www.intersec.co.uk

intersec

The Journal of International Security

May 2023

CYBER SECURITY SPECIAL

Ransomware, insurance, business continuity: everything you need to know...

MEGACITY MAYHEM?

Security benefits of smart interconnectivity

BLOK N MESH

DEFENDER INTERMEDIATE FENCING™

A **robust** and **revolutionary** temporary fencing system, our **DEFENDER INTERMEDIATE FENCING™** is an on-ground relocatable temporary perimeter with the strength of a rigid mesh fence.

Utilising **"V mesh"** and supported by our range of ballast options, this system completely removes the necessity of excavating the ground surface to install a strong, temporary fence, minimising the risk of accidental service strikes, saving time and labour costs with a simple and fast installation.

Available in either **2.4m** or **3m** heights Defender Intermediate Fencing is ideal for site environments requiring a temporary perimeter stronger than standard temporary mesh fencing with no trip hazards on the pedestrian side of the fence.

SCAN TO FIND OUT MORE

UK +44 1226 712500

Blok 'N' Mesh Global Ltd, 10 Christleton Court, Runcorn, WA7 1ST

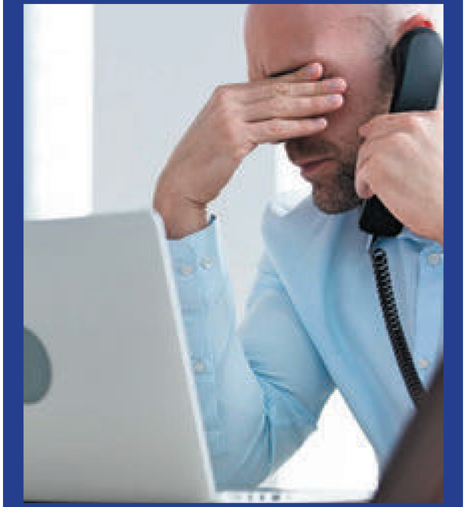
FR +33(0)3.20.02.00.28

Batisec, 67 Rue Du Creusot, 59170, Croix

www.bloknmesh.com

From the makers of POLMIL®

intersec
Volume 33 Issue 05
May 2023



Editor
Jacob Charles

Principal Consultant Editor
Maj. Gen.
Julian Thompson CB OBE

International Arctic Correspondent
Barry Scott Zellen

Design & Production
jellymediauk.com

Published by
Albany Media Ltd
Warren House
Earlsdown, Dallington
Heathfield, TN21 9LY

Tel: +44 (0) 1435 830608
Website: www.intersec.co.uk

Advertising & Marketing
Director of Sales
Arran Lindsay
Tel: +44 (0) 1435 830608
Email: arran@intersec.co.uk

Editorial Enquiries
Jacob Charles
Tel: +44 (0) 7941 387692
Email: jake@intersec.co.uk

Subscriptions/Accounts
Faye Barlow
Tel: +44 (0) 1435 830608
Email: subs@intersec.co.uk
www.intersec.co.uk

EDITORIAL COMMENT

In a rather timely turn of events, cyber resilience specialist Immersive Labs has announced its 2023 Cyber Workforce Resilience Trend Report since the last issue of *intersec*. Conducted by Osterman Research, it will probably come as no real surprise to learn that it reveals a steady increase in cyberattacks and an evolving threat landscape that sees yet more organisations turning their attention to building long-term cyber resilience. Depressingly, and even less surprising, many of these programmes are falling desperately short of their goal and are failing to prove teams' real-world cyber capabilities. The report, which surveyed 570 senior security and risk leaders across UK, US and German-based enterprises with at least 1,000 employees, found that while 86 percent of organisations have a cyber resilience programme, 52 percent of respondents say their organisation lacks a comprehensive approach to assessing cyber resilience.

Unsurprisingly, strengthening cyber capabilities tops the list of strategic priorities for organisations in 2023, with increasing the cyber resilience of cybersecurity team members (83 percent) and the general workforce (75 percent) identified as the two highest overall focus areas. While organisations have taken serious steps to deploy cyber resilience programmes, a worrying 53 percent of respondents indicate the organisation's workforce is not well prepared for the next cyberattack (of any kind) and just over half admit that they lack a comprehensive approach to assessing cyber resilience. These statistics indicate that although cyber resilience is a priority and programmes are in place, their current structure and training are not working as perhaps they should be.

Additionally, organisations lack confidence that their general workforce know how to respond to a cyber incident. For every two out of three organisations, there is a lack of confidence that 95 percent of their workforce will not know how to recover from a cyber incident.

Organisations are questioning the reliability of industry certifications, classroom training, and ad hoc learning pathways to build cyber resilience: While almost all organisations encourage industry certifications, only 32 percent say they are effective at mitigating cyber threats.

Having the right metrics in place to prove cyber resilience amongst teams is important, particularly as Boards and C-level executives are looking for concrete evidence, and yet 46 percent of senior security and senior risk leaders say they do not have the metrics they need to fully demonstrate their workforce's resilience in the face of a cyberattack. Only around 6 percent of organisations are using informative metrics – such as response times – to address vulnerabilities, track intrusion rates, metrics on internal data loss and incidence rates of various threat types.

During the past six months, a request for the security team to prove the organisation's cyber resilience was only made by the Board at 46 percent of organisations. For the senior leadership team, at 51 percent of organisations.

With this in mind, this month's issue is a cyber-security special, looking at some of the biggest issues facing businesses today.

Jacob Charles, editor

Editorial contact
Please address all correspondence to The Commissioning Editor: jake@intersec.co.uk

Subscriptions
Annual Subscription Rates: UK £180,
Europe £200,
USA post paid US$350
Other Countries air-speeded £250. Subscription Enquiries: subs@intersec.co.uk
Average net circulation per issue: 10,510
Intersec (USPS No: 006-633) is published monthly except Jul/Aug and Nov/Dec combined issues, by Albany Media Ltd

Subscription records are maintained at Albany Media Ltd, Warren House, Earlsdown, Dallington, Heathfield, TN21 9LY

