nationalcrcgroup.co.uk

THE SME GUARDIAN

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

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 free and affordable 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 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 cyber crime. 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.

Inside this edition...

What is the CRC Network?

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

PAGE 2

Trust embraces cyber resilience

West Midlands CRC and Cyber PATH deliver training to a long-established name!

PAGE 5

IFA really does see the value of advice

Find out why fmifa, the respected Buckinghamshire IFA appreciates the value of the Security Awareness Training.

PAGE 6

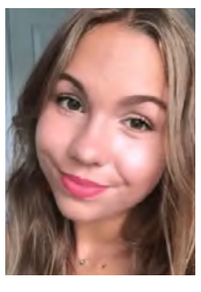
National Ambassador Chainalysis provides valuable training opportunity

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 7

The National Ambassadors supporting smaller organisations

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

The Cyber Resilience Centre Network (CRC Network) comprises nine centres across England and Wales 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 cyber criminals to their supply chains, customer bases, and the wider SME community.

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

Each 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 affordable 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

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. These are recognised nationally as Cyber Essentials Partners.

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.

Joining this publicly funded service is FREE and includes:

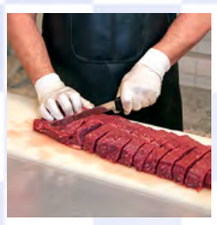
- **A free 30 minute review** with the centre's Head of Cyber and Innovation on your current cyber set up.
- **Access to free resources**, tools and guidance designed to help your business start its cyber security journey including resources from the National Cyber Security Centre.
- **A Cyber Toolkit -** 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.
- **Invites** to webinars, roadshows, and conferences.
- **A monthly newsletter** full of tips, tricks, and resources to help you tackle current cyber threats and trends.

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 BUSINESS RESILIENCE CENTRE FOR THE 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 EASTERN CYBER RESILIENCE CENTRE
ecrcentre.co.uk

THE CYBER RESILIENCE CENTRE FOR WALES
wcrcentre.co.uk




THE CYBER RESILIENCE CENTRE FOR LONDON
londoncrc.co.uk

THE SOUTH EAST CYBER RESILIENCE CENTRE
secrc.police.uk

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



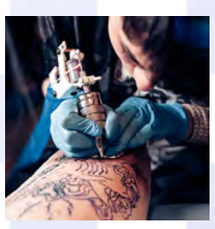







“*The Cyber Resilience Centre Network has a shared sole aim of helping SMEs increase their cyber awareness and resilience.*

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.

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

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.

REMOTE 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.

INDIVIDUAL 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 cyber criminals to target your business.

SECURITY POLICY REVIEW

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

CORPORATE INTERNET DISCOVERY

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.

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.

Cyber security investment leads to a business win

The Cyber Resilience Centre for Wales' First Step Web Assessment is a service that offers Welsh SMEs, charities and third-sector organisations the opportunity to review their online operations to ensure their cyber security is robust enough to withstand a cyber-attack.

Local business Wrexham Chauffeurs is an excellent example of a small Welsh-based organisation whose owner, Geth Thomas, wanted to take positive action in better understanding how his company's cyber security was fairing and what changes, if any, he needed to make. And so, through the WCRC's Cyber PATH team, he signed up for the First Step Web Assessment.

We asked Geth a few questions as to why he chose to do it, how it went and what outcomes he has experienced since doing it.

Q: What prompted you to do the First Step Web Assessment?

A: I wanted to engage with an external agency that could test my security to ensure that my data was safe. I'd had a recent discussion with an individual who I suspected could become vindictive. It was then that I first learned of the First Step Web Assessment, and so I reached out to the Cyber Resilience Centre for Wales.

Q: How useful did you find it to your business? And would you recommend it to other companies like yours?

