TRANSFORM

ISSUE 36

In print and online interactive publication | www.iese.org.uk

Download free report showing vulnerabilities

Find out the results of a passive scan on your authority

Why organisations need to be supply chain savvy

Understand cyber risk and the supply chain

Also inside:

- **Register for iESE cyber awareness conference**
- **Latest news from the Cyber Centre of Excellence**
- **Learn about new cutting-edge cyber protection tools**
- **Latest Cyber Centre of Excellence pilot programmes**

iese
The public sector transformation partner

CONTENTS

EDITORIAL CONTACTS

TRANSFORM IS PRODUCED BY: iESE
www.iese.org.uk
Email: enquiries@iese.org.uk @iESELtd

CREDITS: Designed by SMK Design (Aldershot)
Editorial by Vicki Arnstein

Views expressed within are those of the iESE editorial team. iESE Transform is distributed to companies and individuals with an interest in reviewing, remodelling and reinventing public services.

INTRODUCTION

Capita breach highlights supply chain cyber risk

A recent cyber breach of Capita, a company which provides business process services to a range of organisations including local government, has highlighted the importance of carrying out due diligence on the cyber security of suppliers.

Dr Andrew Larner, Chief Executive

@LaverdaJota

According to a statement released by Capita, unauthorised access was gained on or around the 22 March and discovered on 31 March. While it stated that only around four per cent of its server estate was affected, data belonging to several local government organisations were involved. Colchester City Council wrote to residents and customers to notify them historical data relating to benefits had been compromised. Adur and Worthing Councils also issued a statement which noted they had been informed about the breach by Capita but were assured it had not involved personal data. However, it said its own investigation had found the affected files had contained data belonging to around 100 residents, resulting in extreme unhappiness with both the breach and Capita's failure to provide accurate and swift information.

The incident shows the importance of carrying out due diligence on the cyber security practices of all suppliers, regardless of how well established they are. It also highlights the need to ensure your own systems are secure to limit the chances of a cyber-attack spreading between a breached company and your own organisation.

The CCoE is well placed to advise how to best protect cyber security, including through the supply chain. Our aim is that our ongoing work and mission will help minimise the future occurrences of these attacks which can affect the operation of public services and residents' confidence in the ability to serve them safely.

This edition of Transform Magazine is a whistle-stop tour of what the CCoE has been up to in recent months, we hope you enjoy, don't hesitate to get in touch with us at enquiries@ccoe.org.uk.

iESE CONFERENCE

Registration open for iESE Conference 2023

iese23
CONFERENCE
Wired for Theft: The State of Play

Registration is open for the upcoming iESE Conference which will focus on practical steps local authority officers and members can take to boost their cyber security at home and work.

The conference, entitled Wired for Theft: The State of Play, is taking place in Eastbourne on 22 November. The day will be packed with useful, practical and easy-to-understand cyber advice with some fun twists which are not being disclosed in advance!

Annabelle Atkin, Chief Operations Officer at iESE, said the sessions would be aimed at senior officers and members looking to increase their awareness and understanding of cyber security threats and solutions rather than IT specialists. Spaces are free but limited and will be allocated on a first-come, first-served basis. ***"The conference will focus on practical examples of how to combat the real and immediate risks being faced by local government, both as direct targets and incidental collateral damage. We will outline practical and clear steps on what officers and members can do to better-protect themselves at work, at home and on the go,"*** she said.

The sessions will cover a wide range of issues, including: an outline of the current cyber landscape and global threats, the national local authority position combatting cyber cyber-attacks, introduction to the CCoE, an easy guide to what protection is needed for your devices, endpoints, servers, and operational technology, and how to be safe at home. In the afternoon, six additional sessions will be available, with delegates able to choose three to attend. These will be safe for councillors or safe in the office, safe for the community or safe for communications and safe for partners and local businesses or safe for the supply chain.

Another session will showcase recent CCoE pilot projects (see page 8), with representatives from Merthyr Tydfil County Borough Council, South Staffordshire Council, several parish councils, and local businesses answering questions about their experiences.