Issue Date: May 2023

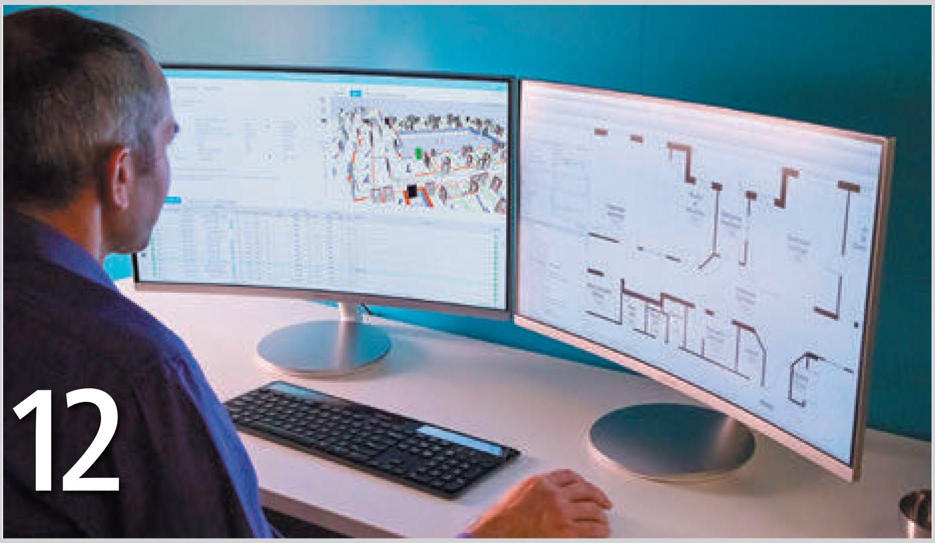
CONTENTS

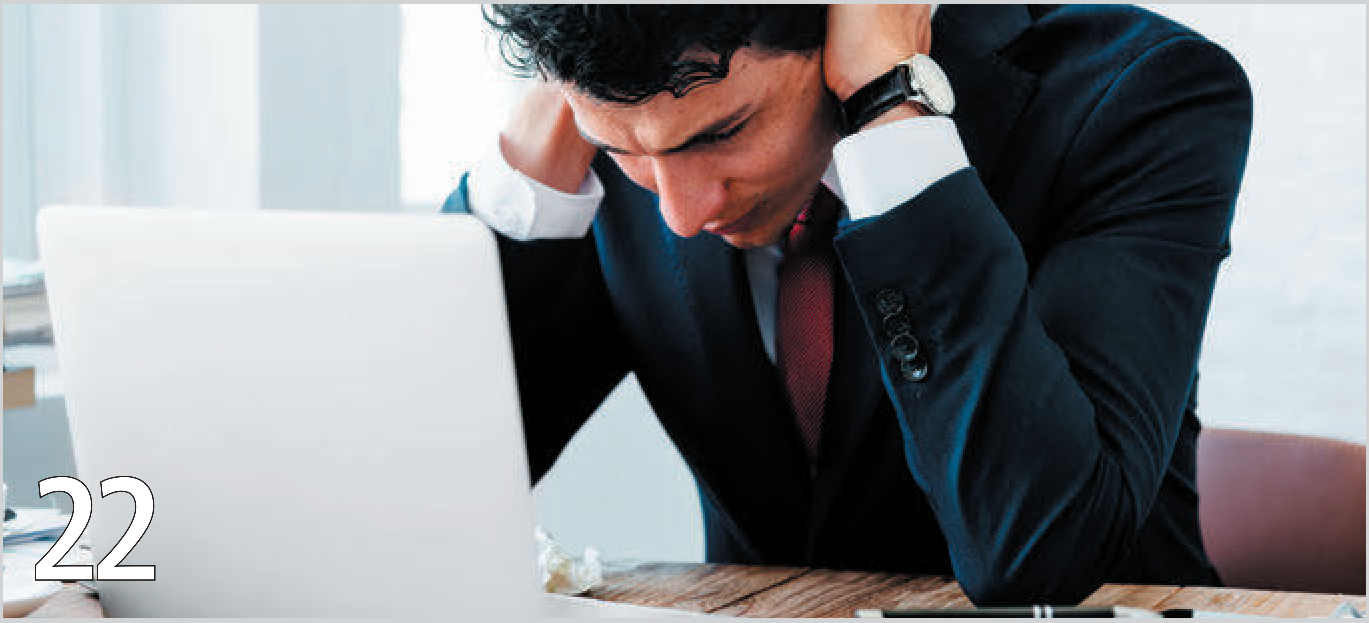
May 2023 www.intersec.co.uk

intersec

Features

Regulars

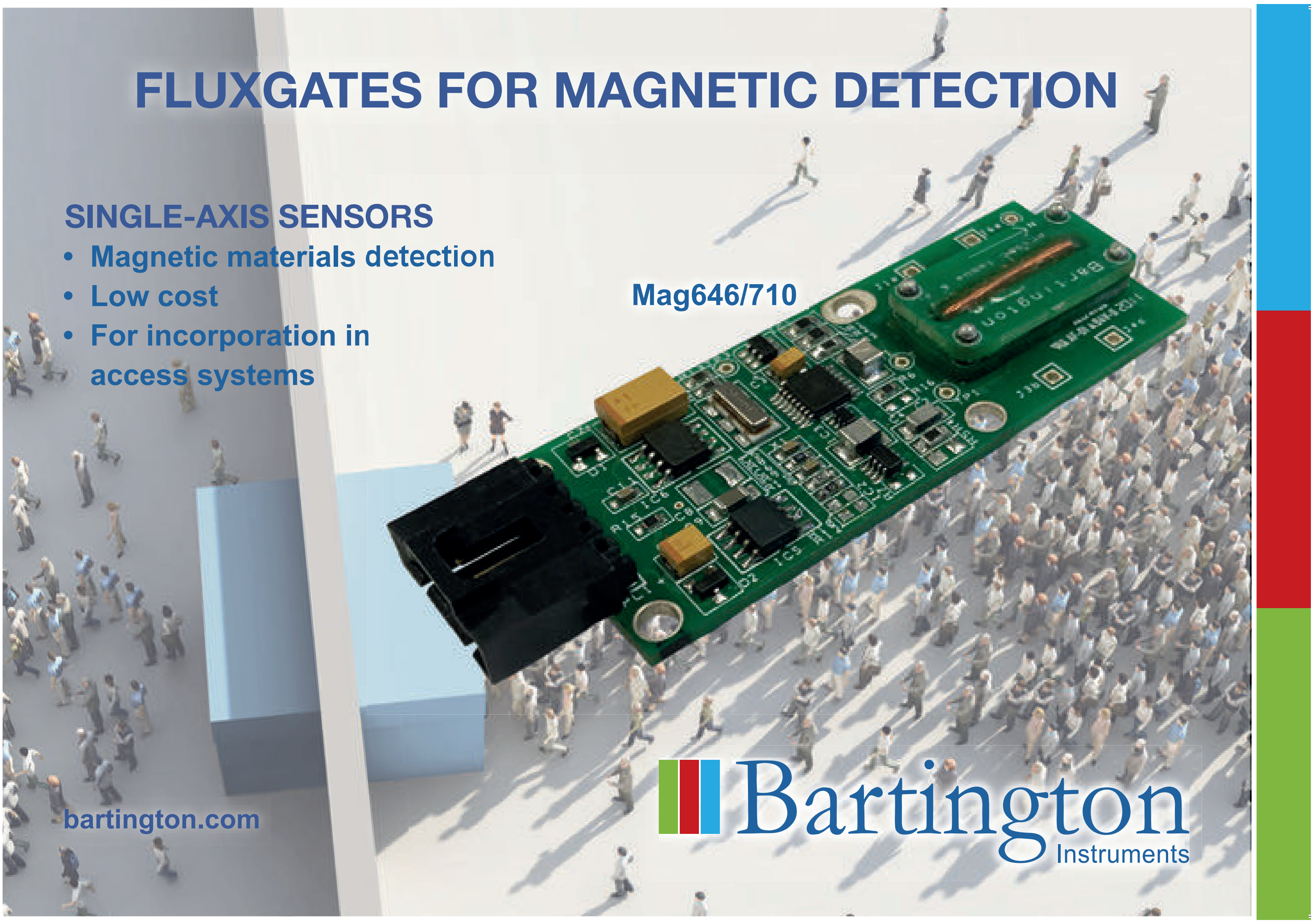



22

www.
Username
Password
Log In
28

32

36



A violent past

Major General Julian Thompson CB OBE Principal Consultant Editor

We too often ignore or dismiss the effect of history on the way humans behave and react. The current war in Ukraine came as a shock to many, but not to military historian David Porter who believes that this war is rooted in: "the nation's military history". Ukraine is a country that has never enjoyed secure borders and through the centuries has lain between, first Poland and the Ottoman Empire, and its protectorate the Tatar Khanate of the Crimea. Later other powers have bordered Ukraine, including the Austro/Hungarian Empire and the Russian Empire. The Cossacks who founded Ukraine originated as serfs escaping from Poland and Muscovy (now Russia) and setting up armed camps on islands in the Dnieper. These people eventually became the Zaporozhian Cossacks and evolved into some of the world's most formidable light cavalry. By the mid-Seventeenth century, the Zaporozhian Cossacks having played a leading role in a succession of Polish victories, rebelled and led by Boldan Khmelnytsky entered Kiev to establish an independent state. The fighting dragged on for years and Ukraine became a Russian protectorate. Throughout the Eighteenth century much of Ukraine was absorbed into the Russian Empire. During the First World War 3.5-million Ukrainians fought on the Imperial Russian side, but 250,000 served with the Austro-Hungarian army.

In the chaos that followed the end of the First World War, Ukraine became a battlefield as Polish, Red (Soviet) and White (anti-Soviet) forces fought each other. The Red Army finally overran most of Ukraine, but their brutal behaviour backed by the secret police (Cheka) provoked a savage resistance. Fighting in Ukraine continued, until Stalin, determined to bring the Ukrainians to heel, staged a deliberately created famine – the Holodomor in 1932-33 – which killed around 5,000,000 Ukrainians. The scene darkened further when Stalin appointed his deputy, Nikita Khrushchev as head of the Communist Party in Ukraine. His oppressive measures provoked the resistance that Stalin sought to avoid. Action by the NKVD, successors to the Cheka, headed by the brutal Beria crushed resistance. As a result of Russian brutality, the German invaders in summer 1941 were greeted by many Ukrainians as liberators.

There was little resistance to the German occupation until the Autumn of 1942, and indeed sufficient Ukrainians volunteered to serve with the Waffen SS to form a new division – 14 Waffen Grenadier Division der SS. The Waffen SS were the armed SS serving with the army like any other division, not as camp guards or police.

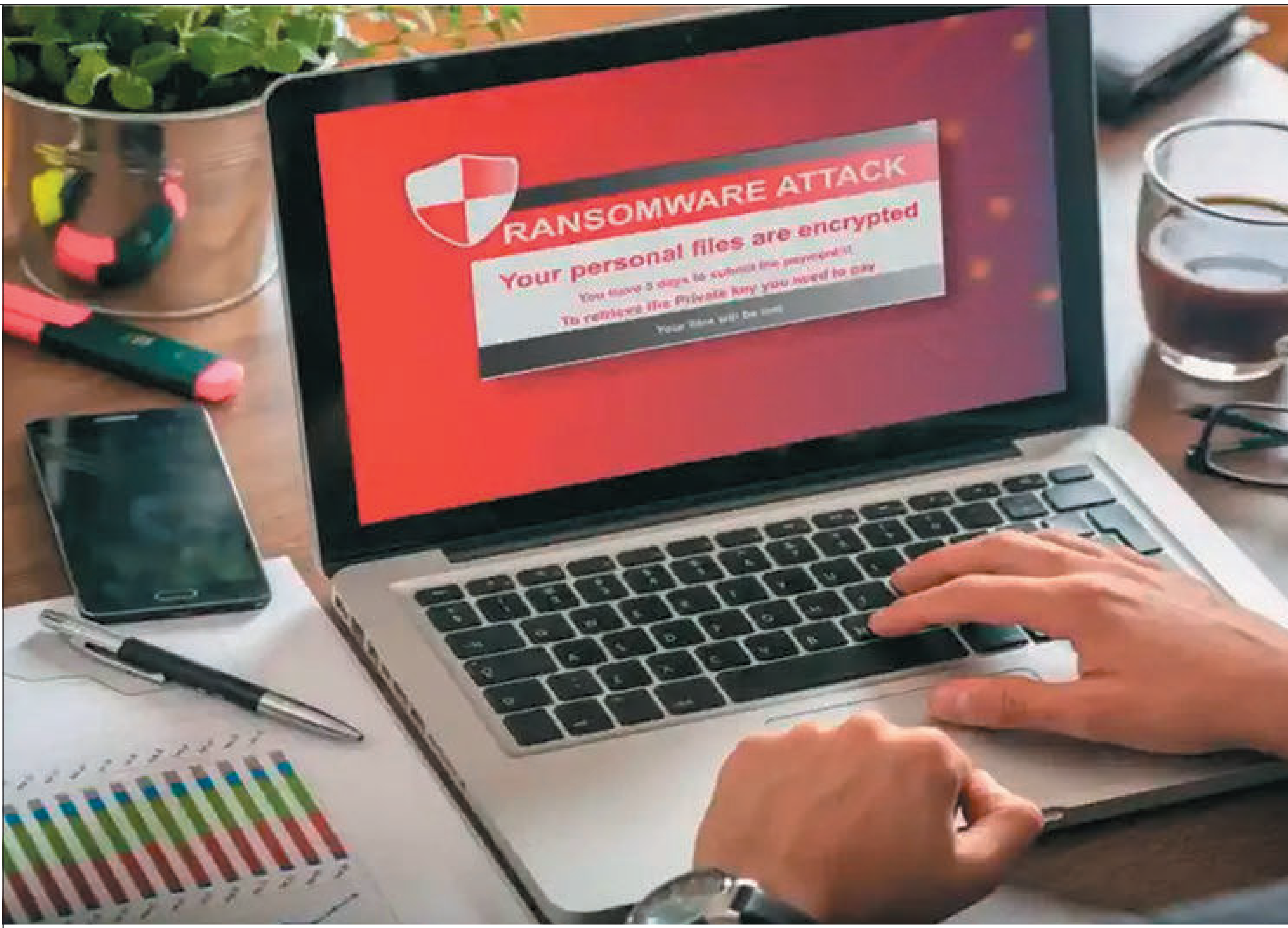
The Germans foolishly increasingly repressed the Ukrainians leading to the formation of the Ukrainian Insurgent Army (UPA). As the Russians advanced into Ukraine in 1944, the UPA turned to fighting the Red Army and NKVD. They ambushed and killed General Vatutin a Soviet Front commander, equivalent to a Western army group commander. This was followed by the annihilation of a NKVD battalion. The struggle continued until Germany surrendered in May 1945. Now able to concentrate their efforts on the UPA, the Soviets began a major deportation programme, so that by 1952 at least 500,000 Ukrainians had been deported, coupled with mass arrests of at least 600,000 people in Western Ukraine, about a third of whom were executed, the remainder being imprisoned or exiled. By the beginning of 1956 all insurgents had been liquidated.

