nationalcrcgroup.co.uk

THE SME GUARDIAN

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

Manufacturing business almost had to throw in the towel

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.

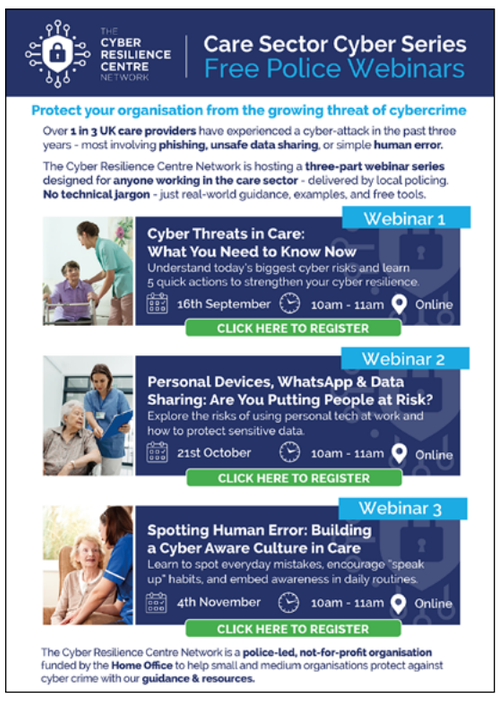
Unfortunately, the incident occurred before engagement with the CRC. Still, it highlights the critical need to make staff aware of the risks and fully understand the vulnerabilities in your operation. Membership of a CRC would have signposted the company to Cyber PATH Security Awareness Training, Vulnerability 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 East CRC 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 **1736** registrations, resulting in **1308** new members in the care sector joining a regional CRC.



The Care Sector Cyber Series has been a great success already; however, it has also led to a further opportunity with Care England, an organisation representing the entire adult care sector in England. Their membership includes organisations of varying types and sizes, among them, single care homes, small local groups, national providers, and not-for-profit voluntary organisations and associations.

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.

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.

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.

Inside this edition...

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 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.