Find out more about the conference, including who will be speaking, what sessions will be included and who will be exhibiting in our latest blog here: www.ccoe.org.uk/blog/registration-open-for-the-iese-conference-2023

- **To book a place at the conference visit: www.iese.org.uk/conference-2023**

CCoE gathers momentum at prestigious events

The Cyber Centre of Excellence (CCoE) has been created to help all organisations across the UK achieve military-grade cyber security at high street prices. With its mission of making the UK the safest place to live, work and play online, the CCoE has already attended a wide range of events to spread the word and start achieving this aim.

SOCITM Top Talent Programme

The CCoE recently sponsored the SOCITM Top Talent London 2023 leadership programme, the first two days of which took place in April in London, with a further two days in June in Brighton. Delegates on the four-day programme with SOCITM, the society for innovation, technology, and modernisation for public service professionals, were given a six-stage fictional incident designed by CCoE Convenor Kurtis Toy and asked to explore the ongoing ramifications and impact on the fictional local authority's reputation and ability to keep delivering public services. Groups of delegates worked together and then presented their strategies and findings at the SOCITM President's Conference.

The scenario the delegates were given was based on a conceivable security breach, the likes of which have taken place in several local authorities:

1) **A trojan ransomware has infected all machines.** Everything needs to be shut down and no one has access to anything held on the network.

2) **A vulnerable adult is missing.** The police want information about this person which is stored on the inaccessible local authority network.

3) **The press are asking for updates.** It has become clear personal data has been breached and the vulnerable adult is still missing.

4) **A backup has failed because this was also infected.** Other stakeholders are asking questions.

5) **An older back up from 12 months ago has been installed from a previous system.** Data on the vulnerable adult is available. Critical components updated in the last year are not available in this update.

6) **The senior management and cabinet members need to be informed that the previous 12 months of data cannot be recovered.** Stakeholders have asked whether a ransom should be paid and about the ramifications of doing this or not. The vulnerable person has been found, however the out-of-date data meant this was delayed and the local authority is now under scrutiny for how this was managed.

Toy, who helped judge the presentations and is currently collating the information and solutions devised to provide recommendations for local government on how to best prepare for such incidents, said he enjoyed working with the cohort: ***"The scenario was designed to represent what unfortunately could be a realistic attack and how it could potentially unfold. The solutions and issues identified by the cohort could help address the gaps in public sector cyber resilience and how we deal with such events in the future."***

Other events

DCN webinar

The CCoE hosted a webinar for the District Councils' Network in June. Five members of the CCoE's high-profile Advisory Board spoke during the webinar hosted by CCoE Convenor Kurtis Toy. Delegates heard from Major General Martin Smith, managing director of CyberPrism, Barrister Sandip Patel KC FCIArb, Irene Coyle, Chief Operating Officer at OSP Cyber Academy and Councillor David Tutt and Dr Andrew Larner, Chairman and Chief Executive of iESE respectively. In the session the speakers covered a wide range of topics including: the global to local position, prosecuting after an attack and key legal defences an organisation needs, an overview of the current CCoE pilot programmes and how local councils can benefit from them and the importance of training your workforce in cyber security.

- **To watch the recording of the DCN webinar, please contact Annabelle at annabelle.atkin@iese.org.uk**
- **Read more about the CCoE pilot programmes on page 8 and about supply chain cyber training courses on page 7.**

LGA Conference

The CCoE held an exhibition stand at the Local Government Association Conference in July. Members of the CCoE were on hand to inform local authorities about the passive scan carried out on all 382 local authorities on their public-facing information found online and to share results as requested by individual councils. Annabelle Atkin, Chief Operations Officer at CCoE partner iESE, said the results of the reports had been well received.

- **Find out more about the passive scan on page 6.**

Senior Leaders Cyber Summit

The Aberdeen Cyber Summit took place at the end of August. Organised by CCoE partner OSP Cyber Academy, the event aimed to discuss and agree practical strategic cybersecurity and resilience solutions, at national and enterprise level, to address the ever-evolving threat landscape affecting senior business leaders.

The event was attended by senior leaders with responsibility for cyber security. Speakers included high-profile figures from the worlds of cyber, technology, national security, business and public services from the UK, US and around the world.

CCoE detects cutting-edge cyber protection

One of the Cyber Centre of Excellence (CCoE) aims is to find and bring cutting-edge cyber security solutions to the wider market, making military-grade protection available to all organisations through collective purchasing power.