Picture credit: Ukraine MOD

The story of Ukraine has been violent for centuries in a way that few Western nations have experienced

With a background that has been described above, we should not be surprised at events in Ukraine today. The story of Ukraine has been violent for centuries, in a way that few, if any 'Western' nations have experienced over such a long period – 400 years at least.

A major factor in destabilising the region was Khrushchev's decision to incorporate the Crimea into the Ukrainian Soviet Socialist Republic in 1954. This led to uncertainty over the location of the Russian Black Sea Fleet, when Ukraine became independent. This might have been negotiated, until Putin took over as ruler of Russia – he had no intention of doing deals with Ukraine and maintains that stance today. Until the background and history is understood in the 'West' there will be loose talk about Ukraine joining NATO and other 'pie-in-the-sky' notions. The answer must be: "Get real".


RANSOMWARE ATTACK
Your personal files are encrypted
You have 3 days to submit the payment
To retrieve the Private key you need to pay
Your files will be lost

RAPID RESPONSE

Patrick Wragg *reports on the importance of responding to a ransomware resurgence*

The intensity of the ransomware landscape has reached unprecedented levels since the turn of the decade. In 2021, we experienced a record-breaking year totalling 623.3-million ransomware attacks, an increase of 105 percent over 2020 figures.

Come early 2022, however, and research shows there was actually a 23 percent drop in ransomware incidents globally in H1, dropping to 236.1-million attempted attacks and continuing the downward trend that had been observed for the previous four quarters.

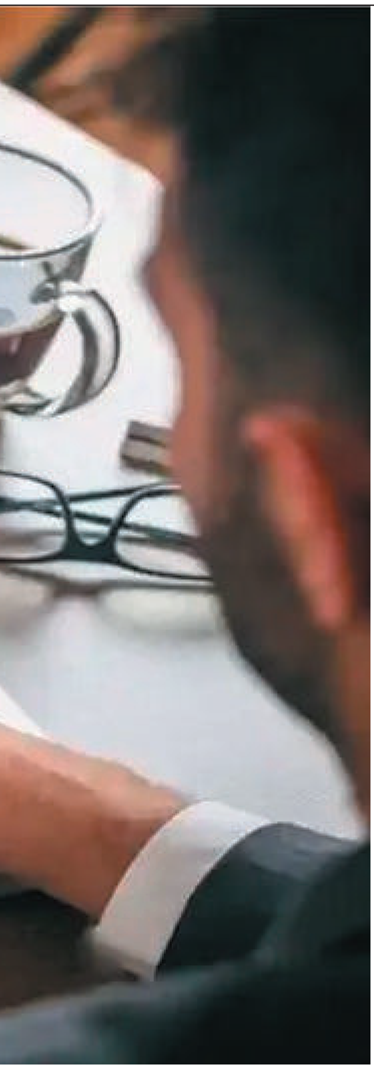
This was in large part down to the disappearance of some of the largest ransomware groups including Conti, REvil and PYSA, owing to the successful actions of law enforcement agencies.

The former, for example, was responsible for an incredibly impactful cyber-attack that paralysed the Costa Rican government in May 2022, disrupting the country's essential services, trade and healthcare systems. It marked the first time a nation declared a state of emergency in response to a cyber-attack.

In response, the US Department of State offered a $10-million bounty for information about the group's leaders, prompting the Conti group to go underground and cease operations.

In spite of successful outcomes such as this, ransomware again saw a resurgence in H2 2022, driven by the return of the LockBit ransomware operation.

Ransomware-as-a-service (RaaS) facilitators such as LockBit (currently estimated to account for over 40 percent



It is estimated that the total global cost of cyber crime will reach $10.5-trillion by 2025

of all global ransomware attacks) are particularly dangerous. Critically, they make sophisticated techniques available to the criminal masses, licensing out code to affiliates who then launch attacks on a broad scale in return for a fee.

The RaaS landscape is particularly worrisome in the current economic climate. As the cost-of-living crisis continues to take hold, more and more people will turn to cyber crime as a means of making money, with sophisticated outfits such as LockBit enabling these criminal opportunities.

Today, the ways in which exploitation gangs coercing victims into paying ransoms is changing. We're witnessing a growing trend towards double extortion techniques involving both the encryption and exfiltration of data, enabling threat actors to add pressure to targets by threatening to leak or sell sensitive information.

All these factors combined suggest that the ransomware resurgence will only continue in 2023 and beyond. In fact, come 2025, it is estimated that the total global cost of cyber crime will reach $10.5 trillion.

Staggeringly, if this were quantified in terms of economic output, cyber crime would be the world's third largest economy, only inferior to the USA ($25.03-trillion) and China ($18.32-trillion).

The statistics ultimately speak for themselves. Now, more than ever before, it is vital that organisations take steps to properly protect themselves in the face of intensifying threats.

So, how can companies make changes to improve their security posture? I believe there are three key areas firms should be focusing in on as a priority.

Improving prevention to combat encryption and leakage. First, organisations should look to rebalance their cybersecurity focus so that prevention plays just as central a role as detection and response.

Threat detection has been a huge focus of organisations and the wider security market, driven by the fear of advanced 'APT' threat actors. Resultantly, preventative controls have often fallen by the wayside – while they are often present in existing security platforms, they are typically underutilised or not properly configured.

While industry statistics tend to suggest that attacker dwell time is in the region of 200-plus days, my experience has shown that the initial stages, access and impacts of an attack can happen extremely quickly, and often in an automated manner. In such instances, those companies relying too heavily on detection are often too late to respond.

Such prevention techniques should be modernised to deal with new-age attacks. The need for capabilities around fileless malware and machine learning-based threat prevention is growing increasingly important and should be aligned with endpoint detection and response capabilities for a full prevention and detection strategy.

Modernising in this manner will aid organisations in preventing threats upfront and ensure you're not seen as an easy target.

Educating employees on phishing threats. Second, organisations shouldn't overlook the value of improving awareness and understanding of phishing among their employee base.

Today, threat actors view the human as the weakest link in the cybersecurity chain, and for good reason. The statistic stemming from IBM research that 95 percent of data breaches involve human error remains prevalent, making the individual a primary target for attackers.

When employees are left to their own devices, even the best technical efforts will fail. Therefore, any new security solutions need to be supplemented with an improved consciousness of the risks and implications associated with specific behaviours.

By far the most common way in which individuals are targeted is with phishing emails that are ultimately designed to infect an endpoint with malware to gain a foothold into their network. Education efforts should therefore centre around the detection of phishing emails with security awareness training, phishing simulations and behaviour change programmes.

If successful, these efforts will also bolster attack prevention, reducing the risk of employees inadvertently downloading a malicious email or attachment that spreads ransomware.

IBM RESEARCH REVEALS THAT 95 PERCENT OF DATA BREACHES INVOLVE HUMAN ERROR

Improving visibility. Thirdly, firms must focus on improving visibility of their networks in 2023.

It's vital for any organisation to regularly assess and reduce gaps and exposure in systems. Further, having clear oversight of your data and who has access to it is also crucial.

Without visibility, entities are operating blindly, putting themselves at much greater risk of being targeted by cyber criminals. By achieving holistic oversight of systems and vulnerabilities, organisations can better prevent threats in the first instance as well as detecting and responding to incidents quickly, before they can cause significant damage.

Further, greater transparency can also enable companies to track the effectiveness of their security measures and adjust them as needed to improve their overall security posture on a continuous basis.

The need to adapt in these various manners has never been more important. Keeping advanced cyber threats at bay is what many organisations aren't equipped to do. As the complexity of threats has increased, security teams have struggled to keep up, relying on legacy security controls that are ineffective at detecting and containing these dangers.

However, making the necessary adaptations to improve protection is unfortunately much easier said than done. A key reason why so many organisations continue to rely on ineffective solutions is because they lack the internal expertise or resources to orchestrate effective strategic improvements.

Enhancing visibility, education and prevention requires skills, technologies and mindsets that many simply don't have. Further, changing that typically requires investing in skilled staff and solutions that command high wages or fees – something that may not be realistic for many companies, particularly in the current economic climate.

So, what's the solution? How can organisations access market-leading expertise and solutions at speed, without breaking the bank? Here, Managed Security Service Providers (MSSP) and Managed Detection and Response (MDR) services can provide the answer. MSSPs are external providers that will supplement an organisation's internal security team, offering market-leading solutions to provide services spanning detection, investigation, threat hunting, response and remediation. In other words, they can help companies to more quickly and effectively respond to incidents to minimise potential costs and impacts.

MORE PEOPLE ARE TURNING TO CYBER CRIME AS THE COST-OF-LIVING CRISIS TAKES HOLD

MDR services are also offered by external parties. Unlike MSSPs, these involve in-depth security monitoring and incident response supplemented with proactive security support. In this sense, MDR providers can work with you to undertake advanced threat testing to uncover hidden vulnerabilities and develop adequate defences and response plans.

The fact that both solutions are delivered by external providers is critical – it removes the need for organisations to invest in expensive and advanced expertise in-house through the provision of access to market-leading security support. In this sense, they can also help companies to bridge the cyber skills gaps in a cost-effective manner.

Here, we'll consider some of the core benefits of MSSPs and MDR solutions, starting with their ability to enable rapid incident response. When it comes to ransomware attacks, time is money. The more time between detection and containment, the more damage will likely be done.

MSSPs and MDRs can provide organisations with on-demand support from experienced security professionals to rapidly detect, analyse and contain security incidents, reducing the chance that ransomware attacks will materialise. This approach eases the load on the internal security teams, saving them hours that would have to be spent sifting through false positive alerts.

Secondly, external providers can help organisations to align with increasingly complex data privacy regulations and ensure that their security strategies are compliant. By providing complete visibility over the security of their environment through proactive reporting and auditing and remote support from 24/7/365 security professionals, MSSP and MDR solutions can help to maintain compliance posture.

