PATH students learn from the industry leaders

Cyber PATH is delighted to report on an exciting collaboration with one of its national ambassadors, Chainalysis, which will allow its students to gain an exceptional understanding of blockchain. The exclusive 5-week virtual session will allow Cyber PATH students to dive into cryptocurrency and blockchain fundamentals, network with their professionals, and learn about careers at Chainalysis. At the end of the session, students will have the opportunity to sit for your Chainalysis Cryptocurrency Fundamentals Certification (CCFC) exam and add a credential to their list of accomplishments.

Not only will the students gain invaluable knowledge, but they will also be able to network with Chainalysis professionals and have the chance to win a £1000 scholarship.

Speaking about the Crypto Capstone initiative, Alex Cable (pictured), Vice President N-EMEA at Chainalysis, said: "We are excited to be working with the Cyber Resilience Centre Network and the Cyber PATH students. We are committed to developing a strong talent pipeline and encouraging young people to pursue careers in cyber and blockchain. Through this course, we aim to help the students recognise the value and context of cryptocurrency relative to the traditional financial system and understand the underlying blockchain technology enabling cryptocurrencies.



"Upon completion, the students will be able to describe key concepts and technology, recognise the value proposition of cryptocurrencies and understand how to begin constructing risk assessments drawing on blockchain analysis.

"For Chainalysis, it's an opportunity to work closely with students who are already pursuing a technical career in related topics such as Engineering, Computer Science, Cyber Security or Information Technology. These are the people we want to encourage and attract. We hope that the course engages them and whets their appetite to work in and around blockchain."

The course sessions were run on Monday afternoons and, started on the 17th February and are running until the 24th March. Lucy Taylor is one of the 37 students enrolled on the course, here's what they said about the experience so far: "The Chainalysis course is a great opportunity to get an industry-recognised certification that will really help when it comes to getting a graduate job. The instructors are passionate and knowledgeable about crypto, and I always feel comfortable asking questions about things I'm unsure of."

Also on the course is student Bartlomiej Kajak who said: "The course provides fresh, up-to-date information on blockchain technology and explains its fundamentals. The tasks are engaging and help reinforce the concepts. I enjoy the deep dive



into how blockchain works and the cryptocurrency economy. Additionally, the course provides insight into cyber security and forensics around the main topic, which is particularly interesting for me. Despite having previous knowledge, I have learned many new things and looking forward to the upcoming sessions."

Detective Chief Inspector Fiona Bail, Head of Cyber PATH added: "We'd like to thank Chainalysis for the opportunity they have provided for our Cyber PATH students; this is precisely the kind of initiative that will help to develop the talent pipeline. The information and knowledge they share are invaluable to the students, who will gain valuable insights from a global leader in blockchain technology.

"The students on the course are enthused and engaged; the opportunity to network with and learn from industry experts is exceptional and greatly appreciated".

Chainalysis is a blockchain data platform that provides data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cyber security companies in over 70 countries. Its data powers investigation, compliance, and market intelligence software that has been used to solve some of the world's most high-profile criminal cases and grow consumer access to cryptocurrency safely.

Award-winning Cyber PATH alumni student continues to make an impact



We are very proud of the quality of students we attract to our Cyber PATH programme. The aim has continually been to develop a genuinely elite workplace ready talent pipeline for industry and law enforcement". Our recruitment process has helped us to identify not only the most talented students but also those who are truly committed to helping shore up the nation's defences against cybercrime and who want to develop the essential skills, knowledge and experience they need to succeed in the workplace upon graduation in a live, commercial setting.

Since the inception of the Cyber PATH programme, we have worked with many promising students who are now starting to join the workforce, many of whom have taken on key cyber roles. It is now that we can see the impact of the Cyber PATH programme, and we're

excited to watch as our Cyber PATH alums begin to play an essential part in strengthening the resilience of our businesses and organisations in the UK.

In September 2023, we were excited to report that one of our students, Sophie Powell, was named a finalist in the Cyber Student of the Year 2023 category at the prestigious National Cyber Awards. We were even more delighted to announce that she won!