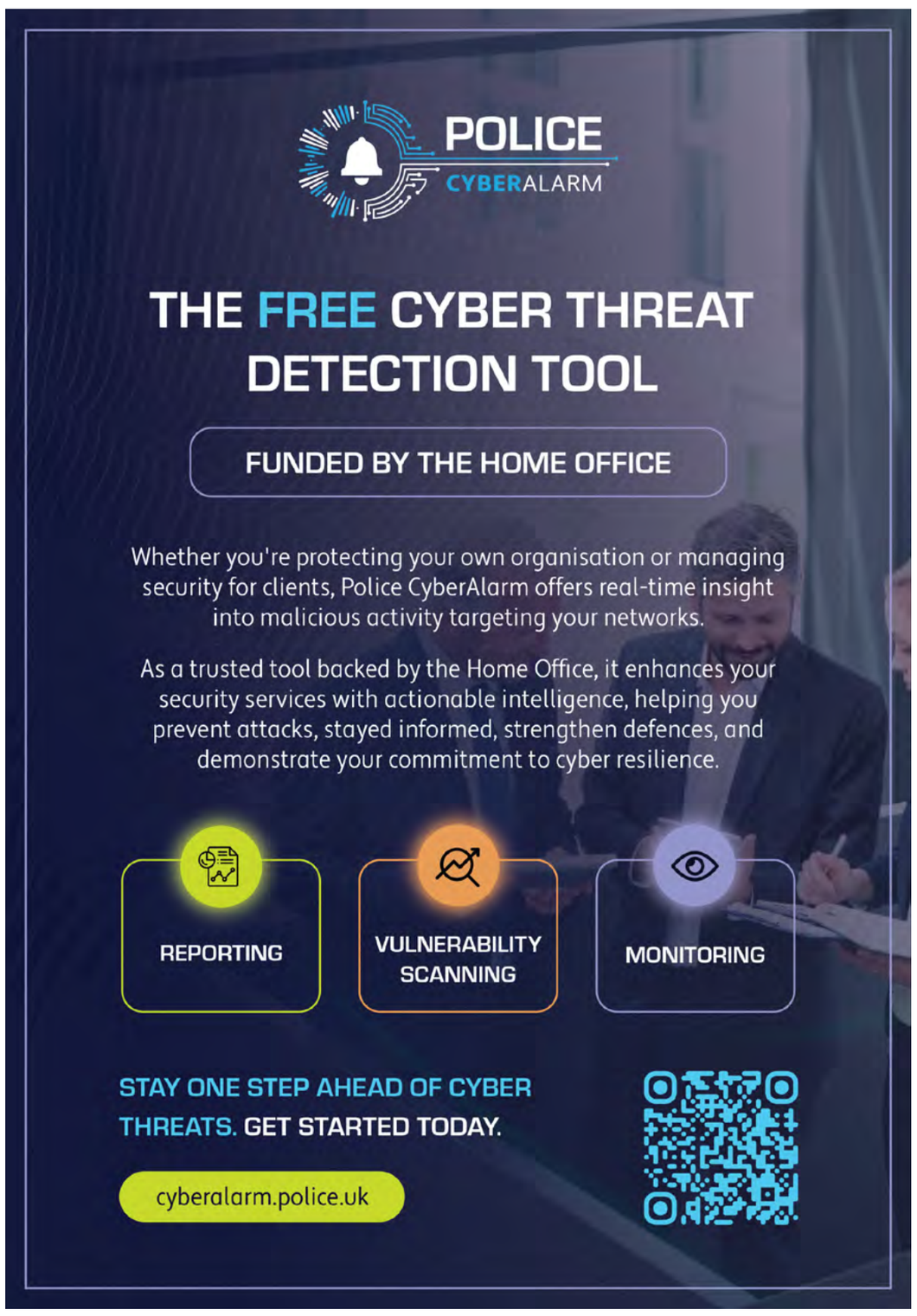
The Network is delivered by the **National Cyber Resilience Centre Group** (NCRCG), which is a not-for-profit organisation funded and supported by the Home Office, policing and private sector partners. It provides a platform to coordinate a strong defence against cybercrime and, by doing so, makes the 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. NCRCG works closely with the National Ambassador companies to devise and run bespoke outreach campaigns designed to encourage their SME customers and those in their supply chain to engage with their regional Cyber Resilience Centres. We also support the National Ambassadors' employees if they opt to use staff volunteer days to promote cyber resilience to SMEs in they communities where they work and live.

Each of the nine centre works closely with its 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 fully funded solutions to local businesses while providing students with real-life work experience to encourage them to explore cyber as a rewarding career choice.

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.



Start your cyber resilience journey

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

- **Fully funded Security Awareness Training** for staff with little or no cyber security or technical knowledge.
- **One-to-One cyber resilience discussion** with someone from your regional Cyber Resilience Centre about your current cyber set up.
- **Police-Approved Resources, Guidance & Practical Tools** designed to help your business start its cyber resilience journey including resources from NCSC that are relevant to smaller organisations.
- **A range of fully funded technical services** specifically designed to help SME businesses and third-sector organisations.
- **Regional threat updates and scam alerts.**
- **A Monthly Newsletter** with details about webinars, roadshows, and regional business networking events.

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.

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 uses 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 has organised a series of briefing events delivered online by police officers working in the regional CRCs. The staff briefing is 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.

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 Cyber Resilience Centre for the South East, 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 Cyber Resilience Centre for the South East. 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.***

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 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 a call 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."

Sector-specific approach delivers meaningful impact in the North East

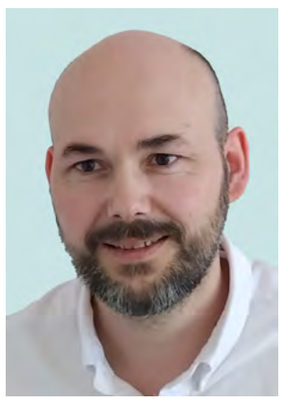
THE CYBER RESILIENCE CENTRE FOR NORTH EAST | YORKSHIRE | THE HUMBER

The CRC Network is committed to creating opportunities for businesses across key sectors to strengthen their cyber security posture.