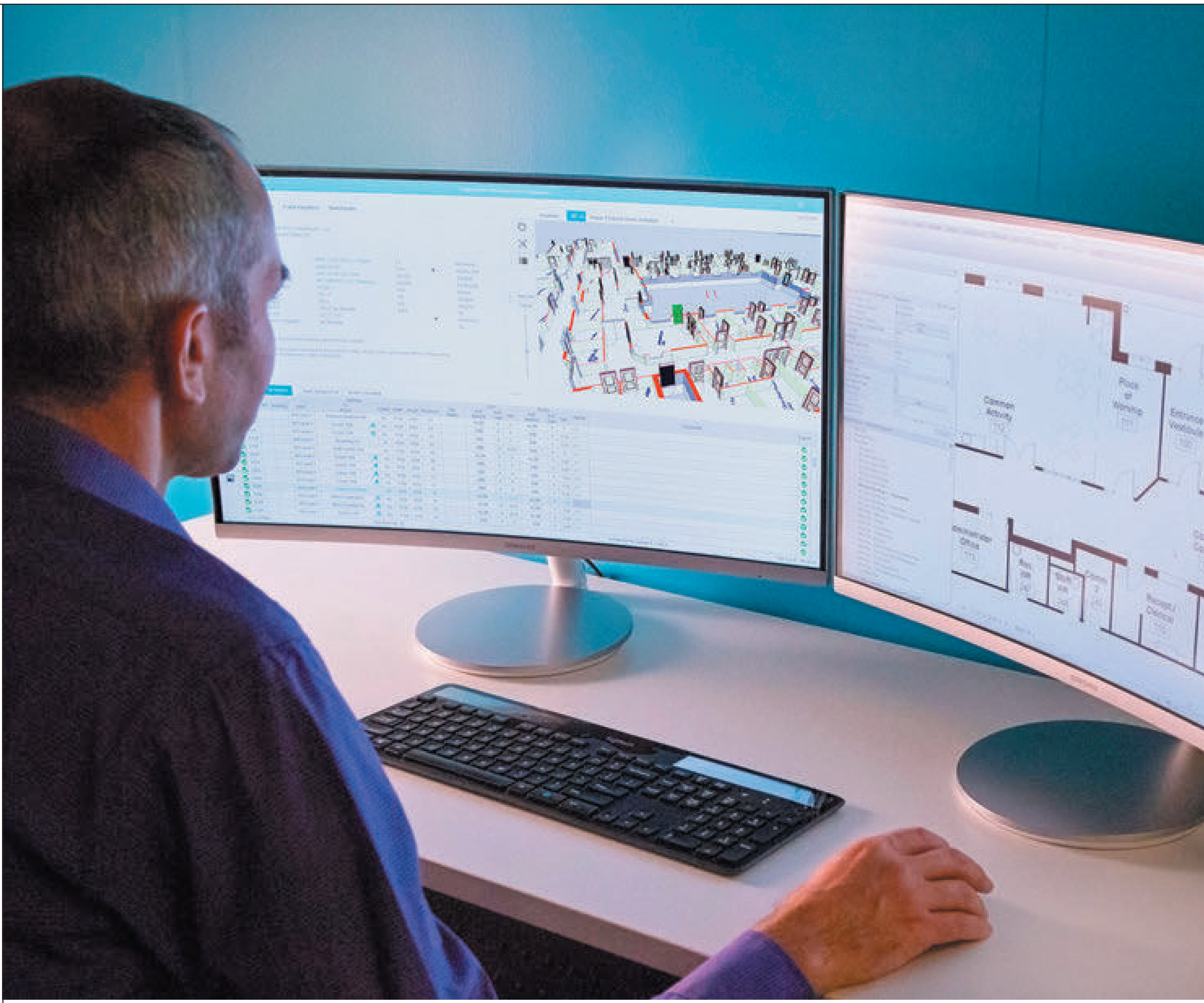
MDR enables organisations to maintain their compliance posture by providing them with complete visibility over the security of their environment through proactive reporting and auditing, as well as remote support from 24/7/365 security professionals who can help prevent intruders from accessing sensitive data and also fill in general compliance gaps.

Thirdly, external support can be the difference in achieving continuous, dynamic security improvement. As threat actors continue to evolve their methods, static security strategies are becoming outdated and obsolete ever more quickly. To ensure that their customers' security strategies are moving in tandem, MDRs and MSSPs will use threat intelligence feeds to identify the types of exploits and attacks cyber criminals are using, and tweak and improve the security posture incrementally over time.

With the threat of ransomware expected to continue to grow over the course of the coming months, it is vital that organisations make the most of these resources and build effective, modern security strategies capable of defending against evolving threats. By working with a trusted and proven external security provider, they will be well placed to mitigate the most critical risks in their environments, and in turn stop ransomware attacks in their tracks ●

Patrick Wragg is Head of IR at Integrity360.

A cyber-attack that paralysed the Costa Rican government in May 2022 marked the first time a nation had declared a state of emergency in response



Picture credit: ASSA ABLOY

NO COMPROMISE

Paul Thompson *discusses how BIM is enabling doorsets to be specified, installed and managed as a sustainable holistic solution*

Sustainability is critical in the built environment, not just when it comes to the construction of a building, but also its ongoing management and maintenance to reduce cost and the overall impact that it has on the environment.

Whether that involves using renewable and recyclable building materials, reducing energy usage or minimising waste – sustainable processes must be implemented throughout all stages of a building's lifecycle.

However, there is sometimes the misconception that sustainability and being 'greener' means having to make compromises when it comes to security, but that is not the case. By using BIM as a tool to manage buildings as holistic systems, it provides information to design, construct and operate facilities safely and effectively, while ensuring security provisions.

The uptake of BIM technology has been rapid, with awareness and usage rising from 13 percent a decade ago to 71 percent in recent years. The evolution of BIM technology has coincided with the introduction of The Building Safety Act, with emphasis placed on the 'golden thread' approach.

BIM is a tool that reduces waste and risk of error, and facilitates the sharing of detailed information throughout the design, construction and operational phases of a project, which ultimately results in more efficient buildings.

By creating virtual reality simulations that allow workers to experience a construction site before work

BIM-enabled tools can be used to extract, develop and update all relevant door design information, including configurations, hardware and performance criteria against each door

begins, BIM can revolutionise better ways of working and outcomes, making the process easier and faster.

Having one easily accessible source allows architects and specifiers to update relevant information automatically without having to manually input each specification, saving time and money, as well as keeping those on site informed. At the specification stage, BIM can also help drive efficiency by integrating and linking to fire certifications and energy performance documents.

Contractors and installers can view all relevant information to assess precise quantities, pricing, compliance, links to supplier websites and installation instructions, as well as being able to track the status of installations across the project much more effectively.

After installation, BIM can be used to monitor the performance of sustainable building systems and elements, such as doorsets and access control. It can also help verify that sustainable buildings operate as intended by tracking energy use, water consumption and waste generation.

The ongoing performance and maintenance of a building may also be monitored via QR code asset management, where all documents and certificates are located in a central software hub.

THE GOLDEN THREAD

Dame Judith Hackett first suggested the 'golden thread' approach to constructing and managing buildings in her report, *Building A Safer Future*. Subsequently, the Building Safety Act was implemented, designed to fix historic and ongoing building safety issues. This now makes building owners more accountable and holds the construction industry to higher standards of building product safety.

BIM enables greater transparency and produces the 'golden thread' of information, allowing building elements such as doorsets to be managed through a single platform – from specification to installation and further ongoing inspection.

However, it is also imperative that holistic systems come from one trusted source responsible for developing and producing complete solutions. Otherwise, there is the risk that suppliers might end up shopping around and piecing the solution together from individual parts, based on cost competitiveness in preference to compliance.

This can not only impact the security provided by an access solution, but it may also make the doorset non-complaint, therefore endangering the occupants of a building in the event of an emergency.

As well as providing access around the property, fire doors are a critical part of the fire compartmentation requirement. New regulations introduced to the Regulatory Reform Order 2005 (Fire Safety Order) contain a requirement for responsible persons in buildings above 11m in height to provide additional safety measures.

This includes things such as providing occupants with fire safety instructions and information on the importance of fire doors. Responsible persons will also be required to undertake annual checks of entrance doors and quarterly checks of all fire doors.

New provisions of the 2022 Building Safety Act came into force on 1 April 2023, including a duty to keep the safety and standard of buildings under review, facilitating improvement in the competence of industry and building inspectors, and a duty to establish a system for the giving of building safety information.

Full implementation of the Act is due by October 2023. So, those responsible for the safety of high-rise buildings in England must register with the new Building Safety Regulator and have their building safety regime in place by this time, or face investigation and potential prosecution.

The 'golden thread' approach provided by BIM is a recommended method to create an effective building safety regime in higher-risk environments such as high-rise constructions.

As well as meeting these new regulations, fire doors are already required to be tested to either BS476 part 22 or BS EN 1634-1, and ideally be certified under a third-party certification scheme, such as Certifire or the equivalent – a position that is fully endorsed by the Door & Hardware Federation (DHF).

> **IT IS IMPERATIVE THAT HOLISTIC SECURITY SYSTEMS COME FROM ONE TRUSTED SOURCE**

Other standards that should be met include BS EN179 Emergency Escape for when the building occupants are aware of the building environment, BS EN1125 Panic Escape for environments used by the general public, and BS EN 13637 Electronically Controlled Escape Systems (for use on escape routes).

When it comes to doorsets and ironmongery, using BIM-enabled tools such as ASSA ABLOY's Openings Studio can truly unlock the full potential of BIM.

Openings Studio provides a direct interface with the building design model and can be used to extract, develop and update all relevant door design information within the model, including configurations, hardware and performance criteria against each individual door.

Utilising this digital collaboration tool enables the specifier to work closely with the manufacturer in real-time to develop the design intent through to a compliant specification.

The application provides visual representations of not only the bespoke product, but also indicative imagery of product in-situ within the 3D model. Each asset carries all relevant technical and design data, and as this is a live working environment it captures and logs progressive design changes throughout design and construction

ASSA ABLOY can seamlessly use this data to provide product specific cost information, but most importantly manufacture and supply the door solution in accordance with the latest design intent.

An extension to Openings Studio has recently been launched, which, through a mobile app, directly accesses this data for capturing production-quality inspections, but also for use during the door installation process, ensuring full validity of the finished product prior to project completion.

Regular inspection and maintenance is essential to ensure safety and security – not just for Higher Risk Buildings covered by the Building Safety Act, but in every building in which the public reside, work or play.

A fully comprehensive inspection should be carried out by a company with competent and certified inspectors (such as ASSA ABLOY Door Group) every three, four, six or 12 months.

EACH ASSET CARRIES ALL RELEVANT TECHNICAL AND DESIGN DATA AND LOGS PROGRESSIVE CHANGES

The app gives access to the as-built door data, enables easy comparison between product at last review and current review, captures details, and facilitates detailed inspections and reporting. It then can capture details of any subsequent completed works, such as repairs or upgrades so this cyclic process can start over again at the next inspection.

Following inspections, detailed reports containing any advice and recommendations on necessary improvements should be compiled, with the knowledge that identifying any potential issues that can potentially impact safety and product performance can be lifesaving.

In the event that any issues do occur, Door Group will prepare a tailored repair proposal to include anything from replacement doors to a regular maintenance programme.