A: The assessment was very useful. It found a small issue that I subsequently arranged to have patched within two to three business days. Yes, I would recommend it to other companies; it is up to each company to assess and mitigate what they perceive their exposure to risk is, but for a low cost, the Cyber PATH First Step Web Assessment service does provide peace of mind.

Q: You were able to use the assessment evidence to secure a new client. Please can you tell us more about that?

A: A new client contacted us regarding pricing for a service; they told us from the get-go that there would be other suppliers competing for the same work. Because I was able to demonstrate that I'd been through this assessment and passed, it separated me from the other suppliers - and I successfully secured the work. In fact, that client is now a repeat customer.

Q: How aware as a business are you generally when it comes to cyber security?

A: My clients cover multi-national corporations and private individuals, so it's imperative that my data is always secure, and we constantly review our security to ensure that we remain industry-leading.

Q: How proactive, in your opinion, are Welsh small businesses when it comes to their cyber security?

A: I think the Welsh SME community could still do so much more when it comes to improving their cyber security protection. Staying one step ahead of the criminals is key and taking measures, like accessing the various services the WCRC offers, is a great starting point.

THE CYBER RESILIENCE CENTRE FOR WALES

Q: Have you accessed any other services on offer through Cyber PATH?

A: No - I've not yet accessed any other services on offer through Cyber PATH, but we are always looking for what we can do next to remain one step ahead of the criminals, so I think we probably will utilise other services soon.

Q: What advice would you give other small businesses when it comes to getting better protected against cybercrime?

A: Contact the Cyber Resilience Centre for Wales and get assessed so that you have peace of mind that your business is protected. And, if it does show up any issues, deal with them as soon as possible. Doing nothing leaves you vulnerable to attack, the consequences of which could destroy your business overnight.

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, 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."

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 Interval Vulnerability Assessment (IVA). An IVA looks at what a cyber criminal 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."

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.***

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.

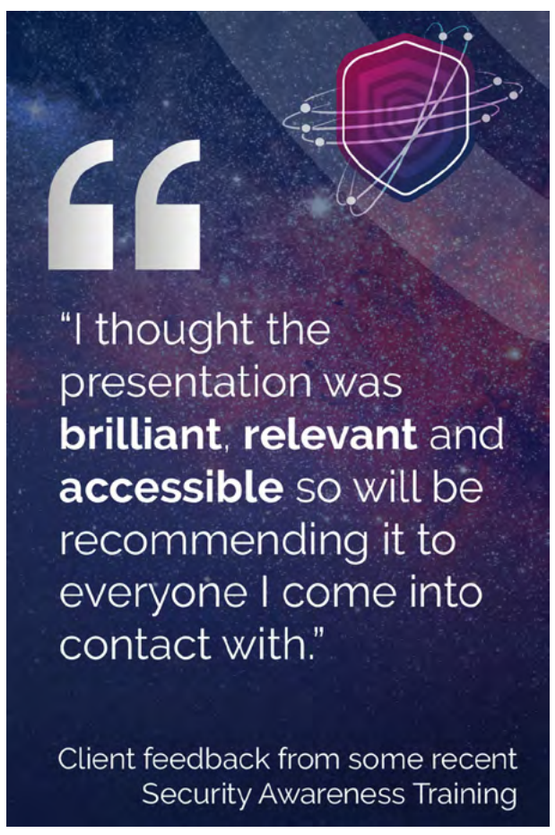
Cybercrime is fluid; it keeps changing and advancing as technology evolves. That is why we are bringing in the brightest and the best young people from academia to develop a second-to-none talent pipeline both for policing and the private sector.

The CRC Network havs 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 are 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 cybersecurity 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 cybersecurity 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.

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 and third-sector communities 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.

SME businesses and third-sector organisations 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.

West Midlands School fortifies its internal network

Cyber PATH student Dominic Johns, while studying an MSc in Computer Systems Security at the University of South Wales, carried out an Internal Vulnerability Assessment (IVA) for a school in the West Midlands.