The cyber security market is crowded, with many vendors making similar claims. To help officers and members secure the best protection, the CCoE Advisory Board continually reviews and assesses new cyber security providers and tools on the market with the aim of raising awareness of these best-in-class solutions and offering access to them through preferential rates. Since the CCoE launch, a few providers have been identified as offering game-changing solutions for cyber security: Blackwired, MessageMatrix and FractalScan Surface.

Blackwired

Blackwired is a next-generation threat intelligence company whose flagship offering Zero Day Live (ZDL) takes a fundamentally different approach to traditional detect and respond solutions. While anti-virus protection can stop known threats, zero-day attacks are new and unknown and therefore can breach security protection unseen, often resulting in devastating destruction, high recovery costs and extended business interruption.

ZDL makes what is intentionally hidden in the dark web, open, indexed, and searchable through a combination of machine learning and input from specialised analysts. The intelligence provided by Blackwired to its customers, including governments, law enforcement agencies, global corporations, and providers of critical infrastructure, takes clients out of the zero-day cyber-attack victim pool. It does not consume, repackage, or replay secondary intelligence, instead it is a primary source of precision anticipatory intelligence on cyber weapons (Zero Days and Malware), and adversaries.

The orchestration of prevention instructions to security infrastructures is made by unsupervised machine learning AI on the day of detection. This automated operationalisation of precision intelligence means the enterprise is always protected against the latest cyberattack threats found, days, weeks, and even months ahead of the Information Security Industry, Security Operations Centres, and the release of patches and upgrades. Enterprise leadership (the CRO, CISO, CEO) can report that they have taken positive action to mitigate their cyber threat risk and produce evidence to positively confirm it.

Customers have been afforded prevention from attacks by Anonymous Sudan, Cl0P, Lockbit, Blackcat, and supply attacks such as the MOVEit MFT Service platform. The intelligence is anticipatory and refreshes in near real-time as the cyber battle develops, it never sleeps and can fully automate prevention against severe threat risks, including ransomware and extortion.

The principal co-founders of Blackwired have decades of experience in the fields of clandestine cyber intelligence operations, leading-edge sector and government security consulting, with the company rapidly establishing itself as the lead player in Predictive and Preventative Threat intelligence. Blackwired solutions are non-intrusive, require no access or upload of customer data at all, and are delivered in seamless process of feed delivery of Zero Day Live intelligence via secure APIs. Blackwired monitors and manages the intelligence feed flows to optimise the efficacy of threat risk prevention, and meet the enterprise capability to consume the feeds in terms of operational capacity and cadence.

The company is pleased to have joined up with the CCoE to help extend the level of protection for UK public bodies and other CCoE organisations. ***"In the cyber war, attackers are assaulting our organisations, government bodies, healthcare systems with cyber weapons that are learning machines and industrial platforms. At any time, the cyberattack threat risk profile can dynamically change, yet our cyber defences do not dynamically change to counter the attacks and prevent that risk, leaving us as an exposed potential victim. At Blackwired we believe that all cyber defences must be intelligence-led and directly orchestrated machine-to-machine, only in this way we can draw level with the adversarial considerable advantages,"*** said Iain Johnston, managing director at Blackwired.

UK public bodies have fallen victim to cyberattacks in recent times, despite increased spending on cyber security assets and personnel. Operations in Environmental Protection, the National Health Service, and Local Government have been damaged, and in some cases devastated. ***"In many of these cases Blackwired's ZDL orchestration would have prevented these attacks, days or weeks, ahead of these events, saving a vast amount of cost, damage to mission, and reputation,"*** added Johnston, ***"We are excited to partner with the CCoE to help protect the public sector and other organisations that would not normally have ready access to cutting-edge technologies such as ZDL."***

• To find out more visit: http://blackwired.com or contact enquires@ccoe.org.uk

FractalScan Surface

FractalScan Surface is an attack surface management tool which scans the Internet to look for misconfigurations, security vulnerabilities and exposed data to give organisations a real-time report of their security risks and likelihood of being attacked. Knowing where these vulnerabilities are allows these potential gateways into the organisation to be fixed before they are found by cyber criminals.

