TRANSFORM

ISSUE 23

In print and online issue | www.iese.org.uk

How the cyber threat landscape is changing

Learn about the increasing risks to local authorities

Transformational zero-day protection

iESE partnership brings exciting new technology to UK councils

Also inside:

- How iESE is supporting local authorities around cyber risks
- What to consider around 5G and the Internet of Things
- The supply chain and potential threats
- Homeworking: how to protect staff and your organisation
- Councils get behind virtual high streets

iese
The public sector transformation partner

CONTENTS

WELCOME LETTER

Evolving cyber risk needs step change in security

Dr Andrew Larner, Chief Executive

@LaverdaJota

Through our work with councils, we have seen a range of cyber protection models in place. Some authorities are undoubtedly very vulnerable, especially in an age of targeted sophisticated attacks.

Gone are the days where a hacker was a lone teenager in a dark room, hacking is a multi-million-pound business, and the goal has moved from overtly locking users out of their own networks to getting inside unseen to steal confidential data before demanding a ransom.

It is tempting to think those recently badly hit, such as Redcar & Cleveland Borough Council and Hackney Council, must have had weak defences but we know this isn't true. These were authorities doing all the right things, yet they were taken down catastrophically with clean up bills estimated to be £10m upwards.

With the Internet of Things undergoing an exponential explosion due to the advent of 5G, it is clear the IT boundaries a local authority used to need to protect are gone. Everyday items are now digital and the links into your network are many, including service delivery partners, suppliers, customers through digital apps, employees' own devices and more.

A generational leap in protection is required for this generational leap in technology. That is why we have partnered with AppGuard, a technology new to the UK designed in the US defence environment. We are excited to offer it at a preferential rate and have set out this issue of Transform to introduce you to the technology and to explore the changing nature of cyber security risks.

Dr Andrew Larner and the iESE team

NEWS

iESE launches cyber club and defence test service

LOCAL AUTHORITIES ARE BEING ENCOURAGED TO JOIN IESE'S NEW CLUB TO SHARE BEST PRACTICE AROUND CYBER SECURITY. THE AIM IS TO CREATE A SAFE SPACE WHERE COUNCILS CAN SIGN A JOINT NON-DISCLOSURE AGREEMENT TO SHARE SENSITIVE INFORMATION TO HELP PREVENT BEING HIT AND RECOVER QUICKY SHOULD THE WORST OCCUR.

The club will be free to join and will operate as a private group with input from iESE experts. The aim is that there will be a library of digital resources and virtual meetings hosted by iESE.

iESE is also setting up a cyber defence test service to allow local authorities to assess their existing defences. This follows two 'Hackathon' online events where members of iESE's Innovation Club and other attendees from 20 other councils were invited to see how the AppGuard technology – now offered through iESE at preferential rates – worked and how quickly malware could defeat some other anti-virus software available.

"We hosted the Hackathon for Leaders and Chief Execs so they could see how exposed they were," said Dr Andrew Larner, Chief Executive of iESE, "They are becoming much more aware generally about the power of digital to reshape the way they run their services, but many do not appreciate how at risk they are.

"AppGuard is the only edge-protection technology that hasn't been breached and we have proved it time and again. Doing our due diligence, we took the WannaCry threat that took NHS systems down in 2017, got the version of AppGuard from six months before, created an isolated network, launched the attack and it just bounced. It did the software equivalent of shrugging its shoulders."

- **To find out more about the cyber security club and test service or to see a demonstration contact: annabelle.spencer@iese.org.uk**

Making the UK safer 'one council at a time'

SEVERAL COUNCILS WHICH SECURED A PLACE ON OUR PROOF-OF-CONCEPT TRIAL FOR THE CYBER SECURITY SOLUTION APPGUARD HAVE GONE ON TO PROCURE THE TECHNOLOGY AT A PREFERENTIAL RATE.

One representative from a council in the Midlands said: "While we're just a few months into the partnership, it is clear AppGuard offers us full protection against increasingly sophisticated cyber-attacks so we can, with confidence, deliver our ambitious transformation programme for staff and residents."

Dr Andrew Larner, iESE's Chief Executive, said iESE teamed up with Assurity Systems Ltd, the European distributor of AppGuard, to bring the transformational technology to the UK's local government environment after undertaking a worldwide search for cyber security technology which met the needs of the changing digital world and how local government services are delivered.

The iESE White Paper, *Digital local public services: The path to an effective digital and technology strategy for local government,* mapped out the future of the community from the use of drones through to electric roads. This, in turn, outlined the what the future of local government would look like.