By way of example, the Cyber Resilience Centre for the North East (NECRC) has recently been working in partnership with the Cleveland Local Resilience Forum, delivering fully funded cyber security assessments to small businesses in the adult social care sector. The initiative allows eligible organisations to access expert support at no cost, helping them identify vulnerabilities and take actionable steps to improve their security.

Local resilience forums (LRFs) are multi-agency partnerships comprising representatives from local public services, including the emergency services, local authorities, the NHS, the Environment Agency, and others.

Programmes like this demonstrate how targeted, sector-focused support can make a meaningful impact. By combining local partnerships with specialist expertise, we're able to reach organisations that might otherwise lack the time, budget or in-house knowledge to address growing cyber risks.



Stuart Marshall, Chief Emergency Planning Officer, LRF Manager, comments: *"During COVID-19, the critical role that the local care sector undertakes was made clear, as was the significant variation in social care providers' models from multi-nationals to small family-owned businesses.*

"While focusing on delivery of care, many small and medium-sized businesses lack the skills and knowledge that larger organisations rely on to maintain strong cyber security and awareness. Given this challenge, it was a natural decision to discuss the issue with the Cyber Resilience Centre for the North East. We wanted to explore the support they could provide within the sector while gaining a better understanding of the risks.

"The benefits are two-fold: an increase in the resilience among care providers and awareness of the work of the NECRC, but we also get a better understanding of the vulnerabilities and appetite for support within a critical sector."

Speaking about the partnership, NECRC Director, Steve Leach, said: "We are delighted to be working with Cleveland Local Resilience Forum, they are an established and recognised forum with access to the types of businesses and organisations we want to support. Working with them on this programme helps us to engage with adult care sector providers at scale.

"Every business and third sector organisation is a potential target for cybercriminals, so cyber security is everyone's responsibility. Working with established and trusted bodies enables us to engage with businesses that are difficult to reach and not be fully aware of the threats or the funded support that is available to them."

THE CYBER RESILIENCE CENTRE NETWORK

The Cyber Resilience Centre for the North East is one of nine CRCs throughout England and Wales that make up the CRC Network. We are happy to speak to any organisation, trade body or association about sector-specific campaigns to support SMEs and third sector organisations either regionally or nationally.

Shakespeare Birthplace Trust embraces cyber resilience

Shakespeare birthplace trust

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.

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 provide via Cyber PATH.

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, 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, Director at the Cyber Resilience Centre for the West Midlands, 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."

THE CYBER RESILIENCE CENTRE FOR THE WEST MIDLANDS

Cyber resilience delivered in the heart of the community...

DOROTHYPARKES Community Centre

Dorothy Parkes Centre in Smethwick, West Midlands, has a long and fascinating history dating back over 300 years to when Dorothy Parkes left £800 (equivalent to over £500,000 today) to build, amongst other things, a chapel, minister's house and a church school. Over the years, trustees have ensured the legacy continues to offer support to the local community via the Dorothy Parkes Centre, which opens its doors daily and provides people with a place of welcome and opportunity.

The centre is a busy and thriving hub, with over 40 scheduled group meetings every week and a packed calendar of other events, all of which keep the team extremely busy. In the long-established spirit of responsible stewardship, the centre's management team recently decided to review and improve their cyber resilience, something prompted by the increasing need for Cyber Essentials accreditation, particularly in tender situations.

In order to find out more, CEO Rob Bruce and a colleague attended a Cyber Security Masterclass breakfast in Sandwell, where they were made aware of the Cyber Resilience Centre for the West Midlands and the Cyber PATH programme. In turn, this led to a meeting with Cyber PATH team member Danielle Healy, who outlined the Cyber PATH programme and made recommendations about the services best suited to the needs of the centre. The two services they agreed on were Security Awareness Training and an Internal Vulnerability Assessment.