Rob Stemp, CEO at Red Maple Technologies, the company which offers FractalScan Surface, said organisations could purchase the service to scan for vulnerabilities daily, weekly, or monthly. The company has partnered with the Cyber Centre of Excellence (CCoE) to give reduced rates for local authorities and other CCoE members.

Besides scanning for an organisation's own risks, FractalScan Surface can also be used to check a vendor's security posture to assess potential supply chain vulnerabilities (see page 7 for an article on supply chain risk). Doing so is completely legal as the passive scan only accesses Open Source information visible to anyone online.

"New risks and vulnerabilities emerge every day. The fundamental issue FractalScan is finding is mostly either badly configured services or out of data software that has vulnerabilities," explained Stemp, ***"Things change all the time. A configuration change might be made by mistake, or a planned configuration change might have an unintended consequence, and you would want to know about that as early as possible. New vulnerabilities are discovered every day, but you don't know they exist until you go looking."***

For example, Stemp explained that FractalScan regularly detects instances where cloud storage or administration pages for Content Management Systems have been made publicly available accidently or due to a software configuration. The scan can also check the email settings of an organisation, which if set optimally can massively reduce spam and phishing emails.

When a scan takes place, the organisation also receives an overall rating of between 1 and 5, where 5 is the gold standard. ***"A level 5 is aspirational but doable and with some effort any organisation can get there. If you score 4 or a 5 you are not very likely to get hacked. A level 3 they are starting to look a little bit risky but with hopefully not too much work required to get to 4. Unfortunately, at level 1 they are very likely to get hacked quickly,"*** he explained.

In partnership with the CCoE a one-off FractalScan Surface report was recently produced for all 382 councils in the UK (see page 6 for more information). ***"Now there is a very large and powerful data set that gives a nationwide view of cyber security and risk for every local authority in the UK and hopefully that will give the national bodies the information they need to make decisions around priorities and triage, where to put the funding and also where common issues might have a common solution,"*** Stemp explained, ***"The CCoE has the remit to help local authorities using this data and the local authorities can also now buy a subscription to FractalScan through the CCoE and get scanning daily, weekly or monthly. Knowing the risks is important, but being able to take those actions through to resolution is the critical bit."***

Besides local authorities, any organisation can use and benefit from FractalScan Surface, including other public sector bodies, small businesses, and schools. ***"We want to help every small business and government organisation in the UK and have a desire to improve cyber security at a national level,"*** he added.

The company behind FractalScan Surface, Red Maple Technologies, offers a range of other solutions to help protect organisations against cyber security threats, with the founders and majority of its staff coming from an ex-government national security and defence background.

• To find out more about FractalScan Surface visit: https://fractalscan.com or email enquiries@ccoe.org.uk

MessageMatrix

WhatsApp is the most-used mobile messaging app worldwide with an estimated two billion active users. With most clients and colleagues using the platform, conducting business matters over WhatsApp is tempting, however doing so may expose an organisation to multiple security risks.

With bulging email inboxes and the general expectation of instant responses it is hardly surprising many employees take to WhatsApp for work purposes. While WhatsApp uses end-to-end encryption, the platform still exposes an organisation and its employees to risks. For example, there is a possibility the app could be hacked whilst using public wi-fi networks or being targeted by or forwarded messages through human error containing malware which could penetrate a mobile device and steal or corrupt data. There is also the risk of information being widely shared and passed on to unintended recipients and of sensitive business information being held on private channels which are lost if the employee leaves.

A Government department recently found itself being reprimanded by the Information Commissioner's Office (ICO) for its use of private messaging channels, including WhatsApp, and the CCoE is aware that some councils are now moving to ban the use of this popular messaging platform due to security concerns. In the US, several major organisations have recently been fined large sums for using the platform due to lack of compliance with industry record-keeping rules.

An ICO report in 2021 called on Government to review the use of private correspondence channels after they were found to be used by Government ministers during the pandemic. The report highlighted the risk of sensitive information being held on outside servers and the related risk of inadequate data security. John Edwards, the UK Information Commissioner, said: ***"Public officials should be able to show their workings, for both record keeping purposes and to maintain public confidence."***

The reprimand issued by the ICO to the Department of Health and Social Care stated that the department and other public bodies should not send information containing personal data using private communication channels due to lack of compliance with the General Data Protection Regulation and the Data Protection Act.