Realising that the 'Internet of Things' was going to have an "exponential explosion", Dr Larner and his team set about finding a way to protect every digital device that might connect into a local authority network and pose a security risk. "What we realised was that there was great promise in that environment but also huge risk," he explained, "Our concept is to make the UK the safest place to live, work and play one council at a time. AppGuard's pre-exploit technology is totally different to what is currently on offer in the way it works, the outcomes it achieves and its ability to protect Operational Technology (OT) and Information Technology (IT). It is a generational leap in protection which is required for the generational leap in technology taking place," he added.

The technology protects against malware attacks, even those known as zero-day (never-seen-before). "At the moment if you are sensible, you have layers of protection, you throw up the best outer defence you can and then it is a bit like a medieval castle, you have rings of defence and then internally you separate spaces so if someone gets in, they can't get anywhere else. Having those layers of protection is still sensible, but what AppGuard does is recreate that outer wall and that buys you time," Dr Larner explained.

As an investor in the product, iESE has secured highly preferential rates with discounts exceeding 50 per cent for local authorities for a full managed solution, including licence fees. A server version also available and if you need extra monitoring and support, iESE has also secured preferential rates on Security Operation Centre (SOC) services.

- **Find out more about the changing nature of the cyber threats on page 3 and more about AppGuard on pages 4 and 5**

EDITORIAL CONTACTS

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

CREDITS:
Editorial by: Vicki Arnstein
Designed by: SMK Design

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

Cyber chameleon: a changing threat

Headlines emerge daily of another successful and damaging cyber attack. The threat landscape has dramatically changed in recent years and it's clear from the scale and severity of attacks that it's time to rethink cyber defence to protect local government services and systems and the valuable data they hold.

Ten years ago the number and sophistication of malware attacks was relatively trivial compared with those experienced today. Even five years ago, a defence strategy with a perimeter defence (a firewall) and a good antivirus (AV) product could reasonably protect endpoints. Details of any attacks would be quickly shared by AV vendors around the world resulting in the creation of patches to prevent malware spreading. Provided an organisation was not patient zero (or more likely one of the first 10,000) – and had the resources to apply patches in a timely fashion – it was unlikely to be severely affected.

Today's attacks are much more sophisticated. There is no longer a perimeter to protect because most organisations have transformed (or are in the process of transforming) their services to be fully digital, systems are moving from on-premise to the cloud, including finance systems, and client interactions are increasingly delivered via digital applications.

Cyber criminals are now operating organised businesses designed to make profit and have more money available to design one targeted attack than some organisations being attacked have in their whole annual IT budget. Last year, the BBC reported that cyber gang GandCrab Crew was seemingly reoperating despite formerly announcing its retirement after hitting £1.6bn in earnings.

"I have seen examples of these criminals having helpdesks, so if they say the ransom to unlock captured data is £5,000 and you can't pay, they might reduce it to £1,000 because it is a business and they want to make money," says Dr Jason Nurse, Associate Professor in Cyber Security at the University of Kent.

Back in 2017, the public sector received a wake-up call when the NHS experienced the WannaCry ransomware attack. Ransomware is often delivered via emails designed to trick the recipient into opening an attachment which releases malware. Once a computer is infected, files are locked and encrypted, access denied, and a ransom sought in exchange for an encryption key. None of the NHS organisations affected (a third of NHS trusts and eight per cent of GP practices in England) paid but the Department of Health & Social Care later estimated the attack cost £20m during the outbreak, plus an additional £72m in the aftermath.

In 2020, both Redcar & Cleveland Borough Council and Hackney Council were also seriously affected. At Redcar, the ransomware attack reportedly left council workers using pen and paper, while news reports indicated a repair bill of between £11m and £18m. Six months after the Hackney attack, the council's website highlighted a long list of key services still affected. There has already been a flurry of attacks on universities in 2021, including Northampton, the University of Central Lancashire, Peterborough College and University Centre Peterborough.

Dr Nurse believes criminals are now hitting organisations where they believe there is a higher probability of a payment being made because the longer they are offline the bigger impact it has on society.

While ransomware is rife, the worrying new development is extortionware. "Ransomware is the most common attack, but criminals have started to recognise that some companies will not pay. What they are doing more recently is going in and extracting data and then locking it up. They say pay me to unlock it and, if the organisation refuses, they say 'well I downloaded a copy of your data beforehand so if you don't pay, it will be released publicly'," Dr Nurse explains.