In October, five members of the team attended an online Security Awareness Training session, hosted by Cyber PATH Student Eli Bowen, all of whom found it interesting, insightful and highly beneficial in highlighting the things they could do for themselves to become more resilient. All of the attendees appreciated the tone, clarity, and pace of the session, as well as the fact they were given plenty of opportunity to ask questions throughout. Since the session, the five attendees have shared the messages with the broader team, including volunteers at the centre.

The second service opted for by Dorothy Parkes Centre was an Internal Vulnerability Assessment (IVA). An IVA looks at what a cybercriminal could see and what they could do if they were to gain access to an organisation's internal network. It involves plugging a small computer into your internal network and carrying out a scan and thorough review to identify any weaknesses, e.g. insecure WiFi networks and access controls or opportunities to steal sensitive data. If any weaknesses are found, we rate the risk that they pose to your organisation and advise you on the next steps you can take with your internal IT team or an external partner to address them.

Cyber PATH's Isaac Day undertook the assessment in October/November 2024 and submitted their findings to Rob and their external IT support providers in November. They followed up with a call to go through the report in detail.

Both Rob and the IT team appreciated the in-depth nature of the assessment, the explanations, and the recommendations, and all the fixes were implemented quickly by the team.

Speaking about the Cyber PATH sessions, Rob Bruce said: "Five members of our staff team attended the Security Awareness Training online, which was delivered by Savva and Eli, and we all found it very thought-provoking. It certainly raised our awareness in relation to cyber security, and there were some important links and hints that we will use going forward to ensure that we are more secure.

"We also learnt a lot from some of the real-life scenarios we looked at. The training was delivered at a good pace; it was interactive, allowed for short breaks, and provided plenty of time for questions. We also received a helpful handout.

"I think all businesses in all sectors should take up this training. I also think it should be rolled out in schools and colleges to ensure that everybody is aware of potential scams and the detrimental effect they can have."

Rob was quick to acknowledge the help and support he had from the Cyber PATH team and the Cyber Resilience Centre for the West Midlands. He strongly recommends speaking to your local Cyber Resilience Centre prior to seeking Cyber Essentials or Cyber Essentials Plus accreditation. In his words: "It was good preparation that makes us much more confident as we start our Cyber Essentials journey, I'd recommend it to all organisations as a fantastic starting point."

THE CYBER RESILIENCE CENTRE NETWORK

CYBER PATH™ POLICE & ACADEMIA TALENT HORIZONS

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






The effects of cybercrime can be far reaching so be sure to also let your peers, customers and supply chains know about us by directing them to our regional Centres.





THE CYBER RESILIENCE CENTRE FOR NORTH EAST | YORKSHIRE | THE HUMBER
nebrcentre.co.uk

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST
nwcrc.co.uk





THE CYBER RESILIENCE CENTRE FOR THE EAST MIDLANDS
emcrc.co.uk

THE CYBER RESILIENCE CENTRE FOR THE WEST MIDLANDS
wmcrc.co.uk

THE CYBER RESILIENCE CENTRE FOR THE EAST
ecrcentre.co.uk

THE CYBER RESILIENCE CENTRE FOR WALES
wcrcentre.co.uk




THE CYBER RESILIENCE CENTRE FOR LONDON
londoncrc.co.uk

THE CYBER RESILIENCE CENTRE FOR THE SOUTH WEST
swcrc.police.uk

THE CYBER RESILIENCE CENTRE FOR THE SOUTH EAST
secrc.police.uk



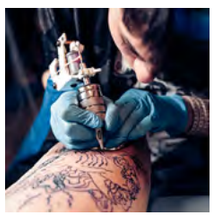







The Cyber Resilience Centre Network has a shared sole aim of helping SMEs increase their cyber awareness and resilience.