Since then, Sophie has gone from strength to strength, and we are delighted to say she is firmly rooted in a cyber career, having joined Cyberfort, the well-established and highly-respected cyber security services provider. However, the story doesn't end there. Sophie continues to demonstrate her commitment to the cyber industry in a very positive manner. Sophie is co-founder and director of CyberWomen Groups C.I.C.

CyberWomen Groups C.I.C. brings together and supports women interested in or studying cyber security at university. They work within universities to organise events that encourage diversity and positive change within STEM subjects. CyberWomen Groups is an inclusive community that any student can

join, regardless of gender identity. Their mission is simple: creating a community that inspires learning, networking, and positive change.

They are forming a community of like-minded students within UK universities with an interest in cyber-based subjects to come together and empower women in this field. Their initiative is stand-alone: they are entirely student-led. Their executives lead the way in their branches, setting out the individual goals and ambitions they want to achieve that year. They work hard to ensure their students are heard and provide the support and guidance they require to help them achieve their goals.

CGI However, the link to Cyber PATH, the CRC Network and NCRCG doesn't stop there. We are delighted that one of our founding National Ambassadors, CGI, has shown its commitment to developing cyber talent by becoming a Silver Founding Strategic Partner of CyberWomen Groups. Speaking about their involvement, Maxine Bulmer, Vice President of Cyber Consulting at CGI in the UK, said: "The tech industry thrives on innovation and




diversity of ideas, and only by harnessing talent across all genders can we create meaningful change for our clients and communities. At CGI, we strive to be unconditionally inclusive and are passionate about inspiring the next generation of young professionals to pursue STEM careers. We are proud to partner with CyberWomen Groups C.I.C. to encourage the next generation of cyber security consultants."

It is rewarding to see the Cyber PATH programme delivering its original objectives, which were to develop a first-class cyber talent pipeline for policing and the private sector by enlisting the brightest students to work alongside senior Cyber Security Practitioners and police officers to deliver high-quality and tailored cyber resilience services to smaller organisations. Sophie's story embodies all of our goals and more. Not only has she brought her considerable talent into the cyber ecosystem, but she continues to encourage others to follow her example!




Pick of the pods!

Dr. Mandy Haeburn-Little, Cyber Woman of the Year 2021, in conjunction with the National Cyber Resilience Centre Group (NCRCG), brings listeners access to strategic conversations with industry leaders and figures in the UK's cyber resilience landscape.

With a changing roster of high-profile guests from across policing, government, academia and business, stay tuned for the latest in the UK's cyber security thought leadership landscape.



Scan the QR code to listen to or download all CyberVersed podcasts. Or, find them on all popular podcast platforms.



CyberVersed

HOSTED BY
DR. MANDY HAEBURN-LITTLE



National Ambassador Focus

Feat:

- Marc Carney, Director, Security Solutions Group
- Gabriela Graddien, EMEA Security Sales Director
- Joseph Boland-Scott, Security Product Manager

HOSTED BY MANDY HAEBURN-LITTLE

Topics discussed include:

- Zero Trust frameworks
- Microsoft's mission statement
- Secure Future Initiative
- Password-related attacks
- Microsoft's security posture
- AI and automation.
- Repivoting of attackers
- AI-based attacks
- Phishing and identity attacks
- Microsoft Security Copilot
- Democratisation of knowledge
- Carbon emissions from data centres
- Deepfake

Duration: 47 mins



National Ambassador Focus

Feat:

- Nigel Smart, Director of IT & Development, Logistics UK
- Natalie Chapman, Head of Public Affairs, Logistics UK

HOSTED BY MANDY HAEBURN-LITTLE

Topics discussed include:

- Background to Logistics UK
- Compliance and training
- Media presence
- Engagements with governments, MPs, backbenchers and policymakers
- Lobbying and evidence-based analysis
- Logistics Productivity Index
- Investment priorities
- Decarbonisation
- Skills shortage in the sector
- Generation Logistics.
- Cyber awareness
- National Ambassador benefits

Duration: 31 mins



National Ambassador Focus

Feat:

- Richard Meeus, Director of Security Technology and Strategy EMEA
- Matthew Payne, Regional Director, EMEA Financial Services Industry and Public Sector

HOSTED BY MANDY HAEBURN-LITTLE

Topics discussed include:

- The water cooler moment and background to Akamai
- How Star Wars trailer helped to validate the platform's design
- The three main verticals of the business: Delivery (of content) Security Cloud
- The Security Operations Centre
- State of the Internet Report (SOTI)
- Ransomware attacks
- Impact of AI on cybercrime

Duration: 40 mins



National Ambassador Focus

Feat:

- Rachel Vigor, Business Services, Governance, Risk & Controls Director, Nationwide Building Society
- Sharon Gould, Supplier Security Manager, Business Services GRC, Nationwide Building Society

HOSTED BY MANDY HAEBURN-LITTLE

Topics discussed include:

- Nationwide's history and what it stands for.
- A 'Mutual' explained
- Building a safe and secure future
- Nationwide's approach to risk
- Encouraging open, honest and transparent conversations
- Risk in relation to the supply chain
- NCRCG/Nationwide supply chain campaign
- Working with IASME
- The acquisition of Virgin Money

Duration: 32 mins



Ambassador Focus - HP

Feat:

- David Scutt, Head of Software Sales EMEA at HP

HOSTED BY MANDY HAEBURN-LITTLE

Topics discussed include:

- Core focus areas of the business: Personal Computing & Printing 3D Printing Hybrid Work Gaming
- Maintain cyber security across the business
- The HP Work Relationship Index
- Innovative solutions that improve efficiency and productivity.
- HP Customer First Community
- Making products secure by design
- Sustainability

Duration: 27 mins



In conversation with Nik Adams

Feat:

- Nik Adams, Assistant Commissioner, City of London Police, National Coordinator of Economic and Cyber Crime, Chair, NCRCG, National Ambassadors Steering Group

HOSTED BY MANDY HAEBURN-LITTLE

Topics discussed include:

- The range of National Ambassadors
- Understanding the vulnerabilities sector-by-sector
- Tapping into the expertise and experience of the right people
- The CRC Network and how the CRCs Supporting SMEs in their communities.
- Supply chain challenges
- The Cyber PATH programme
- Diversity and engaging with a range of people, particularly those who are neurodivergent.
- Gratitude to the National Ambassadors for their support

Duration: 27 mins



Ambassador Focus - Trustify

Feat:



- John Madelin, Advisory Board Member, Trustify Cyber

HOSTED BY MANDY HAEBURN-LITTLE

Topics discussed include:

- Background to Trustify
- Over complicated messaging and demystifying and simplify cyber security.
- Risk assessments
- Customised action plans
- The need for continuous monitoring
- 15 signals used by cybercriminals
- A case of champagne challenge
- Collaborating with NCRCG to help make cyber resilience more attainable to the SME community
- Inclusivity and encouraging young people into careers in cyber

Duration: 33 mins



Ambassador Focus - Sir Robert McAlpine

Feat:

- Andy Black, Chief Information Security Officer, Sir Robert McAlpine
- Rachel Lloyd-Moseley, Head of Procurement - Nuclear, Sir Robert McAlpine

HOSTED BY MANDY HAEBURN-LITTLE

Topics discussed include:

- The background and brief history of Sir Robert McAlpine
- Constructing a better world for future generations
- Sir Robert McAlpine's strong family values
- The support and backing of the Board
- Inter-department collaboration
- Why Sir Robert McAlpine joined NCRCG as a National Ambassador
- Raising awareness of cyber security throughout their supply chain
- Embracing AI to achieve greater levels of efficiency and safety

Duration: 34 mins



National Ambassador Focus

Feat:

- Ed Parsons, VP, Global Markets & Member Relations
- Dr Sarjana Mehta, Senior Director, Advocacy
- Andy Woolnough, EVP, Corporate Affairs
- Alex Mortimer, Manager, Global Academic Partnerships

HOSTED BY MANDY HAEBURN-LITTLE

Topics discussed include:

- Background to ISC2
- Leading the way as a membership association for cyber security
- Gold standard certification, CISSP
- ISC2's work in research, training, and certification
- Advocacy and ensuring policymakers understand members' needs in three areas: - Workforce development - Professionalisation - Critical issues of the day.
- Developing cyber talent pipeline
- Making a positive impact in local communities