ASSA ABLOY Opening Solutions has used the shift towards greener operations as a driver to innovate and boost business while lowering operations costs. We have implemented a combination of focused initiatives and continuous improvements, as well as ensuring sustainability is closely aligned to, and is a positive enabler of our strategic objectives, aligning with the UN Sustainable Development Goals.

Our increased focus on sustainable buildings is a growth driver and we invest in a sustainable product offering, with accompanying transparency and verification documentation.

Collaborative working is key, and ensuring the entire organisation buys into the concept of a more sustainable future – everyone from those in the factory, to office workers and senior management.

For example, we have recently created a significant reduction in carbon emissions at our Lisburn site through a variety of methods, including advances in packaging, lighting and welfare facilities.

For our business, putting sustainability at the heart of our operations only positively impacts our customers. Whether that's using BIM to specify, install and manage doorsets as a sustainable holistic solution, or in reducing our own CO2 emissions.

Ultimately, the products and ongoing maintenance we offer not only maintain security, but also ensure the safety of a building's occupants, now and in the future ●

Paul Thompson is BIM Manager for ASSA ABLOY Opening Solutions

BIM can be used to monitor the performance of sustainable building systems and elements such as doorsets and access control

Picture credit: ASSA ABLOY

Kestrel TSCM ® Professional Software

Tap Capture Plot (TCP) TM Total Energy Capture with Dimensional Geo-Location Heat Mapping!

Signals Intelligence Support System TM

Developed in Canada the Kestrel TSCM ® is Well Positioned to Hunt in a Complex Signal Environment!

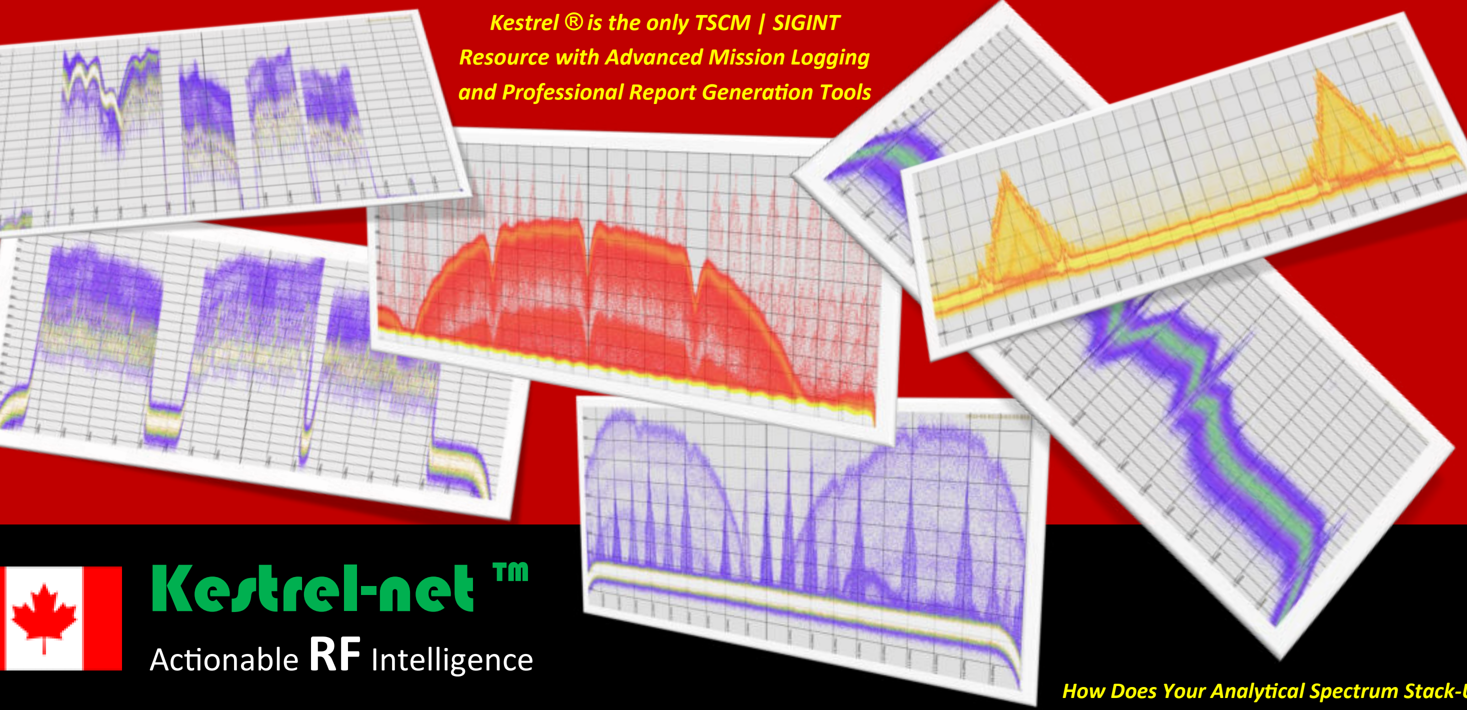
This is Not Just Another TSCM Spectrum Analyzer! | Now You Can Have Tomorrows TSCM | SIGINT Software — Today!

Kestrel TSCM ® Professional Software

Powerful—Disruptive SDR Technology for the Modern TSCM | SIGINT Spectrum Warrior...

Radio-Frequency, Power Line, and Optical Threat Technology Detection within a Standards-Based Software Defined Radio (SDR) Environment

he Kestrel TSCM ® Professional Software is by Definition and Reputation the Leading ext Generation, Mission Critical TSCM | SIGINT Technology for Scalability, Flexibility ase of Use, Low Procurement Cost and Powerful Near Real-Time Deployment Ready odern Features that Address Today's and Tomorrow's Emerging Threat Technology



Kestrel ® is the only TSCM | SIGINT Resource with Advanced Mission Logging and Professional Report Generation Tools

How Does Your Analytical Spectrum Stack-

Kestrel-net TM

Actionable **RF** Intelligence

Professional Development ***TSCM*** Group Inc.

www.kestreltscm.com www.pdtg.ca www.ctsc-canada.com

Picture credit: Photostock

MEGACITY MAYHEM?

Jon Hill *looks to the future as he explores the many security benefits provided by smart interconnected cities*

By 2030, it's estimated half the world's population will live in urban areas. There's even projected to be 41 megacities each with over 10-million inhabitants. Our urban centres are evolving and there's no doubt this kind of population density needs management.

Urban planners, municipal governments and businesses welcoming this influx have to make important decisions about safety and security. Safe cities attract businesses, foster innovation and provide countless opportunities. By working collaboratively, public and private sectors can contribute to a foundation for the success of these cities.

But how do we construct and manage cities so that everything, flows smoothly? In short, how can we ensure that our cities continue to succeed as they grow? A key indicator of success is a city's resilience. We know that the ability to get back to normal as quickly as possible following an incident, unplanned event or emergency is essential as it makes citizens feel safe and allows businesses to continue to thrive. And, since cities are seen as hubs of commerce and leisure, heightened levels of crime – or even fear of it – can call the nature of life into question.

The challenge then is how do we put systems and processes in place that will keep our cities safe while allowing them to adapt and grow as populations increase and technology advances? How do we ensure cities continue to be resilient even as their make-up changes? After all, a city that works is a city you want to live in.

The solution? Smart cities: a living organism defined by the European Commission as: "a place where traditional networks and services are made more efficient with the use of digital solutions for inhabitants and business."

This technology can take many forms, including sensors, data analytics, machine learning and artificial

Detroit's Project Greenlight involved businesses deploying HD video cameras that could live stream to the police at the push of a button

intelligence, and can be used to collect and analyse data on everything from traffic patterns to air quality to public health. It can be implemented in many different ways and careful consideration must be paid to how privacy and cybersecurity are baked into the very core of the system.

In my opinion, top-down approaches that begin with technology are doomed to fail. Instead, municipal leaders should start smaller. They should focus on specific challenges to be resolved. For example, high rates of crime or poor traffic flow. Then look to technology to help.

Increasingly, the resilience of cities depends on the open communication and connection between a variety of systems and organisations. Gone are the days when urban safety was the sole responsibility of law enforcement. Businesses, traffic control, public works, schools, transit authorities, hospital administrations, *etc*. all have important roles to play and can add input into response plans.

For example, the earthquake and Tsunami that struck Japan in 2011 destroyed one of the country's main highways. Within six days, as part of the country's emergency plan, it was completely repaired. This facilitated the movement of supplies and work crews into and citizens out of the area, increasing their resilience. The Japanese government and other organisations were able to determine the best course of action required to address very real, but not obvious problems through advanced communication and preparation.

In many cities, however, and for a variety of different reasons, we see stakeholders who are not collaborating with one another. Business leaders, city planners, municipal infrastructure leaders, fire departments and law enforcement can end up working in silos, ultimately leading to breakdowns in communication, missed opportunities and lapses in city security. This is felt most acutely during an emergency when silos turn into blind-spots and a lack of cooperation can create opportunities for criminal activity, making a city and its people more vulnerable.

SHARING AND CARING

A good example of this is video surveillance cameras. Over 99 percent of camera systems are in private ownership. A mugging happening on the street is most likely to be captured on the cameras of a local business, meaning police regularly need to negotiate access before they can proceed with an investigation. Nobody would suggest the police should have 24/7 access to private systems. But most would agree the process of a business choosing to release this footage when it is in their civic interest to do so should be seamless. Yet, the reality is it is still often painful. It doesn't have to be that way. Cloud-based digital evidence management platforms which allow footage to be shared when the owner decides to do so are the way forward.

As we've seen in Detroit with its Project Greenlight initiative, breaking down "data silos" in physical security is crucial. The city had identified that the vast majority of crime was taking place after 10pm in the proximity of petrol stations. It subsequently launched a programme that involved these businesses deploying HD video cameras that could live stream into the police control at the push of a button.

The resulting deterrent effect was of immediate benefit to the police who had better coverage of these high crime areas. It was also valuable to the petrol stations themselves who now found citizens felt safer and were more willing to visit them. Ultimately it benefitted all taxpayers who were left with a safer community and an appreciation that should an incident unfold, the police were now better equipped to respond rapidly.

Our task is to establish strong foundations that support and maintain the efficient flow of people, assets and ideas in our cities. These foundations must allow our city and community stakeholders to communicate effectively both now and in the future. Because, when given the opportunity to share technology, resources and information, cities can significantly improve the way they meet challenges and solve problems – making an ordinary 'everyday' possible via extraordinary technologies and collaboration.

CAMERAS THAT MONITOR PUBLIC SPACES CAN HELP TO IDENTIFY AREAS WHERE CRIME IS HIGH

Advances in IP technology have brought us better video surveillance, access control, automatic licence plate recognition (ALPR) and powerful analytics. These elements can work together to deliver physical security that helps cities to protect urban areas.