After Hackney was hit, stolen data was reportedly published on the dark web. "This has the impact of damaging the organisation because not only are the systems locked up and they can't function, or they can't function that well, they have the threat of sensitive information on employees and customers being released and then the Information Commissioner's Office has to be involved because of GDPR and fines may come into play," he adds.

Chris Cooper is an experienced cyber security leader and member of the ISACA Emerging Trends Working Group, affiliated with the global tech professional association. He agrees that the landscape of organisations affected by cybercrime has increased. "There are a lot of ransomware attacks and local authority can be a target because they have lots of external communication, which means plenty of opportunity to click on a link or open an attachment and infect the network. The other side is that hackers are getting access to data they can try to secure funding for in return for not releasing it. The hackers believe anything carrying a government tag potentially carries extra value."

In today's environment, there is unfortunately a much greater likelihood of being taken down by a cyber-attack, even when an organisation has solid strategies in place. "Organisations should recognise that they will be hit at some point. They may be unlucky and impacted by attacks like ransomware, through to much more targeted attacks," adds Cooper.

Besides the risk of being directly targeted for sensitive data, cyber criminals may infiltrate systems through third parties, including partner organisations, the supply chain, through service apps, via Operational Technology and the Internet of Things (smart watches, web cameras etc) and employees working remotely on their own devices or bringing these devices to the office.

In the over-stretched position of CEO, it might be tempting leave cyber security to the IT department, but a successful attack could leave a local authority exposed to enormous costs, reputational damage, and a logistical nightmare. For cyber security experts this makes cyber security a boardroom issue. "I wouldn't recommend leaving cyber security in IT anymore. It is very much a holistic thing – it is people and process and technology. If you don't address all three, and ensure they are all directly interlinked, you can't really get a good solid cyber security posture," Cooper concludes.

• To read more about risks outside of the organisation, such as homeworking and the Internet of Things, see pages 6 and 8.
• To read more about a new cyber security solution being offered to the local authority market through iESE see pages 4 and 5.

Patient zero protection: introducing AppGuard

AppGuard is a newly available endpoint cyber security solution which will protect your systems from all threats – even the never-seen-before attack known as 'zero-day'. Developed in the US defence environment, it has recently become commercially available in the UK and is being offered to local authorities by iESE through a partnership with its European distributors, Assurity Systems Ltd.

Local councils reportedly face as many as 800 cyber-attacks every hour. Whilst the majority are thwarted by traditional cyber security solutions, a sophisticated targeted attack could have a devastating outcome.

"The changing nature of attacks means that, unless defences change, it's not a matter of 'if' but 'when' local authorities will be breached," says Colin Jupe, Director of Strategy at Assurity Systems Ltd. "The nature of the threat has changed dramatically. A few years ago, a good anti-virus and firewall would be a solid approach. Today that's simply not enough, the hackers are more sophisticated – it's big business."

Most local authorities currently have a layered approach to cyber security, incorporating several well-known vendor solutions to protect their infrastructure, known as a 'strength-in-depth approach'. Traditional endpoint defences will incorporate anti-virus and anti-malware solutions, however even with the latest Endpoint Detection and Response (EDR), Machine Learning and Artificial Intelligence, this combination of defences still relies on recognising the signature of the threat or recognising it as being similar to one seen before.

The problem with the new sophisticated wave of targeted cyber-attacks, is that if malware has never been encountered by a defence system before, there is a high probability it will be able to penetrate endpoints and activate. Local authorities may feel they are unlikely to be directly targeted but Jupe says this is not true. "Criminals understand the value of council data and the mayhem and headlines they are able to achieve. Besides the potentially huge cost of recovering from an attack, without access to digital systems, local authorities are unable to effectively deliver much-needed services, meaning some of the most vulnerable in our society will suffer," he explains.

Many organisations take the view they will be hit at some point and choose to rebuild from a back-up. This is time consuming and there is no guarantee that an Advanced Persistent Threat (ATP) will not have been left in the system or that data will not have been stolen. They might also take the view they are unlikely to be first hit and therefore their cyber security will have been patched in time. But if you are first (patient zero), or your already-stretched IT team has not yet patched your systems, the fall-out can be devastating.

What is AppGuard?

AppGuard offers the required step-change in endpoint and server defences because it operates in an entirely different way to traditional solutions. The patented technology monitors everything and trusts nothing, meaning it offers protection without the need to detect previously known exploits. It has been described as employing zero-trust to combat zero-day attacks.