An IVA looks at what a cybercriminal could see and do if they were to gain access to an organisation's internal network. In this interview with Dominic, he explains more about the service, what it taught him and how it benefits organisations.

This is the first time you have carried out an IVA. How did you feel about delivering the service?

Both excited and nervous. More so excited because I knew I would have the support of Cyber PATH supervisors, who would be on hand if there was anything I wasn't entirely sure about. Overall, I was confident it would enable me to build important skills I need for my CV.

Was the training you received from your Cyber PATH supervisors effective?

Absolutely! They created a comfortable environment for me to learn, with helpful insights at every stage, but also let me push myself. They were always happy to accommodate any requests I had to make sure I could balance my workload and university studies.

How does this service benefit organisations like the school you were working with?

An IVA identifies critical vulnerabilities, as well as more technical issues, within an organisation's everyday systems. It breaks down very technical problems and issues into digestible chunks.

Most importantly, I would say an IVA gives organisations peace of mind – they know that experts have reviewed their systems and can rest assured that any risks that may have previously gone unnoticed have been identified. They also receive accessible and practical guidance on where their cyber security can be improved.

How did the experience improve your understanding of cyber security within organisations?

It enabled me to see how common policies and security measures are implemented in the real world, as opposed to in a textbook example. For a student, this kind of firsthand insight into how organisations view and manage their cyber security is both unique and invaluable.

> *The genuine kindness and passion the Cyber PATH supervisors show towards students rival the most devoted teachers and lecturers*

It also helped me to build my confidence in delivering services and learn more about what it's like to work in a cyber security role.

What would you say to a university student who is thinking about applying to the Cyber PATH programme?

This is the opportunity of a lifetime. From developing your cyber security knowledge and skills to building your network to directly supporting SMEs, the opportunities the programme offers are exceptional.

The genuine kindness and passion the Cyber PATH supervisors show towards students rival the most devoted teachers and lecturers – they really want to see you thrive and make the most of the experience. I would absolutely recommend joining Cyber PATH!

Protecting our Nation's charities from the threat of cybercrime

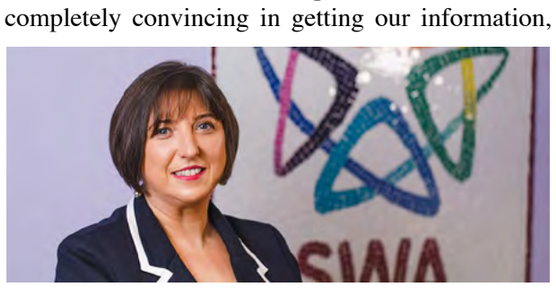
Every organisation in this country is potentially a target for cyber criminals, including our nation's charities, which are providing vital and often life-changing support to the end users and communities they serve. There are over 169,000 charities in the UK which could be impacted by cybercrime. It is, therefore, essential that they have a robust cyber posture and appropriate cyber protections in place to safeguard their ability, and the ability of those in their supply chains, to continue delivering this crucial work.

The CRC network is set up to deliver precisely the kind of support and advice that charities and third-sector organisations need to strengthen their cyber resilience. Experts at each centre deliver affordable, high-quality and easy-to-understand guidance to small and medium-sized charities and businesses in their localities. Importantly, these specialists are aware of threats specific to the sector and are well-versed in the business demographics of the area.

Sara Ward, Executive Officer at Black Country Women's Aid in the West Midlands, whose team received security awareness training from the West Midlands Cyber Resilience Centre, said:

"The training was excellent and led by cyber security experts who had the most up-to-date and relevant information. It was informative and related to real-life examples that enabled us to gain a greater awareness of this insidious crime. The trainers created a safe space for us to be honest, share our experiences, and understand the ease with which our information could be obtained.