Duration: 46 mins



National Ambassador Focus

Feat:

- Caroline Barnett, Principal Consultant
- Nicky Furlong, Sr Director, N. Europe, Public Sector, Health and Life Sciences
- David Sharroon, Head of Hyponormalisation, UK&I
- Dr Iain Brown, Head of Data Science, Northern Europe

HOSTED BY MANDY HAEBURN-LITTLE

Topics discussed include:

- Background to SAS
- Making the best use of structured and unstructured data
- The need for transparency when using AI and Generative AI
- How they predict what's coming next
- Their work in healthcare
- AI_PREMie - this potentially life-saving solution aims to empower clinicians by developing a powerful risk stratification tool
- How to avoid being frightened by AI
- The difference between Artificial Intelligence and Automation

Duration: 44 mins



SECURITY AWARENESS TRAINING

DID YOU KNOW **YOUR EMPLOYEES CAN BE YOUR BIGGEST ASSET TO PROVIDING A BARRIER TO CYBERCRIME?**

Our security awareness training provides simple and effective knowledge for people to understand their environment and provide the confidence to challenge when something doesn't look right.

Security Awareness Training is a Cyber PATH service delivered on behalf of our Regional Centres.
cyberpath.co.uk



CYBER PATH™
POLICE & ACADEMIA
TALENT HORIZONS

Shaping Cyber’s Future: Why Inclusion Must Be at the Heart of Progress

Author: **Natalie Billingham**, Senior Vice President of Sales and Managing Director for EMEA at Akamai



As the digital world grows more complex, our cyber security challenges aren’t just technical—they’re human. At this year’s CyberUK, conversations around innovation, risk, and resilience are rightly front and centre. But just as vital is the conversation around who is shaping those solutions—and whether they truly reflect the world they aim to protect.

Cyber security is about far more than firewalls and code. It’s about trust. It’s about creating safe digital environments where businesses, communities, and individuals can thrive. To do that well, we need teams and leaders that are as diverse as the challenges they face.

Today, women still make up less than one in five cyber security professionals in the UK, with similar figures across much of Europe - according to recent LinkedIn data and the UK government’s Cyber Security Skills study. This gap isn’t just a statistic—it’s a signal that we’re not drawing from the full breadth of talent and perspectives available to us.

If we are serious about shaping a future-ready, resilient cyber security workforce, we must start by making space for more voices. That means actively addressing the factors that limit women’s participation and advancement in the field. Promoting STEM education from an early age, showcasing visible women role models, and building inclusive mentorship and networking opportunities are critical. Just as important is the need to challenge bias in hiring and promotion, and to create workplace cultures where every voice is heard and valued.

At Akamai, we’re working to change this narrative. Our FLAME initiative —Female Learning and



Mentoring Experience—connects women across the industry through mentoring, skills development, and shared experience. It’s one part of a much larger effort needed across the sector to support, retain, and elevate women in cyber.

This week at CyberUK, I’ll be joining the Women in Cyber Breakfast and serving as a judge at the CyberDen startup competition. Events like these are powerful reminders that the future of our industry is being shaped not only by technological innovation, but also acts as a reflection of the people behind it.

Inclusion is not a box to tick—it’s a force multiplier. When we broaden who gets a seat at the table, we don’t just create fairer workplaces—we build smarter, more adaptable, and more resilient cyber security systems for everyone. Because the future of cyber isn’t just about keeping up with threats, it’s about making space for more people to help lead the way forward.

Search ‘FLAME (Female Learning And Mentoring Experience)’ in LinkedIn Groups to join the community. www.akamai.com

ARE YOU READY TO BECOME MORE RESILIENT?



Join our free community by scanning the QR code and using our postcode tool to find your local Cyber Resilience Centre.



Immigration consultancy begins their Cyber Essentials journey

Consultancy firm The Westwood Organisation has been working with The South East Cyber Resilience Centre to train and update their staff about cyber threats as part of their preparation for Cyber Essentials certification.



The Westwood Organisation works with employers, education providers and individuals in all areas of immigration work. Founder and Director Ian Westwood, a former immigration chief, set up the business over twenty years ago to provide niche consultancy services focused on immigration advice, training and consultancy. While they ultimately work with individuals, the primary source of their work is referrals from educational institutions for student support and commercial organisations for employee support.