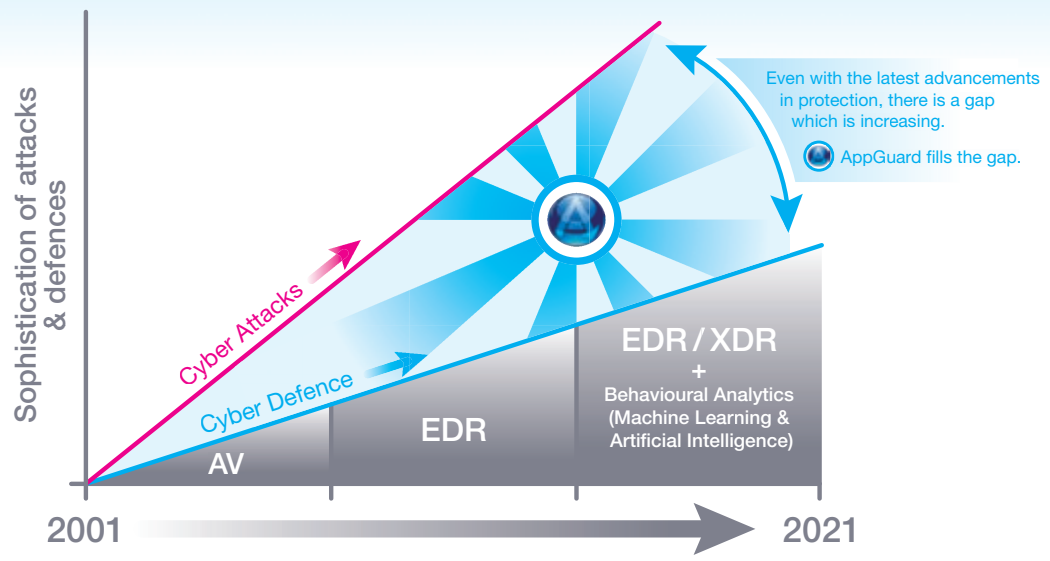
"Local government has done pretty well in cyber defence and the model works well if you are not the first to be attacked," explains iESE's Chief Executive, Dr Andrew Larner. "But as the Internet of Things takes off in care and other areas of our communities, the current reactive model to cyber defence will be severely tested. It is now possible to put cyber defence on the front foot – you don't need to have seen the type of attack before to trap it and kill it."

New to the UK, AppGuard already protects millions of endpoints around the world, including military and defence organisations, government departments, large corporations and small and medium-sized business. It has already been successfully tested in the local authority environment to ensure compatibility with the unique complexities of council systems and to allow quick and painless implementation without system downtime. It doesn't need libraries of signatures to work and continues to offer protection when not connected to the internet. A server version of the technology is also available.

"AppGuard is already installed and working in a number of UK councils. It protects all programs and applications on both servers and endpoints, including bespoke third-party applications essential to services," explains Jupe.

Jupe acknowledges there is a lot of confusion around existing cyber security solutions, partly because vendors all make the same claims and use the same language. Add to this the competing pressures and stretched budgets of local authorities and the choices can seem bewildering. "There is a lack of knowledge and, as a result, local authorities are buying more of the same. This is exacerbated by the fact that everyone is saying the same things, so many local authorities take the option of better the devil they know," he adds. "Local authority IT teams are being stretched from pillar to post, responsible for maintaining systems as well as defence, often under-resourced in terms of both human and monetary resource, meaning there are necessary compromises. Cyber criminals do not suffer from these compromises or stretched resources. They have one focus only – to get

Traditional endpoint protection is losing the battle



through your systems – and they have more money to develop one attack than most councils have in their whole annual IT budget."

With AppGuard installed, all workers (even homeworkers) can carry on as normal. Even if they inadvertently click on a malicious link or open a nefarious email it can do no harm. AppGuard can be remotely installed in hours and is offered as a managed service, so has little or no impact on IT resources. "In fact, teams have noticed that they have more time to deal with their day-to-day challenges because AppGuard simply blocks malicious activity as opposed to quarantining or highlighting it as a potential threat, meaning the team has fewer false positives to investigate," Jupe says.

It also offers invaluable protection for applications awaiting patches, some of which are critical and leave high-risk vulnerabilities. With AppGuard, patching can be programmed to meet resources, safe in the knowledge malware will not exploit the applications in the meantime.

iESE has teamed up with Assurity Systems Ltd to bring this exciting, transformational technology to the UK's local government environment. AppGuard is offered as a fully-managed solution, and we have secured highly preferential rates with discounts exceeding 50 per cent. A server version is also available and if you need extra monitoring and support, we have also secured preferential rates on Security Operation Centre (SOC) services.