"At times, we have felt like fools at the ways criminals have charmed, persuaded and been completely convincing in getting our information, but we are not fools; we were just not as aware of the lengths that they will go to. Once they have our information, we know how difficult it is to get it back or have control over it. I can't explain to you how



> *The trainers created a safe space for us to be honest, share our experiences and understand the ease with which our information can be obtained.*

strong some of the expert's real-life examples were and how relevant they were to us. They understood where we are as a charity and how we fit into the cybercrime equation. The training has definitely influenced a culture change across our organisation. We all went away with a greater understanding of our responsibilities around cyber security. The information we hold about our clients and ourselves is precious – we know that now more than ever. It was simply excellent!"

Fiona Bail, Detective Chief Inspector and National Cyber PATH Lead at NCRCG, said: "Cybercrime is something that impacts small and large charities, businesses and organisations across the country – it is not limited to one size of the organisation, one location or one sector. Our nation's charities are doing crucial work for the communities they operate in, and, as such, we want to do what we can to help them be safe and secure from the threat of cybercrime – allowing them to continue to focus on what they do best. At NCRCG and across our CRC network, we are committed to strengthening the cyber resilience of charities and third sector organisations, ensuring they have access to the affordable, high-quality and straightforward advice they need."

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 cybersecurity 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.

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!

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.

CYBER ESSENTIALS CYBER ESSENTIALS PLUS

www.ncsc.gov.uk/cyberessentials

Immigration consultancy begins their Cyber Essentials journey

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

TWO THE WESTWOOD ORGANISATION

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.

THE SOUTH EAST CYBER RESILIENCE CENTRE

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.

Cultivating relationships in the South East

It's always great to receive positive feedback from members who have made use of a Cyber PATH service. However, we're doubly delighted to hear about a satisfied client who has used Cyber PATH services twice, both times with a positive outcome.

Kebur Garden Materials has been working with our Cyber PATH team via the South East Cyber Resilience Centre.

Kebur Garden Materials is a family-run landscaping supplies business established over sixty-five years ago. Clearly, Kebur cares about customer service and the customer experience; not only do they offer everything you'd need for any size of garden project, but they can also provide impressive garden landscaping services. Their website is extensive, with a vast range of high-quality products available to buy online.

Undoubtedly, reputation matters to Kebur, and a significant portion of what they offer is reliant on a trusted web presence. It is also evident that the team at Kebur take their responsibility to protect their website very seriously; therefore, they are proactive in becoming cyber resilient and doing what they can to ensure a great user experience while ensuring the site is safe for customers to use. With this in mind, they asked our Cyber PATH team to conduct a First Step Web Assessment (FSWA) exercise on their website. FSWA is a light-touch assessment of a website's security, which highlights the most pressing weaknesses, for example, sensitive data exposure or vulnerable and outdated components. Via the South East Cyber Resilience Centre, our Cyber PATH team completed the assessment and presented their findings in an easy-to-understand format.

Referring to the service, Jo Holtom, Business Partner, Marketing and Change at Kebur, emailed us to say: "I just wanted to let you know how valuable we found the FSWA. It was a truly revealing exercise, and I've already had a colleague report a suspicious email to me this morning."

Having completed the FSWA, Kebur could also see the value in training the staff to be more aware of the threats posed by cybercriminals and what steps they could take to become more resilient, so they booked one of our Cyber Security Training courses. This service 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.

Following the course, here's what Jo had to say about the service:

"We wouldn't hesitate to recommend the Cyber Security Awareness training from SECRC. We covered a lot of material in the time available, and the content was delivered at a good pace in a really engaging way. There was plenty for all our team to relate to, whatever their roles, and learning that could benefit them in both their professional and personal lives."

Chris White, Director of SECRC, also added: "We have built an excellent relationship with the team at Kebur Garden Materials; they have a very responsible attitude to cyber and appreciate the need to protect their online assets and to provide training for their team.

"We are delighted that they view SECRC as their 'go to' place for cyber information, and we look forward to working with them as they continue their cyber resilience journey".

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.