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.




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

Dedicated to local communities:

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

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) and The Cyber Resilience Centre Network (CRC Network) 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, large and small. The evening was a resounding success, with many local companies signalling their intent to join the Cyber Resilience Centre and start their journey towards better cyber resilience.

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. Invariably, these small business owners are time-poor and need to be focused on running their businesses. In many cases, they are not entirely 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.

"I'm delighted I can use my knowledge of the threats, and with the support of Sir Robert McAlpine and NCRCG, I can play a small part in helping local companies and charities by signposting them to a government-funded, police-led initiative where they will get proper support and guidance to trusted resources."

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: "It's been a pleasure working with Rachel and Andy at Sir Robert McAlpine; as National Ambassadors, they are genuinely engaged in supporting SMEs throughout the country. Their supply chain campaign has already helped hundreds of small businesses start a journey toward better cyber resilience.

"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."

Rachel is currently working on a series of online presentations and in-person workshops for her local community. We thank her for her commitment and dedication to the SME community.

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 aadded: *"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."

National Ambassador support for SME community

Our National Ambassador companies are some of the largest organisations in the UK and operate in a diverse range of sectors, from finance to construction and retail to professional services. However, they have one thing in common: they are committed to supporting the SME in becoming more cyber resilient.

Our National Ambassador Programme provides an opportunity for these organisations to join together with senior law enforcement officials and the government to inform national developments on cyber resilience and reduce the risk posed by cybercriminals.

The National Ambassadors all appreciate the critical need for a robust supply chain; however, they also understand the many challenges faced by SMEs in their respective supply chains. Often, they are unsure where to begin or what information to trust. For others, it may be a lack of awareness that is leaving them exposed to the ever-increasing threat of cyber attacks.

We are working closely with the National Ambassador companies to create supply chain campaigns that encourage their suppliers to join our free community by signing up for their regional Cyber Resilience Centre. In doing so, they will start a journey that will provide trusted guidance to government resources that will help better protect them against cyber attacks in the future.

SMEs need to accept that shortcomings in their cyber operations create possible weaknesses for all of the companies they deal with, both customers and their suppliers! Nobody wants to be the weakest link in any supply chain, so it is essential that all organisations, big or small, do what they can to raise awareness of the threats and provide relevant information and easy access to trusted support. That is why our National Ambassador companies are committed to running supply chain campaigns.

Aeronautics supplier begins a journey to better cyber resilience

THE CYBER RESILIENCE CENTRE FOR LONDON

The CRC Network often meets small businesses that have suffered cyber attacks. In most cases, these attacks occurred due to a vulnerability; they were not specifically targeted because of the business's sector, location, size, or trading activities.

It is essential to recognise that cybercriminals primarily target technical and human vulnerabilities, such as unpatched software, weak passwords, and phishing, rather than specific companies. This means that all organisations, regardless of size, are potential victims. However, cybercriminals often succeed with small businesses simply because they have limited cyber security resources. This, in turn, creates challenges for larger companies that rely on SMEs in their supply chains.

People often assume these SMEs are low-tech startups run by inexperienced owners, but that's not true. The Cyber Resilience Centre for London recently helped a small, well-established, and innovative business that develops advanced technology for the aeronautics industry. Their clients include many top global companies in aeroplane design and manufacturing.

The CEO clicked a link in an email she thought was from a customer. By the time she realised it was fake, the damage was already done. Malware had entered their systems, causing ongoing data corruption and hurting their ability to analyse information. The team tried to keep the business running as usual, and all of this was happening during an important period of growth. They didn't know what data had been lost or how to respond.

Soon after signing up with the London CRC, they received the standard one-to-one consultation call during which they disclosed the ongoing problem. We immediately guided them through the Report Fraud process and advised them to use the 0300 123 204 telephone service, given the urgency of their situation.