- **Find out more: www.iese.org.uk/project/appguard**
- **To book a short jargon-free introductory call at a date and time that suits you, please contact craig.white@iese.org.uk**

AppGuard: the benefits

- **AppGuard** AppGuard is not reliant on whitelisting, Host Intrusion Prevention Systems (which stop malware by monitoring the behaviour of code) or sandboxing (an isolated environment used to run suspicious code without risking harm to the network).
- **AppGuard** does not need to scan libraries of files to work – it doesn't even require internet connection to keep you protected.
- It blocks malicious code at the kernel level, its Zero Trust Framework does not need to guess if there is suspicious activity, it shuts down malware before it detonates.
- It only uses 1MB on a hard drive and 10MB of memory, resulting in virtually no degradation of processing power.
- **AppGuard** can run for months without updates. There are no alerts for staff to prioritise because they are blocked in real time before they can cause harm.
- **AppGuard** allows a reduction in the layers of edge defences, potentially saving money and reducing the volume of data analytics and burden of patch management.

"AppGuard should be your first and main line of defence in an increasingly dangerous cyber and human threat environment."

Mark Kelton,
Former Deputy Director of the National, Clandestine Service for Counterintelligence, CIA

"AppGuard is incredibly forensic, providing an extremely high level of security which provides us with real peace of mind as we look to transform the organisation into a digital-first council."

Senior Infrastructure & Communications Officer,
A Midlands Council in the UK

Glossary: Understanding the jargon

MALWARE: Any type of malicious code designed to infiltrate a device, including a mobile device, without the user's knowledge. Malware gets activated by the user unwittingly downloading or installing the malware, such as by clicking on a link or visiting a malicious website. Malware includes ransomware and extortionware (see below).

RANSOMWARE: Malware which typically locks or denies access to files until you pay a ransom to the hacker. Any organisation storing sensitive information is at risk. Even if you pay the ransom the hackers could leave coding (an ATP) set to activate later (see below).

EXTORTIONWARE: With this type of attack the cybercriminal gains access to and exfiltrates your data; they may publish a sample online so you know they have it. This will be followed by a demand, usually for money. Your data may be auctioned on the dark web to the highest bidder. Even if you pay, the hackers could leave coding (an ATP) to activate later.

ADVANCED PERSISTENT THREAT (ATP): An ATP uses continuous and sophisticated hacking techniques to gain access to a system and remain inside unknown. This method of attack is usually levelled at high-level targets with the goal of stealing valuable information. It is also possible that an ATP attacker could target smaller companies in the supply chain as a way of gaining access to larger organisations through these often less-well defended routes. Even when an ATP attack is discovered and dealt with, the hacker could leave routes open to return.

ZERO DAY ATTACK: This is where a cybercriminal exploits a previously unknown software vulnerability. It is so named because software engineers have had zero days to fix the issue. Zero Day attacks are especially difficult to detect and defend against because traditional anti-virus, Endpoint Detection and Response (EDR) software and firewalls can only stop attacks where the code (signature) or behaviour has been seen before.

DARK WEB: The dark web refers to websites which cannot be found using traditional search engines or visited using traditional web browsers. It is different from the Deep Web, which is where information may sit not intended for public view (such as a test webpage). In the event of an extortionware attack this is where the hackers will auction stolen information.

Case study: Why one forward-thinking council is using AppGuard

One council based in the Midlands, already using AppGuard, is currently embarking on the second phase of an ambitious digital transformation programme. Data is at the heart of the transformation and involves sharing and collaborating with people and organisations outside the traditional boundaries of its network. Along with this agile way of working, it recognises the risks posed by a new wave of sophisticated attacks and the need to combat them to protect its data and service delivery.

The AppGuard technology was supplied under a special arrangement with iESE. The council's Assistant Director, Business Transformation, said: "While we're just a few months into the partnership, it is clear AppGuard offers us full protection against increasingly sophisticated cyber-attacks so we can, with confidence, deliver our ambitious transformation programme for staff and residents."

iESE and Assurity Systems, AppGuard's European Distributors, worked closely with the council's ICT team to establish a proof of concept. Being the first local authority to adopt AppGuard in the UK, it undertook a robust assurance process to ensure the technology provided the expected protection, as well as ensuring there was no disruption to systems, staff or customers. Implementation was achieved smoothly during lockdown and the impact on the council's ICT team was, and continues to be, minimal due to Assurity's fully-managed service. "The support and responsiveness of the iESE and Assurity teams has been fantastic during the proof of concept and staged rollout of AppGuard," the spokesperson added.