Today's technology can provide security professionals and law enforcement with greater situational awareness. When it comes to ensuring public safety, and maintaining a secure environment, having a complete picture can make all the difference. Smart cities rely on solutions that can allow public organisations to work closely with law enforcement to develop an emergency response plan where video surveillance streams and other data from IP sensors can be correlated, analysed and shared quickly with relevant parties.

Comprehensive unified security solutions offer smart cities the tools they can use to improve overall public safety. And if they choose a provider that enables smarter collaboration between different stakeholders then it has a much better chance of proving effective. A comprehensive security platform that combines video surveillance, access control, ALPR, communications, intrusion and analytics enables cities to work smarter by providing that emergency preparedness, enhanced situational awareness and improved operational efficiency that is so desperately needed.

Specifically, these unified systems can deliver the capability to improve traffic and mobility operations. Traffic systems combined with video surveillance and incident response solutions can help law enforcement identify incidents, communicate detours and coordinate responses faster, resulting in smoother traffic flow and happier citizens.

Improved technology in physical security systems can also deliver the opportunity for collaborative investigation management, which is a boon to law enforcement. By using a safe city-focused security platform, police officers, investigators and security managers can gather and have access to digital evidence from a variety of sources and easily store, manage, review, and share it from within a single application. Incorporating a smart security solution that breaks

▶

down walls and freely shares information (only with those approved to have such access, of course) provides comprehensive response coordination that can literally save lives. An effective public safety strategy requires more collaboration and connectivity between agencies, cities and the private sector. Using physical security components that include video surveillance, ALPR and access control gathering and consolidating data from a multitude of sensors can provide a dynamic – and unified – view to dispatchers and emergency responders so they can make insight-driven decisions during a mission.

> BREAKING DOWN DATA SILOS IN PHYSICAL SECURITY IS CRUCIAL TO MOVING FORWARD

Interconnected surveillance, which can include sensors, cameras and other forms of data collection, can provide a wealth of information to city officials and decision-makers that can help inform policy decisions. Such vast amounts of data can help smart cities make informed policy decisions by providing real-time data on various aspects of urban life. For example, cities are moving towards curb management to improve parking and mobility policies. With the high demand for the curb, managing it has become critical, but many cities lack the essential data needed to make informed policy decisions. Advanced parking management systems can collect and correlate data from multiple sources, generating actionable information that can be used to implement more effective parking and mobility policies in almost real-time. Curb management uses data to help cities make informed decisions on how to improve overall curb space efficiency and compliance.

Interconnected surveillance can also help smart cities identify areas of concern that may require policy interventions. For example, cameras that monitor public spaces can help identify areas where crime or safety concerns are high, allowing officials to allocate resources to address those issues. Similarly, sensors that monitor water quality or temperature can identify areas where environmental concerns may be present, allowing officials to take action to mitigate those concerns.

Another benefit of interconnected surveillance is that it can help smart cities monitor the effectiveness of policy interventions. For example, if a city implements a new policy to reduce traffic congestion, a city could use ALPR and its parking management system to produce weekly occupancy surveys. The data collected in these surveys would allow officials to accurately determine whether or not its free parking initiative is encouraging people to visit the city's core. In the future, city officials could continue to use this data to make other informed decisions around parking to support businesses and tourism with the goal of improving overall access and revenue.

The growth of urbanisation has led to a need for efficient management of the cities, and smart cities have emerged as a solution. In order to ensure that smart cities can safely and securely accommodate the increasing number of residents seen in urban areas across the globe, it's essential for community stakeholders – government, law enforcement, businesses – to leverage advances in physical security systems. Technology plays a crucial role in enabling cities to improve their physical security, with comprehensive unified security solutions such as video surveillance, access control, ALPR, intrusion and analytics forming a powerful solution that can improve public safety, emergency preparedness, situational awareness and operational efficiency. The key is collaboration and balance. Ultimately, cities that embrace new technologies and collaboration can yield stronger, safer communities that citizens want to live in and do business with ●

Jon Hill is an Account Executive for the Transport and Public Space sectors at Genetec – a leading technology provider of unified security, public safety, operations, and business intelligence solutions.

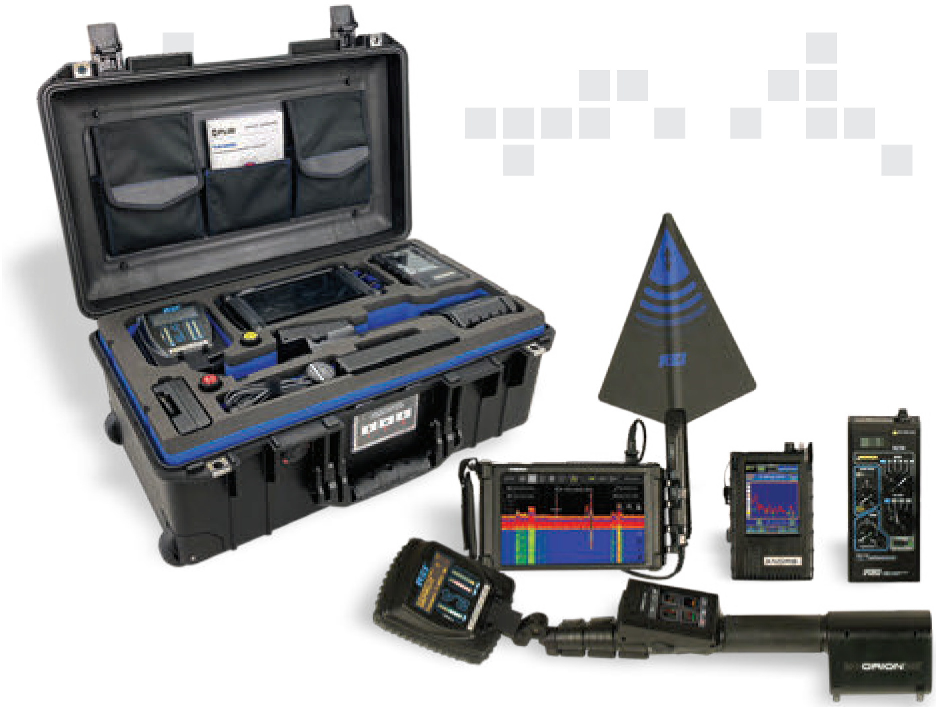
Lack of cooperation between stakeholders can create opportunities for criminal activity, making a city and its people more vulnerable.

Picture credit: Eric Seals

NEW TTK TACTICAL TSCM KIT

lbs/kg

The TTK weighs approximately
25lbs/11.3kg - for easy transport.



MESA® hand-held Spectrum Analyzer

ANDRE® Broadband Detector

ORION® 2.4 HX
Non-Linear Junction Detector

CMA-100 Countermeasures Amplifier

Compact, Portable, Tactical

The TTK Tactical TSCM Kit is packaged for mobility in a durable hard shell carry-on case that includes necessary tools for an effective TSCM sweep.

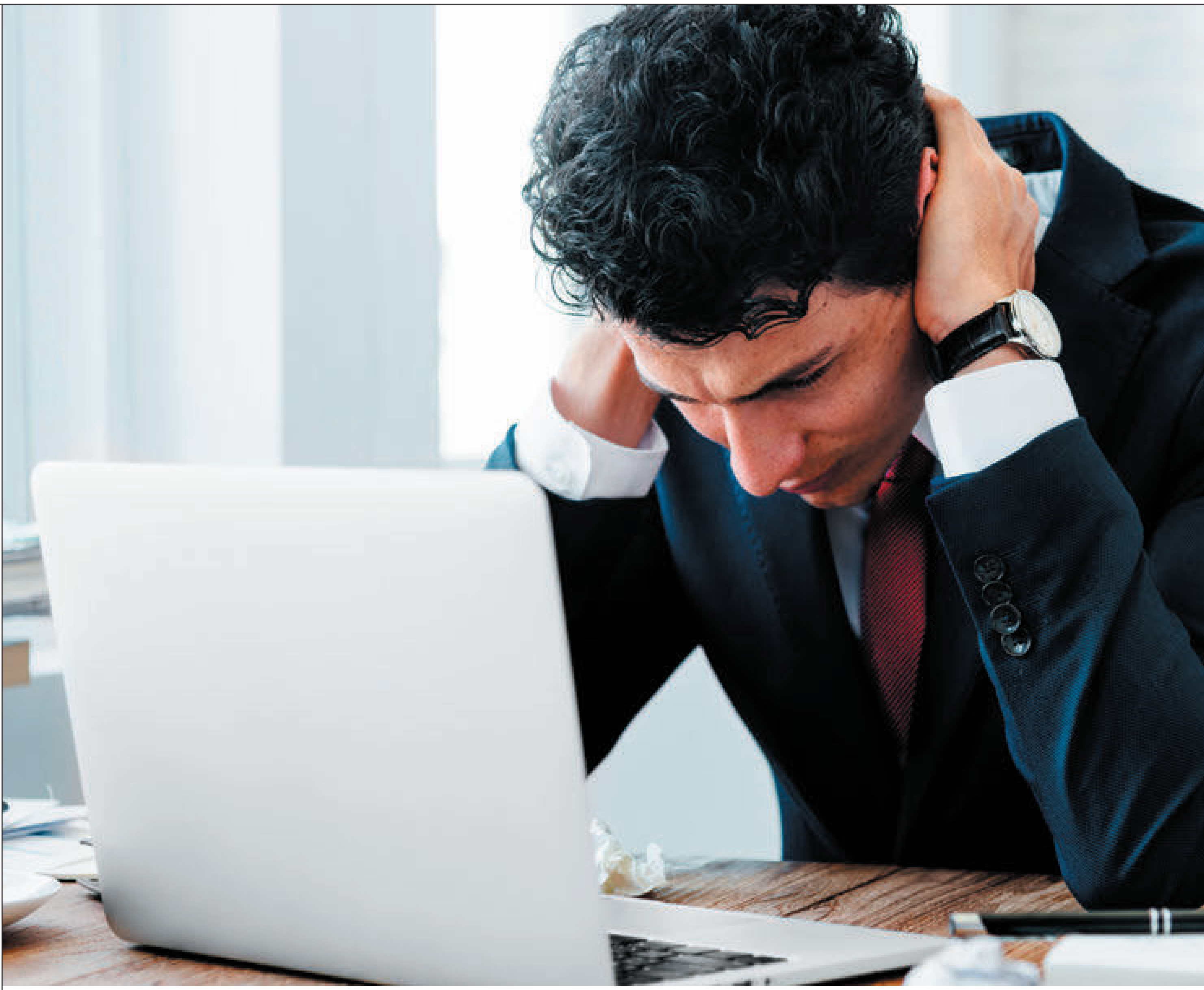
- Locates hidden electronics, transmitters, microphones, and illicit surveillance devices
- Includes Spectrum Analyzer, Broadband Detector, NLJD, Audio Amplifier, *thermal industrial multimeter, and accessories
- Double layered custom foam
- Retractable extension handle
- Quiet rolling stainless-steel bearing wheels
- Weighs approximately 25 lbs/11.3 kg

**Kit contents may vary*

International Procurement Services (Overseas) Ltd
118 Piccadilly London W1J7NW
Phone: +44 (0)207 258 3771
Email: sales@intpro.co.uk

REI®

www.reiusa.net



Picture credit: Adobe Stock

ARE YOU COVERED?