Aware of these risks and of the temptation to use private messaging for ease and speed, one of the tools the CCoE is offering preferential rates for through its combined purchasing is an innovative solution called MessageMatrix.

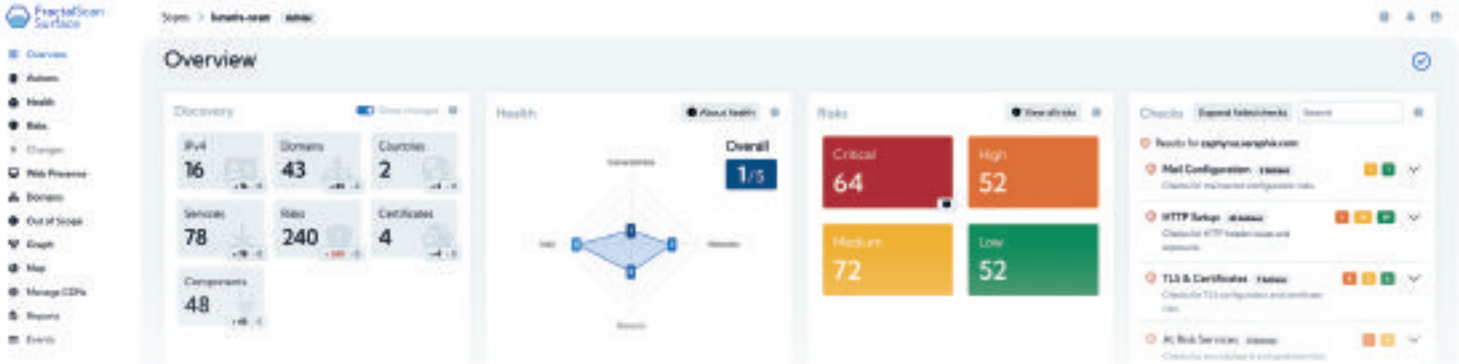
The platform takes WhatsApp and SMS messaging and wraps it in a secure platform which allows employees to message clients through these applications without comprising their own or the organisation's security. Beyond offering a secure way to interact and store sensitive information, staff members can bring colleagues into the conversation without surrendering their contact details. In addition, if a staff member leaves the organisation, the data remains in the secure platform to enable other colleagues to take forward relevant projects. Understanding data security is key, MessageMatrix has partnered with Glasswall, a company which enables ultra-secure document sharing. Users can also voice and video call through the platform.

"The indisputable fact is that people are using WhatsApp in their professional as well as their personal lives because it convenient and faster than sending an email which might not be responded to quickly. This is problematic for them and their employers. It means there is communication which cannot be captured, monitored, or audited for meeting the standards of the organisation," explained Douglas Orr, Founder and CEO of MessageMatrix, ***"There is a fundamental desire to provide a service over WhatsApp and that conflicts with the tools organisations currently have. MessageMatrix allows us to bring the best of an organisation's people and processes to a client without compromising the security, privacy and control of that process."***

Using the example of a social care client, Orr explains how using MessageMatrix might benefit the client whilst keeping their personal information and the details of staff secure. ***"You know that no matter how little they have left in the world, most clients probably still have a mobile phone with WhatsApp installed. Through this you can facilitate services and give them a case worker or team of case workers. They may have various issues, such as needing emergency shelter, and through the platform you can add someone from this team to the conversation, or even colleagues from partner organisations, such as charities. The whole backstory is there to see, they don't need retell the whole story,"*** he explained. Multiple switchboards can be created for different services within an organisation, such as council tax, parking fines and benefits, for example.

"The world we are trying to enable is engagement with controlled security. We think the CCoE is a very valuable organisation which can co-ordinate the purchasing of innovative technology such as MessageMatrix which might otherwise be out of reach of public services."

• For more information or for a demonstration of MessageMatrix visit www.messagematrix.io or contact enquiries@ccoe.org.uk



Download free report on online vulnerabilities

Local authorities are being encouraged to download a free report highlighting potential routes into their organisation which could leave them open to cyber-attack.