Unlike traditional systems, AppGuard has such a light footprint that it does not bloat or slow down systems, taking up only 1MB of space on endpoints. It also provides continual protection even when devices are not attached to the internet and does not rely on constant signature updates to remain protected against the latest threats. These benefits make it an attractive investment for the council. "Staff are unaware of the work going on behind the scenes to give them this extra protection – this is exactly how cyber defences should be, effective but unintrusive to day-to-day operations," the spokesperson added.

The council's Senior Infrastructure & Communications Officer, ICT Services, is also impressed. "AppGuard is incredibly forensic, providing an extremely high level of security which provides us with real peace of mind as we look to transform the organisation into a digital-first council. The council's strategic approach to cyber risks is employing a best practice defence in-depth model. AppGuard provides a novel solution for the council to enhance the protection of its endpoints."

- **To download the full case study visit: www.iese.org.uk/downloads/council-improves-cyber-security**

Limit cyber risks of homeworking

The Covid roadmap aims to end all social restrictions by June 21 but with homeworking looking likely to stay, local authorities should carefully consider how to manage cyber security, especially if employees mix both home and office days with devices that switch between networks.

While some of us are itching to get back to the office, working from home is likely to continue post-Covid. Research from the CIPD has found employers expect the proportion of staff working from home regularly to increase to 37 per cent compared with nine per cent before the pandemic. A similar poll by the IoD found 74 per cent of business leaders would be maintaining increased home working after Coronavirus.

While employers may be confident the work is getting done, there is evidence increased homeworking raises an organisation's vulnerability to cyber-attacks. "Many organisations have suffered cyber attacks over the course of the pandemic, causing significant disruption, loss of revenue and in many cases, date theft. The potential for reputational damage can result in long-lasting consequences," says Joe Fizsimons, Senior Policy Advisor at the IoD.

Research by the Ponemon Institute, *Cybersecurity in the Remote Work Era: A global risk report,* found that while 71 per cent of IT and IT security personnel rated their organisation's security posture as effective at mitigating risks, vulnerabilities and attacks before Covid, this dropped to 44 per cent during Covid.

Of those asked, 59 per cent said access to business-critical applications had significantly increased (26 percent) or increased (33 percent), while 67 per cent say remote workers' use of their own devices to access business-critical applications and IT infrastructure had decreased their organisation's security posture.

The research found that 60 per cent of respondents said their organisations had experienced a cyberattack during Covid, while 51 per cent of respondents said exploits and malware had evaded their organisation's intrusion detection systems and almost half (49 percent) said their organisation's anti-virus solutions had been evaded.

Chris Cooper is an experienced cyber security leader and member of the ISACA Emerging Trends Working Group, affiliated with the global tech professional association. He says working from home changes how an organisation protects its employees. "There is a whole different view you have to take of the security posture when you have that open environment of people working from home. Some organisations maybe don't have controls in place because working from home was an unexpected development but that will need to change because it is going to be staying around," he says.

One of the big risks is BYOD (Bring Your Own Device), which some IT professionals refer to as "Bring Your Own Disaster". There is potential that devices used on potentially less-secure home networks might become infected and then transfer this infection to the office network once connected. "You have to adopt a different approach if you are going to have that hybrid environment," Cooper adds. "The more common way now is through zero-trust architectures, so everything is assumed to be untrusted, whether it is in the office or home and you manage the accesses and permissions from that perspective."

Dr Jason Nurse, an Associate Professor in Cyber Security at the University of Kent, believes besides taking solid security measures in terms of software and hardware solutions, there is also an education issue around staff returning to the office. "There will almost be a learning period again of coming back to the office and a question of training people about security. A number of people hired in the Covid period have probably never seen their office and potentially haven't had the security training they would have had, so there is a big challenge bringing these individuals back in, even if it is staged."

Cooper agrees regular training is vital. "One of the key vulnerability for any organisation is still the user, so making them cyber aware and doing simulations, such as sending out phishing emails to educate them about how to respond to these things is important. With a test I ran for a client recently, 25 per cent of people clicked on the link which could have been a fairly major infection."

In terms of more practical measures, Cooper says vulnerability management is key. "I have still never found a client who has got the patching of systems under control and yet it is one of the most fundamental things. Whether it is zero-day attacks or a targeted attack, they all rely on vulnerabilities in software. If you are not patching and keeping up to date all the time you are massively increasing your risk. Another big one is an audit of users. With many organisations you will find that people who have left years ago or changed jobs still have access to systems they don't need, so management of starters, leavers and movers is important and so is the perimeter security."