Leyton Jefferies *examines the importance of cyber insurance in the event of an attack*

The recent trend of insurance companies tightening their standards is a challenge for organisations. Recent research by CSI Ltd found that only two in ten (19 percent) security decision-makers are fully confident that their cyber insurance will cover their cyber risk in 2023. Less than a third (29 percent) are fully confident they're compliant with the new stricter terms that insurance companies are now stipulating.

Cyber insurance is designed to protect businesses against internet-based risks, such as data breaches, cyber-attacks and other threats. Policies generally cover expenses associated with a cyber incident such as investigation, legal fees, customer notification costs and regulatory fines.

Yet, the risk level only looks to increase. CSI's research found that 78 percent of organisations believe the current cost-of-living crisis will increase the risk of a cyber threat occurring in their organisation. When asked what factors they anticipate will increase due to the economic climate, 43 percent said fraud and phishing attempts, 45 percent said new and emerging threats, 39 percent said greater risk of supply chain

Only two in ten security decision-makers are fully confident that their cyber insurance will cover their cyber risk

partners being breached and 34 percent said reduced budgets leading to lack of third-party services and tools. So, what is the scale of the challenge in the cyber insurance industry?

In 2021, ransomware disrupted infrastructure and brought down public and private networks as never before. These dramatic events and insurance companies paying hundreds of millions in cybersecurity-related claims each year are being blamed for organisations now facing rising cyber insurance rates, tightening of standards and limiting coverage.

With average ransom payments reaching $812,000 during 2021, the true cost of ransomware is in fact much more when the cost of downtime and reputational damage is included.

> THE VOLUME, VELOCITY AND VARIETY OF CYBER ATTACKS IS GROWING EXPONENTIALLY

The uptick in cyber-attacks and pay-outs has meant mounting losses for cyber insurance companies and has forced change. Insurers are becoming much stricter about what risks they will underwrite in a "hardening of the market". One major insurer underwrote 80 percent of the risks presented to them last year. Now it's just 10 percent.

Despite this, cyber insurance isn't going anywhere, in fact, the market is set to grow drastically over the next few years. The global cyber insurance market was considered to be worth $6.15-billion in 2020. It's projected to grow from $7.60-billion in 2021 to $36.85-billion in 2028 at a CAGR of 25.3 percent during the period.

Digital transformation means that the attack surface is now larger and more diverse than ever. The traditional network perimeter no longer exists, *identity* is the new perimeter. The volume, velocity and variety of attacks is growing exponentially. Overall security spend is increasing to record highs, but unfortunately so are the costs of successful attacks.

With dynamic, personalised attacks, hackers will have significantly more power to cause damage. Then there are the unknown threats. Given the pace of technological development, it's likely we will be hit within the next few years by forms of cyber-attacks that are hardly conceivable today.

A single click or minor misconfiguration can lead to a major breach. And if your organisation fails to meet the security requirements defined by the insurance provider, your policy will be in jeopardy.

The huge shortage of cyber-security workers is also adding to the problem and means that it will only get worse as the risk can no longer be transferred to the insurance company.

To protect your organisation, satisfy cyber security insurance requirements and ensure rapid recovery if you are breached, security needs to be a continuous process. Companies need to demonstrate that they have taken adequate steps to safeguard their IT infrastructure before they are granted cyber insurance. It's essential to be proactive and implement effective security controls to thwart cyber-attacks. A reactive approach to identifying and responding to a cyber-attack is no longer acceptable and will make it difficult to obtain cyber insurance and put the company at significant risk of financial and reputational damage.

While the prospect of having no cover may be daunting, it perhaps serves as a point of reflection for companies to adequately reassess their own security posture and strengthen it where required. So how can organisations ensure they are operating on the front foot when it comes to cyber security?

IMMUTABLE BACKUP AND DISASTER RECOVERY

One of the essential controls for an organisation is immutable backup and disaster recovery. Backups allow companies to restore their systems and data quickly after a cyber-attack. While immutable backups guarantee that the data is not altered or deleted, even by an attacker with administrative privileges. This ensures that a company can quickly recover from an attack without losing data or compromising the integrity of it.

ENDPOINT DETECTION AND RESPONSE (EDR)

EDR is another control that should be included as part of an organisation's arsenal to reduce cyber risk. EDR technology provides real-time visibility and response capabilities into the endpoints of a company's network. This allows security teams to detect and respond to threats quickly.

MANAGED DETECTION AND RESPONSE (MDR)

MDR is a service that combines technology with human expertise to monitor a company's network and identify potential threats. It provides proactive defence against attacks by detecting and responding to them before they can cause harm.

PATCH MANAGEMENT

A significant proportion of external breaches are due to unpatched vulnerabilities. A poor regime can have catastrophic consequences on systems, personally identifiable information, and intellectual property.

Keeping software and operating systems up to date with the latest security patches is crucial to prevent known vulnerabilities from being exploited by attackers. Patch management as a discipline also plays a crucial role in improving stability and functionality.

ASSET MANAGEMENT

This involves conducting and maintaining an inventory of your network environment and all cyber-enabled technologies including software and hardware. This will help to identify all the technologies that can be hacked. Once you know what devices need to be managed and secured, you can then implement security around them.

MONITOR ADMIN RIGHTS

Linked to asset management should be the continuous and proactive investigation into

▶

privileged accounts. This includes deciding whether old accounts are needed and looking at whether accounts can be restricted or disabled. It also comes down to investigating all the requests for access to certain files and applications and making sure that they are just being accessed by those that need it within an organisation. This action needs no other financial investment beyond the security team's time, but can reduce the attack surface area of an organisation significantly.

SECURITY OPERATIONS CENTRE (SOC)

This is a centralised function for the monitoring of threats in the network. It concerns people, processes and technology to continuously monitor and protect an organisation's assets including intellectual property, personal data, business systems and brand integrity. The SOC team is responsible for an organisation's overall cyber security strategy. It is the central point of collaboration in coordinated efforts to improve an organisation's security posture while preventing, detecting and analysing and responding to cyber incidents.

EMPLOYEE EDUCATION

Employees are your most important line of defence when dealing with social engineering attacks so it's crucial they are aware of the risks. Regular training can help to make complex cyber threat issues understandable for everyone. It's important that staff understand the 'why' behind the instruction to create a security-first culture.

Make security education consistent, give clear advice and make it very accessible, so that people know what to look for and what to do next, rather than decide for themselves. Reward employees when they do something security focussed. Let the reward be seen and continually build to a zero-trust culture.

MULTI-FACTOR AUTHENTICATION (MFA)

MFA requires users to provide more than one form of authentication before providing access to a system or application. This additional layer of security helps to prevent unauthorised access and protects against phishing attacks.

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR)

Businesses are using their imagination – along with practical security consultation – to identify and remediate risk. SOAR is an additional layer that enterprises are exploring as a way of stitching together disparate toolkits that are often labour intensive and require skilful calibration and configuration. For example, it enables you to integrate security, IT operations and threat intelligence tools to achieve a more comprehensive level of data collection and analysis – even across different vendors. This is important as simplifying and streamlining your toolset significantly reduces your likelihood of breach.

SOAR is a great example where companies are really trying to innovate their security posture.

Despite their best efforts, many businesses unfortunately will still be attacked, so having the right business continuity practices in place and cyber insurance will be critical to survival. Cyber insurance can bring peace of mind for organisations. Remember, it's not a case of 'if' but 'when' you may fall victim to a cyber-attack. Cyber insurance can help you recover from external attacks from bad actors as well as oversights from within the business, putting the focus back on the core operations. However, taking a proactive approach to reducing your risk profile will significantly increase your overall security stance – which is a win, regardless of whether you have cyber insurance or not ●

Leyton Jefferies is head of cyber security services, CSI LTD.

If your organisation fails to meet the security requirements defined by the insurance provider, your policy will be in jeopardy

Picture credit: Adobe Stock

MGT europe

DroneTERMINATOR

USING EVOLUTION JAMMER TECHNOLOGY

- **DETECTS**
- **TRACKS**
- **NEUTRALIZES**

DroneTERMINATOR utilizes RADAR on the Ku / X band, 2 Watt, 1 GHz bandwidth
Long-Range Radar System to detect UAVs at a distance of up to 6 km,
with micro-drones typically detected at 1-2 km realistically

JAMMING FREQUENCIES:

400 MHz - 900 MHz - 1500 MHz - 2.4 GHz - 5.8 GHz in n. 2 bands

FEATURES:

- Fully modular smart design
- Precise and fully programmable operation mode for each R.F output
- Wideband, clean and precise band occupation
- Very good Narrowband and Wideband spectral purity
- Flexible and multiple User interface options
- Standard USB and Ethernet interfaces available for multiple purposes
- Software oriented approach allows for long product life expectations
- Careful D.C. Power source design choices for efficient power supply utilization
- Waterproof cabinet, rugged and reliable construction
- Linux based, User friendly Graphical User Interface with 7" LCD color Multitouch Display

MGT Europe www.mgteurope.com

ELECTRONIC COUNTERMEASURES

IPS EQUIPMENT & SWEEP TEAM SERVICES

NEW REI MESA MOBILITY ENHANCED SPECTRUM ANALYZER

NEW ANDRE DELUXE 12GHZ WITH ULTRASONIC PROBE

VIDEO POLE CAMERA 2.0 INSPECTION TOOL

EDD-24T NON LINEAR JUNCTION DETECTOR (HANDHELD)