A passive scan recently carried out by the Cyber Centre of Excellence (CCoE) on all 382 UK councils using the FractalScan Surface tool from Red Maple Technologies is now available for each local authority to download. The attack surface management tool scans the Internet to look for misconfigurations, security vulnerabilities and exposed data. Any Open Source information the tool finds could be seen by anyone online, including hackers.

The deep scan uses a domain name or IP address to discover an organisation's online infrastructure, assets, and shadow IT. Scores are generated in four areas, with each area receiving a score between 1 and 5. On this scale, 5 is classed as excellent and a 1 would place an organisation as being very vulnerable to attack. Rather than taking an average across the four elements, an organisation receives the lowest score as their overall score, so they could score a 5 in three areas, a 1 in one element and be scored a 1 overall.

"The key caveat is that the scores do not tell us how cyber secure an organisation is, it just denotes on this one metric how secure they are from an outsider looking in," explained Kurtis Toy, vCISO and Convenor of the CCoE, ***"They could have vulnerabilities relating to legacy equipment that they are not worried about because they have it detached, for example, and there could be other protections behind the scenes that they have focused on. The flip could also be true, they might have a high score, but be vulnerable in other areas not considered by the report."*** However, the fact remains that any vulnerabilities found in a passive scan would potentially be a route into an organisation and what potential hackers are seeking: ***"The elements looked at in the passive scan would be the first point of consideration for a hacker looking to get into an organisation. If they wanted to take down an organisation specifically, these vulnerabilities would be their first step to working out how to get in,"*** Toy added.

At the time of writing, 106 local authorities had downloaded their reports. The feedback has been universally excellent with the reports being well received: ***"We haven't had any negative feedback. The only feedback we have had is that the reports are valuable, with some of those downloading them asking for more details and a full report. What we are giving them is a subset of results due to the huge volume of data the scans have generated."***

The report received by each authority gives an overview of the council compared with their region, and they get a total number of vulnerabilities and a comparison to where that sits for the UK. ***"The report also highlights the top twenty vulnerabilities for the local authority and top twenty actions to address them – importantly we are not just giving them a list of where they are vulnerable and leaving it there. Although we would encourage the local authorities to sort these vulnerabilities themselves, if they are struggling, they can contact the CCoE for help on specific things,"*** he added.

The reports are not intended to blame or shame and the CCoE will not be publishing any related league tables. Besides providing local authorities with valuable data, the scan will also allow the CCoE to look at where there are common issues that could be addressed collectively. ***"It has been carried out to inform and help the CCoE develop the right tools to move things forward in a more informed manner,"*** Toy said.

Vulnerabilities frequently found included badly configured services or out of data software. They might also include forgotten servers and neglected websites affected by mergers or organisational changes. Often configuration changes are made which accidently make information available online without an organisation's knowledge. Quickly finding these and fixing the issue before it is found by attackers offers another line of defence in an organisation's arsenal. Preferential rates to FractalScan Surface are now available through the CCoE which include daily, weekly, or monthly scanning.

"If local authorities find the scan report useful, they can also secure discounted rates for FractalScan Surface through the CCoE. For more information about how to use passive scanning as part of your defense in depth then open the conversation with CCoE," added Toy.

• Request a copy of your council's report by contacting enquiries@ccoe.org.uk.

• Other companies and organisations interested in learning more about FractalScan Surface or subscribing to the service with preferential rates secured by the CCoE can find out more by emailing: enquiries@ccoe.org.uk

• Find out more about FractalScan Surface: https://fractalscan.com or see page 5.

How to avoid a chain reaction

The threat from supply chain cyber-attack is increasing as cyber criminals employ ever more sophisticated techniques to infiltrate organisations. The good news is there are several strategies that can be taken to close off these potential avenues.

Supply chain cyber attacks are increasingly hitting the headlines. This is where an attack spreads from one organisation to another or uses one to access the other, such as provider to customer. A recent breach of the business process services company Capita, for example, which provides services to several public sector organisations, led to the data of some residents being compromised.