In addition, Dr Nurse says keeping regular back-ups is key and to ensure these go far enough back in case they become infected too. "It is about working out whether the back-ups can be segmented in such a way that things can be recovered that don't have ransomware on if this has been left in the system as an Advanced Persistent Threat (APT)." Cooper agrees: "A lot of back-ups are online these days, so it is important to have some taped too and to ensure they go far enough back. If you only have a few months' worth and there is an APT in there, that is going to be a problem."

Organisations clearly need to consider the working from home cyber security conundrum carefully. One thing they could adopt to protect endpoints and servers is AppGuard, a new product being offered in partnership with iESE and the product's UK distributor, Assurity Systems Ltd.

• To find out more about AppGuard see pages 4 and 5.
• To find out more about other security risks outside of the organisation, see page 8.

**None of the experts quoted in this article are affiliated with AppGuard.*

Taking control of virtual high streets

Local authorities are increasingly looking towards supporting the 'virtual high street' as well as the physical one to help boost local economies but creating an experience free from cybercrime should be a vital consideration.

The current outlook for the local high street is mixed. Whilst reports show one in ten high street stores are now empty and ecommerce is ever increasing, many of our essential local stores have thrived through lockdown and this is likely to continue as working from home becomes a persisting trend.

With research showing between 50p and 70p of every £1 spent locally recirculates back into the local economy, councils have been working hard as leaders of place to repurpose town centres and respond to longer-term trends in how high streets are used. The next step some are now taking is to collaborate with online services to give shoppers access to local retailers through a single website.

Jos Creese, an iESE associate who works on digital change programmes, says while some essential local stores have been experiencing a resurgence throughout Covid, it is still important for the local high street to keep up with new trends. "Local shops have proven to be an important part of the infrastructure of our communities and many that have been allowed to open have thrived. In the future we are going to have many more people working at home. The economy is going to be there, but the local high street still has to keep pace with the technology and trends elsewhere to compete," he says.

Creese believes that the local high street will increasingly become somewhere people want to visit to browse and meet local friends and while having thriving shops, good schools and fast broadband will attract residents, local stores which also offer online services adds value and the potential to offer a broader range of experiences and solutions.

Some of the virtual high street solutions now offered, such as Click It Local, aim to enable local independent shops to compete with the likes of Amazon on convenience and choice by making shopping local easier and faster. Shoppers can use the service to buy from multiple local retailers online with one website, one payment and get the goods in one same-day delivery. It aims to combat the mindset that consumers do not have time to go to the local shops and has a low carbon footprint with deliveries staying local and made by electric bikes and vehicles in cities, addressing any environmental misgivings consumers might have about online shopping.

John Comber, an iESE associate and former Chief Executive of the Royal Borough of Greenwich, says the role councils are starting to play in creating vibrant virtual high streets is an important development as they seek to move away from the role of customer-centric service-provider to community enablers: "By utilising a digital platform, the public sector can redefine its role to becoming a catalyst and conduit for matching local supply and demand rather than always seeking to meet the needs themselves," he says.

However, while local authorities carry weight and are respected locally, there will be pressure to ensure that as well as helping provide the technology and publicity, they also help make virtual high streets a safe crime-free shopping experience, just as they seek to make physical high streets safe and welcoming spaces.

"Whilst the plight of the high street and its impact on the local economy is a priority for all councils, not all will have the necessary money and expertise to progress. This combined with the other challenges, pressures and demands they face can lead to a reluctance, even a fear to progress such initiatives. There is a need for authorities to share expertise to develop approaches that maximise advantage and minimise the costs and risks. There is also the ever-increasing challenge of cyber security and the need to protect any virtual presence from attack by hackers. This is imperative to ensuring that citizen and state continue to have a trusting relationship," Comber adds.

Creese agrees that considering the cyber risk element of the virtual high street is vital to avoid poor publicity and loss of trust in the associated council. "There is the obvious concern around personal data and how it is held. If I am leaving my details in a shop or logging onto a website using a council's virtual high street model, I expect the criteria for protecting my data to be the highest possible. It would take little to lose public trust and the local press would have a field day," he warns.

Creese adds that local authorities looking to develop virtual high streets should also consider any partner organisation's credentials. "There are accreditations you would expect to see such as ISO 27001 (Information Security Management) and others. You need to know where the data is being stored, what experience they have elsewhere, how it has done elsewhere. I wouldn't rush to work with a partner with some sexy technology that looks great on the screen, I would be careful about doing the homework appropriately, particularly ensuring the data remains in control of the local organisations and is not going to get used for other purposes to make it all a little bit cheaper," he concludes.

What are local authorities doing?