Ian recently attended a business networking event where guest speaker Katy Bourne, Police and Crime Commissioner for Sussex, was talking about cyber security. Ian took the opportunity to ask a question about what businesses could and should do to become more cyber resilient. Fortuitously, Detective Superintendent Patrick Milford, Director at the South East Cyber Resilience Centre, was in the room and managed to catch up with Ian during the networking session. Patrick arranged for him and Detective Inspector Chris White, South



East CRC’s Head of Cyber and Innovation, to visit Ian at The Westwood Organisation to explore how they could work together to make the company more resilient in the future.

It is fair to say that The Westwood Organisation were reasonably well aware and had taken many of the primary steps towards protecting themselves. However, their work involves the handling of large amounts of personal data, so they wanted to be sure they are adopting best practices in all areas of online protection. The outcome of the meeting was a general agreement that they should be aiming for Cyber Essentials accreditation and that Security Awareness Training for the whole team was an appropriate starting point in preparing for such an application.

Cyber PATH student Ehsan Mehrdad delivered the Security Awareness Training under the guidance of former Detective Superintendent Paul Lopez, Managing Director of the Eastern Cyber Resilience Centre.



Once again, it’s important to stress that the team at The Westwood Organisation were reasonably well-versed in cyber and the associated threats, primarily because they are fully aware of their responsibilities when handling the type of data they do daily. That said, all of them found the session extremely beneficial and worthwhile.

Ian Westwood was delighted with the session and commented:

“It was amazing to see the engagement of the whole team. In all honesty, the entire team were expecting it to be a fairly tedious course, but everyone thoroughly enjoyed it and was blown away by some of the information that was shared.

“The sophistication of cyber attacks and

the information about social engineering was especially relevant and eye-opening. And Ehsan’s delivery was excellent and entertaining, with plenty of time set aside to answer questions and engage with the team. The room was actually buzzing, which was great to see!”

The team at The Westwood Organisation are certainly more aware of both the current status and the emerging threats. And even though they had generally adopted best practices, the partnership with South East CRC has highlighted small things that, with minor adjustments, will make them even more secure. When commenting on where they are now, Ian Westwood said: “We’re happy that there were no significant issues, and we’ve implemented some minor changes in processes and procedures that will assist us as we make our Cyber Essentials application, but more than that, the association with the South East CRC has provided the confidence that we are doing the right things to make ourselves more resilient in the future.

“It really is a fantastic service, and because it’s Home Office funded and led by policing, it is genuinely independent and trusted advice, something we strive to deliver and fully appreciate the value of.”



What is Internet Discovery?

Our Internet Discovery service provides a comprehensive review of publicly available information about your business, employees, suppliers or prospective partners, using internet search and social media tools.



Cyber Essentials & Cyber Essentials Plus

Cyber Essentials

The first tier of Cyber Essentials is a self-assessment option which gives you resilience against a wide variety of the most common cyber attacks. Your organisation can assess themselves against five basic security controls and a qualified assessor can verify the information provided. This includes using firewalls, having secure configuration in place, software patching and having secure user and administration accounts.

Achieving Cyber Essentials allows you to:

- Demonstrate a commitment to cyber security to your customers and clients with a certificate and badge to display in your premises and website.
- Make your organisation more resilient against the most common forms of cyber attacks.
- Achieve more business with the assurance that you take cyber security seriously.

Cyber Essentials PLUS

The second tier of Cyber Essentials is Cyber Essentials Plus. Cyber Essentials Plus offers the same simplistic approach as the first tier, but also involves physical tests to your network and computers by independent professionals. Successful accreditation of Cyber Essentials Plus provides a higher level of assurance that your organisation has a strong cyber resilience regime with correctly implemented controls in place to maintain a robust defence against cyber attacks.

With Cyber Essentials Plus, you can:

- Demonstrate a commitment to cyber security to your customers and clients with an enhanced certificate and badge to display in your premises and website.
- Attract new business with the assurance you have cyber security measures in place.
- Attract new government contracts that require Cyber Essentials Plus certification.



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.



www.ncsc.gov.uk/cyberessentials