The Capita case concerns a scenario where the supplier had direct access to resident data and was processing it on their clients' behalf, but this is not the only type of supply chain attack. Infiltration of software is one risk, as seen with the SolarWinds attack where attackers compromised a software update process affecting many companies, but there are other potential routes into organisations through their supply chain, including through hardware. Increasingly, attacks are coming from hackers gaining access to a third party and then monitoring traffic between the third party and the target organisation before intervening and sending what looks like a legitimate email in a phishing attack.

Irene Coyle, Chief Operating Officer at OSP Cyber Academy, the provider of cyber security training, explains how these are getting past employees: ***"It used to be that badly written emails with poor punctuation and grammar made it much easier to identify when it was a phishing attack but now the level has really increased. They identify, for example, that you are expecting an invoice and they target an individual in the organisation who will think it is legitimate such as in the finance department. The employee inadvertently clicks on the link and that is the hackers into the organisation's network, and you can imagine the carnage that can cause."***

With these types of attack on the rise and constantly evolving, organisations might wonder how it is possible to prevent them. Thankfully, Coyle says several steps can be taken. Firstly, all suppliers should be vetted, with questions asked about their cyber security strategy, and, secondly, they should be asked to sign a contract highlighting cyber security measures expected and what happens if this falls short. ***"What you should be doing is asking a series of questions: Are they Cyber Essentials Plus? Are they ISO2701? How do they protect data on their systems? Do they do backups? Do they have firewall or malware protection? There are several points that should be covered in any contract with suppliers to build that confidence and ensure the supplier knows the weaknesses that could come through the relationship too,"*** she explains.

Evidence suggests vetting suppliers is not yet a standard process. The 2021 CrowdStrike Global Security Attitude Survey found 84 per cent of IT personnel believed software supply chain attacks could become the biggest cyber threat to organisations in the three years to 2024. Despite this, only 36 per cent said they had vetted new and existing suppliers for security purposes in the previous 12 months.

Kurtis Toy, a vCISO and Convenor of the Cyber Centre of Excellence (CCoE) agrees vetting should take place and suggests more rigorous requirements for suppliers whose IT infrastructure touches your own: ***"The Capita attack was a big deal because the organisations affected had their IT infrastructure outsourced to Capita. If it were a contract with a cleaning company, then the cleaner's IT isn't likely to touch the IT of the organisation at all. However, what could still happen is that they might forward something on because they haven't been trained in cyber security and this could have an embedded ransomware attack or phishing link."***

Also important is regularly checking suppliers. ***"As the relationship moves on don't just assume everything is okay,"*** adds Toy, ***"Continue supplier assessments on an ongoing basis so when new threats and standards emerge you are ensuring maintenance of those cyber security standards. It is also sensible to consider what to do if a supplier gets attacked, especially a critical supplier, and what measures can stop it spreading throughout the whole organisation."***

Staff training internally and within the third-party organisations is also key to raise awareness of supply chain attacks and what action should be taken in the event of a breach. OSP Cyber Academy offers a course based on National Cyber Security Centre guidance on supply chain cyber security which is available at preferential rates through the CCoE. It is aimed at all employees but could be particularly useful for departments that deal with third party suppliers, such as finance and procurement. ***"As much as anything it is about ensuring employees think about taking that step back and checking the details,"*** explains Coyle, ***"So they think, yes, we expected this invoice, but it is still good practice to check it has the same bank details as last time. While this creates an additional step, supply chain attacks are becoming so sophisticated that this is the level you must go to."***

Another possible option is to carry out a test of the supplier's public facing information through an attack surface scan (see pages 5 and 6), which is perfectly legitimate, and may reveal potential vulnerabilities in the cyber security of a third party.

With supply chain attacks on the rise, this is an issue no organisation can afford to ignore. ***"You are only as strong as your weakest link,"*** warns Coyle, ***"It's a dangerous situation and I don't think we currently place enough importance on making sure the supply chain is just as secure from cyber-attacks as our own organisation is. The danger comes when organisations are complacent and assume the supply chain is working towards the same level and standard of cyber security as them without asking the right questions."***

• To find out more about the supply chain course offered by OSP Cyber Academy visit, www.elearning.ccoe.org.uk/product/supply-chain-course

Welsh council tests CCoE protection

MERTHYR TYDFIL
County Borough Council
Cyngor Bwrdeistref Sirol
MERTHYR TUDFUL

Merthyr Tydfil County Borough Council is now in the final stages of a pilot with the CCoE to test a package of cyber tools and help assess their suitability as a set of solutions to help boost the cyber resilience of public bodies.