Click It Local has been launched in Cambridgeshire, Brighton, Waverley and parts of London and Essex. **Brentwood Council**, which announced the launch of its Click It Local site in March, negotiated a 0 per cent store fee for two months to help traders take part.

Virtualhighstreet.uk is the newly launched website for Sudbury-based businesses, supported by **Sudbury Town Council, Sudbury Vision, Babergh District Council and Mid Suffolk District Council**. It was designed as a one-stop resource to help residents stay connected with Sudbury's businesses during Covid-19. Other similar models have been introduced in Fleet in Hampshire (www.findyourfleet.org) and Charnwood in Leicestershire (www.shoplocal.charnwood.gov.uk).

Broxbourne Council has linked with **Local Rewards**, an online local points reward system and the Maybe* platform, which helps businesses use social media more effectively to increase sales and online engagement.

Cotswold District Council has also collaborated with **Maybe*** to allow shoppers to discover and connect with local businesses in ten Cotswold towns and villages.

Security beyond the perimeter

Whilst most local authorities will be fully aware of the cyber security risks on their premises there are many risks beyond the perimeter, including those posed by the Internet of Things and the supply chain.

With the introduction of 5G, the already booming Internet of Things (IoT) is set to explode. According to Juniper Research the number of connected devices is set to hit 46 billion in 2021 and 5G is a game changer for this already thriving market. It enables faster, extra stable and more secure connectivity and allows thousands of devices in a small area to be connected at any one time.

With improved speed and reliability, smart devices can operate better in smart homes and smart cities and communicate and share data with each other at higher speeds. Whilst this opens the door for devices to be used in much greater capacity in local authorities, such as within social care settings and improving services such as traffic management, it may also open the door to a greater number of cyber security breaches.

One issue is that many devices have not been developed with security in mind. "There are so many risks and IoT is just one example. Many of these devices are just not very secure," explains Jos Creese, an iESE associate who works on digital change programmes.

Daniel Dresner, Professor of Cyber Security at the University of Manchester and co-founder of The IASME Consortium which helps businesses improve cyber security, says the issue with many devices is that they are immature and being connected to things that were never meant to be interconnected. "The whole infrastructure of the internet is based on something for which it was never intended and the issue with these devices is that they offer another potential route into your systems."

When purchasing new devices consider selecting manufacturers which will provide ongoing support and software updates, and which have in-built security or the ability to install anti-virus software. "The IoT is now a vital part of so many services. The only thing you can do is prioritise devices with the levels of security that you want. That might cost a bit more but often that is a price worth paying," explains Creese.

Dresner advises checking devices meet a standard, such as the one IASME has developed for manufacturers to show they are compliant with best-practice security. "There are questions which need to be asked such as can the device be updated? What happens if I find a fault? Can I disconnect it? Will it still work while it is updating?"

While it is possible to gain some control over council-purchased devices, the IoT also includes employee-owned smart devices, such as phones, tablets, watches, and even digital pens, all of which could potentially access and share company information. Ultimately, there is no guarantee devices will not have been compromised by hackers looking for an open door and at risk of transferring malware to company operating systems. Segmenting systems can help stop security breaches spreading and good detection systems can then allow parts where issues are found to be cut off.

The supply chain is another cyber risk largely outside an organisation's control but there are some mitigating measures it can take. The SolarWinds supply chain attack in 2020, which originated in the American-based system management tools company, highlighted how a threat can come from even the most trusted supplier or partner organisation. In the SolarWinds case, hackers infiltrated SolarWinds' infrastructure and added malicious code to a software update package which was then sent to thousands of its customers.

"The supply chain presents a real risk, and it is it is not just the supply chain of services and products, it is also the partnership supply chain of organisations that are increasingly interconnected. Health and social care, police and education, there are many areas now where there are strong and growing links. If a malicious organisation is trying to break into an important network, they will look for the weakest link and that could be anywhere in the supply chain," says Creese.

What is important is how suppliers are selected, including an assessment and due diligence around their information practices and resilience. "If they cannot demonstrate that they have good cyber practices, due caution should be exercised. Don't rush into it because you like them and they have a good product, if they have not addressed the potential security risk to a public body you should be cautious about doing business with them," he warns.

What is essential, Creese believes, is that cyber takes on cabinet level importance and is allied to risk management, not technology. "I would like to see cyber being a key topic for emergency planning. Too often it is about dealing with fire and flooding and the traditional threats to civic life but cyber should be a much broader business continuity issue for local authorities."

**None of the experts quoted in this piece are affiliated with AppGuard.*