Following the immediate actions provided by Report Fraud Victim Services, we offered a further consultation to support them in becoming more resilient. We introduced them to the Cyber Action Toolkit, an NCSC online platform that provides step-by-step guidance specifically designed for SMEs with little or no internal cyber security resources.

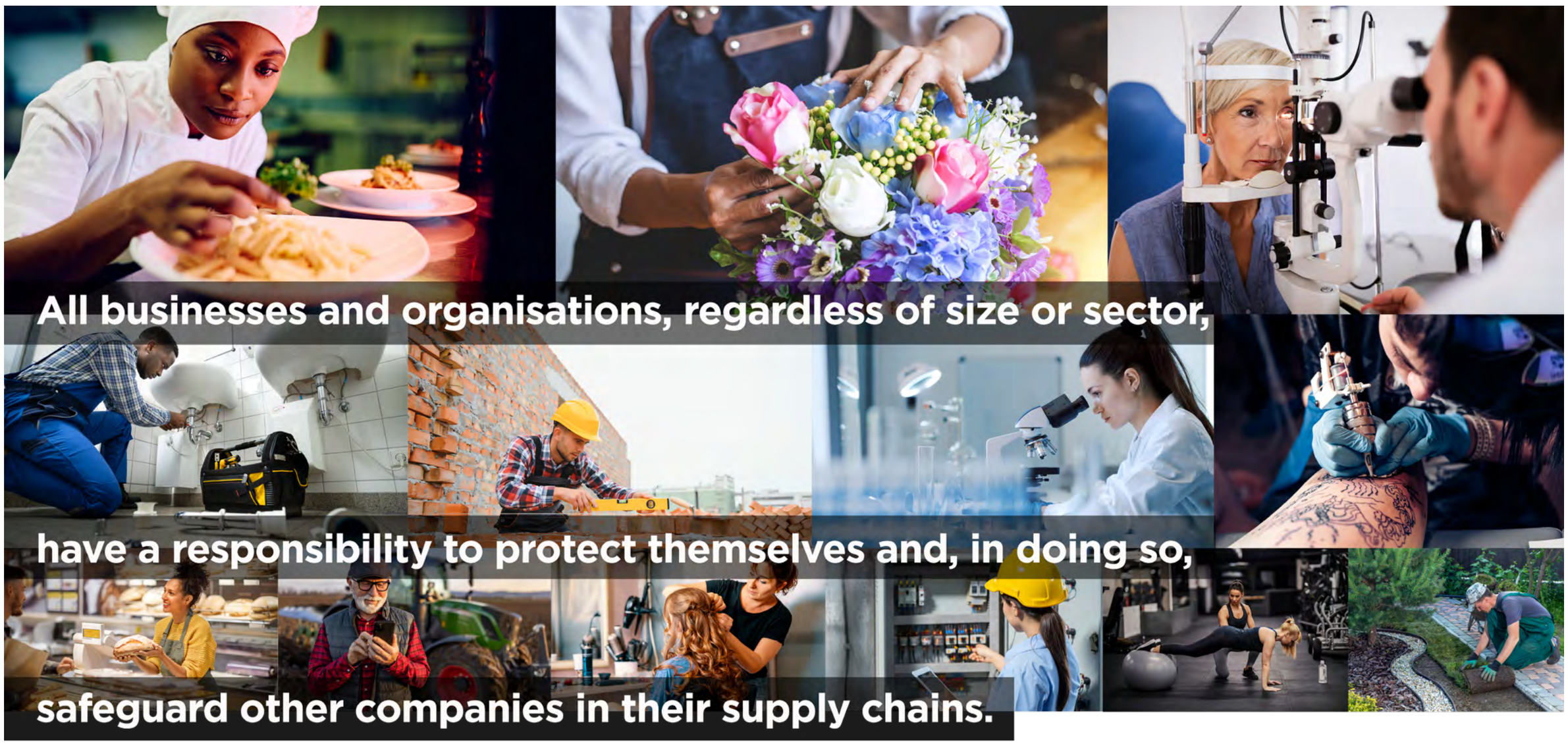
We also suggested our fully funded Cyber PATH Security Awareness Training for all their staff, which they were happy to accept. Since then, the company has become much more aware of cyber risks and has joined webinars hosted by the CRC Network.