Merthyr Tydfil County Borough Council (MTCBC) is a Welsh council which already has a mature cyber security posture. It is currently the only local authority in Wales with an ISO27001 certification for information security management and has representatives sitting on the Cyber Resilience Board for Wales. However, it still saw the benefits of working with the CCoE to test its cyber defences and to gain expert advice on areas to potentially improve. Ellis Cooper, Chief Executive of Merthyr Tydfil County Borough Council, said: ***"We have been very proactive from a cyber resilience perspective and aim to ensure Merthyr Tydfil is as resilient as we can get it, but taking part in the pilot was a no brainer. Whatever your cyber expertise as an organisation, having a mirror held up from an external provider to show you where you are and where there could be gaps is not a bad thing."***

He added: ***"Cyber threat has been on our corporate risk register for years now and its persistent presence underscores the substantial impact it could have. It is recognised as a significant risk and is only one step down from our very highest. Being part of the CCoE pilot has provided an opportunity to do something in response which increases peace of mind and shows elected members and the electorate that we are doing everything we can to manage customer data and protect the services provided."***

The pilot has consisted of five stages: an overview discussion with a vCISO to allow them to understand the systems, standards, controls, and certifications already in place, a scan of MTCBC's network to check for vulnerabilities, a consultation with an operational technology expert and ransomware simulations. Lastly, a report will be delivered by the CCoE with the findings and recommendations.

Ryan James, Chief Information Security Officer at Merthyr Tydfil County Borough Council, said the ransomware simulation was in progress and the operational technology stage of the pilot had been valuable: ***"Stage three of the pilot looked at operational technology, which is not something most local authorities will have generally considered as priority to be a cyber risk – we certainly hadn't previously. Building management systems, door control access systems, CCTV, this all connects to the Internet so are a potential risk."***

While MTCBC already carries out phishing simulations, this is the first time a ransomware simulation has been run, which James said would allow the council to test its business continuity plans to ensure service delivery can continue in the event of an attack, including with homeworking. ***"Ransomware is a big risk to local authorities. It is all very well having plans in place, but unless you have tested them how would you know if they are going to work?"*** he added.

Cooper said he hoped the pilot would offer proof of concept to give other local authorities confidence to engage: ***"We need to take a collegiate approach because we are only as good as the weakest link in the chain. We need all other public sector bodies to increase their cyber security maturity too because we are inherently linked. What the pilot has hopefully achieved is to demonstrate that the CCoE can offer a set of solutions that can increase cyber resilience in a way that is easily engageable and implementable."***

Other CCoE pilots

The Cyber Centre of Excellence (CCoE) is a body which aims to make the UK the safest place to live, work and play online. Since it formed at the end of 2022 it has been running a series of pilot projects aimed at understanding what public sector bodies and their wider communities need in place to stay abreast of cyber threat.

Several councils have fallen victim to a cyber-attack recently and, with the ever-increasing sophistication of the criminals, local authorities are likely to keep being breached and hitting the headlines unless they act. Cyber threat is also affecting local businesses and other organisations which work closely with the public sector, potentially affecting the economy and wellbeing of local areas, making it important to find affordable solutions for our wider communities too.

Like the pilot with Merthyr Tydfil County Borough Council (see above), other pilots have been taking place with a range of other sectors, including a special school trust. Another pilot has recently launched with a group of six care organisations, including national, regional and learning disability providers, as well as with a group of six small businesses. The aim is to find the common problems faced by the different sectors to find the correct solutions to be included in a CCoE Protect Package.

"We know local authorities are a long way behind other parts of the public sector in terms of cyber protection," explained Dr Andrew Larner, Chief Executive of iESE and a member of the CCoE Advisory Board, ***"We also know that we need to protect ourselves but also our wider communities. We are running pilots in parishes, the care sector, schools, district councils, unitary councils, and small businesses. These are looking at technology, people, processes, skills, and support. We are looking at how you can bring all of that together to give cutting-edge defences packaged together to give military-grade protection at high-street prices."***