Speaking to London CRC, the company's CEO said: "I thank you very much for your support, and for the time you have taken to teach me how to protect my business, and to report any cybercrime. As discussed, I already see the positive impact of the Cyber Resilience Centre on my business.

"I feel much better prepared to face and manage cyber attacks to keep my business safe. As soon as the remedial work is finished, I will contact Cyber PATH for further support".

Speaking about the incident, the Director at London CRC, Richard Morrison-Butcher commented: "It was great to be able to support the company, initially on their recovery journey with the help of Report Fraud, but also to be providing ongoing services that will make them more resilient in the future.

"This is an excellent example of how even sophisticated technology businesses can become victims of cyber attacks. Given the significant global organisations they work with, the potential damage could have been far-reaching. It serves as an important reminder that all businesses have a responsibility to protect themselves and those in their supply chain."



Are you ensuring you are not the weakest link in the supply chain?

In simple terms, every business is involved with at least two supply chains: the companies they buy from and the customers they sell to. Of course, for many companies, it is significantly more complex than this. Still, regardless of how complex or how many companies you deal with, one thing is sure: disruption in the supply chain will inevitably disrupt your operation.

Large organisations invest in supply chain management software or systems to ensure the smooth running of their business, but many smaller organisations find the cost prohibitive. Indeed, the majority of SMEs will have little, if any, in-house knowledge or dedicated personnel to manage their supply chain effectively. For the most part, they will tend to address supply chain issues on a reactive basis, responding to problems as they occur instead of proactively mitigating risks.

There is little argument that, despite its significance to all business operations, supply chain management could and should be much better, particularly in SME businesses.

SMEs traditionally focus on building strong relationships with reliable suppliers who understand their business, and they are often good at collaborating with larger companies that have established supply chain networks. It is also fair to note that software management tools are becoming more affordable while AI will inevitably make the task simpler, too.

However, while there appears to be a raised awareness among SMEs about the importance of the supply chain and better opportunities for smaller businesses to be much more proficient, there are also increasing threats, primarily in cyber.

The dramatic increase in cybercrime and cyber attacks in recent years has undoubtedly led to a much greater level of importance being focused on the supply chain and where the weak links may appear. Clearly, for many of the same reasons SMEs find it challenging to manage supply chains, they are equally exposed over their resilience to cyber-attacks. This weakness is a significant concern for larger organisations that invariably rely on multiple SMEs for products and services. If these smaller businesses are exposed to cyber attacks, it not only disrupts supplies but also potentially creates a weakness in the larger organisation's cyber defences!

So, all businesses, and third sector organisations, must accept that regardless of size, sector or location, they have a responsibility to protect themselves, which, in turn, helps protect all of the other businesses in their supply chains.

The Cyber Resilience Centre Network has a shared aim of helping SMEs increase their cyber awareness and resilience. By signing up with a regional Centre, you will be taking the first step on a journey to become more resilient. You will also receive access to fully funded services and access to trusted resources to help you become resilient.

Through the National Cyber Resilience Centre Group's National Ambassador programme, many of the country's leading companies are helping their respective supply chain partners to become more resilient through ground-breaking national campaigns. These companies are genuinely invested in their suppliers and want to ensure they support them in every possible way to become more aware of cyber threats and more resilient to them.

When you join your publicly funded regional centre, you are becoming part of a nationwide community that is committed to making the UK a more attractive place to work and invest in. More importantly, you will be taking positive steps to protect yourself and the companies you work with.

In this edition of The SME Guardian, we have highlighted just a few 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.

Hopefully, it has provided a useful insight to the work of the CRC Network and how the Cyber PATH programme is addressing the cyber talent pipeline crisis, by creating real-work experiences for the country's brightest students.