TSCM TRAINING
COURSES &
CERTIFICATION
UK/US/GLOBAL

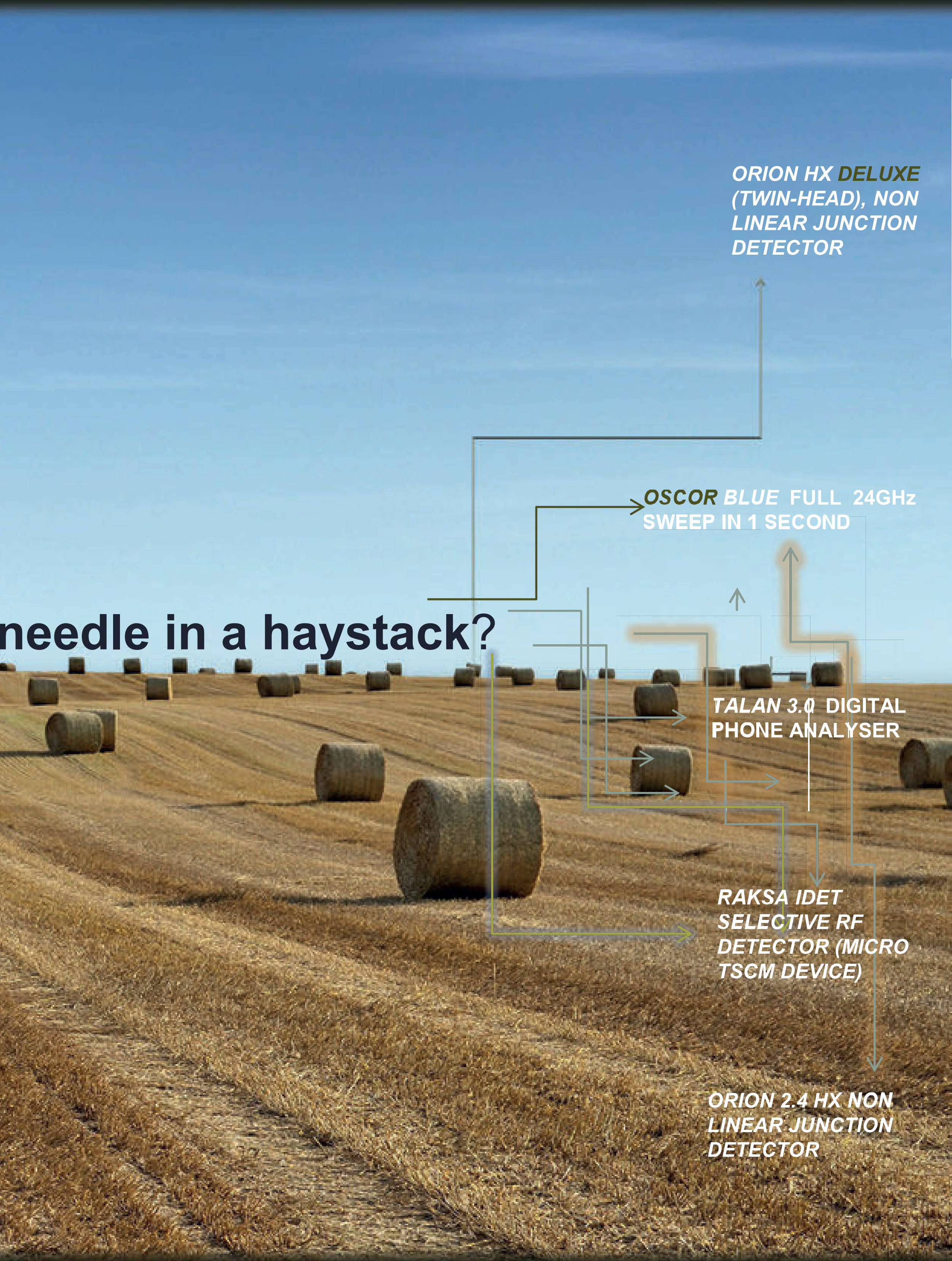
Looking for a

For details, demonstrations, sales and 24/7 response, contact:

International Procurement Services (Overseas) Ltd,
118 Piccadilly, London, W1J 7NW Email: sales@intpro.com
Phone +44 (0)207 258 3771 FAX +44 (0)207 724 7925

Rapid Quote:

Photograph or scan this image with your smart mobile to automatically request info / call back.



ORION HX DELUXE (TWIN-HEAD), NON LINEAR JUNCTION DETECTOR

OSCOR BLUE FULL 24GHz SWEEP IN 1 SECOND

TALAN 3.0 DIGITAL PHONE ANALYSER

RAKSA IDET SELECTIVE RF DETECTOR (MICRO TSCM DEVICE)

ORION 2.4 HX NON LINEAR JUNCTION DETECTOR

TSCM Equipment supply, training and de-bugging services

The preferred choice of Government & Law Enforcement Agencies worldwide.

Web: **www.intpro.com**

BUSINESS CONTINUITY

Mat Clothier, *discusses the importance of managing & configuring systems in accordance with SOC 2 Type 2*

The demand for high-level security within organisations has substantially increased as the technology industry continues to expand. Despite the development of security measures within applications and systems, some of them are yet to be fully protected from viruses and cyberattacks. To ensure businesses maintain the privacy and security of their data, it is important to continually monitor the storage of their information – keeping it safe and taking any necessary precautions to prevent such breaches.

Auditing systems is a great way for organisations to keep their systems in check and monitor for upcoming updates and compliances. As the need for security increases, so does the number of auditing software available – some valuable and some not. When auditing their estate (servers, desktops, laptops, network infrastructure *etc*), the most important aspect organisations should check is that they are complying with the latest industry regulations – and with these changing regularly, they must be continually monitored. An easy and reliable way to ensure this is by running a SOC 2 Type 2 report – these are especially useful to companies who use third-party services, such as the Cloud.

A SOC 2 Type 2 report runs and provides an in-depth analysis and thorough examination of

By managing configuration drift effectively, businesses can ensure their estate is prepared for any unforeseen changes in these environments

a company's security status, including a report on its vulnerabilities and threats. It also offers recommendations on how to improve any systems that are lacking or falling behind on current security measures/protocols. By running a Type 2 report, organisations can gain a SOC 2 certification, which essentially demonstrates that they are running on the most beneficial and efficient systems while keeping their data stored correctly and safely. This certification also proves that the organisation is protecting both the business and its customers from stolen information and bad actors.

Configuration management tools (also known as CM tools) are software tools that assist in the management and maintenance of an organisation's technological infrastructure. These tools typically provide a way for businesses to monitor information and updates within all systems of their estate – for instance, when new regulations, updates or software versions arise that must be complied with. Such tools allow businesses to stay one step ahead and always be prepared for any upcoming changes they need to make. This allows businesses to create a security development plan and allocate time, money and resources to these adjustments. Staying ahead of the changes allows businesses to remain secure and minimise time spent playing catch up with developing software – potentially leaving them vulnerable to an attack while their efforts are focused on making the required updates.

Having CM tools in place helps organisations comply with regulatory requirements and assists in achieving optimal operational efficiency. Certain tools also offer automation services that allow businesses to automate tasks such as rolling out new applications, systems or updates – keeping them ahead of the game and all systems in the best state, reducing the risk of gaps appearing in technology, and therefore increasing the level of security.

Configuration management tools provide great benefits to organisations and can be seen as essential for maintaining business continuity while ensuring compliance with regulations. The primary benefit is that they automate the process of setting up, configuring and maintaining IT systems, while reducing the efforts of employees so their time can be focused elsewhere.

It is becoming increasingly common to see in the news that companies and organisations of all sizes are suffering from cyberattacks and security breaches, with sensitive customer data always at the forefront. According to the Cyber Security Breaches Survey 2022, almost a third (31 percent) of businesses reporting attacks were targeted at least once a week. With these ever-occurring incidents, it is no wonder that more businesses are looking to ensure their own cybersecurity practices are up to date and fully compliant with the latest rules and regulations.

Mishandled data can result in higher vulnerability within organisations, in turn leading to the theft of data and the potential for ransomware and other malware attacks. As previously discussed, one way in which companies can reduce the opportunity for security breaches is by achieving SOC 2 compliance.

SOC 2 provides an assurance to organisations that they have implemented the necessary security controls in order to protect not only their own but customers' personal data too. This certification is becoming progressively important for businesses in the digital age, as customers become more aware of the risks of sharing their personal information online. By proving their security through compliance, companies can provide peace of mind to their customers, allowing trust to be built.

There is a number of benefits that come with achieving SOC 2 compliance, the most important being the reduction of vulnerabilities to cyber-attacks, and the overall building of a more reliable and secure infrastructure. Additionally, it demonstrates to customers that the organisation in question takes its data security seriously and is committed to protecting its information. This can help to build trust and confidence in its brand. It can also give a competitive advantage over other businesses that have not yet achieved compliance; proving to their customers their ongoing dedication to security. Finally, it can help companies to streamline their internal processes and ensure that everyone in the business is aware of and adhering to best practices when it comes to data security.

AS THE SECURITY NEED INCREASES, SO DOES THE NUMBER OF AUDITING SOFTWARE AVAILABLE

Achieving SOC 2 compliance isn't an easy task, but it's well worth the effort for businesses who want to show their commitment to safeguarding their customers' data. Not only that but actually protect their business from bad actors with malicious intent.

Through countless updates and CM tools it can be difficult for organisations to keep up, and if businesses start to fall behind this is when configuration drift can occur.

Configuration drift happens when a company's systems gradually change over time, often without being noticed and leading to them becoming more and more difficult to maintain. This can result in higher operational costs and greater gaps in security, so it is important for businesses to regularly monitor for updates – ensuring they do not drift away from their optimal and most secure states.

Regular monitoring allows organisations to catch any issues early on and make any necessary adjustments before they cause larger problems or become costly to fix. It also encourages systems to operate in the most efficient and secure way – and the way they are intended to. Additionally, with many teams being asked to do more with less, these automated tools are an easier way for employees to monitor the changes rather than finding them manually. With potential personnel or role changes frequently happening this ensures continuous monitoring for compliance, regardless of who is currently in post. It also reduces the amount of valuable employee time spent on checking for and completing updates.

Configuration management tools play a large part in avoiding configuration drift, this is because they allow organisations to monitor possible drifts and

▶

plan ahead. These tools compare the changes in a business' systems and environments over time and provide visibility and control of their configuration flaws, allowing them to proactively act on misconfigurations in a calculated and thoughtful manner.

SOC 2 CERTIFICATION SHOWS A BUSINESS IS RUNNING THE MOST EFFICIENT SYSTEMS

Controlling configuration drift over time can prove beneficial for any organisation as it prevents unnecessary changes to the technological infrastructure and makes businesses more secure from outside threats. It also allows the business to adapt to changing conditions and be prepared for them when they inevitably happen. Managing the ever-growing list of devices, software and company-specific protocols can be a difficult and lengthy task, not to mention ensuring they also align with industry standards.

However, by proactively dedicating time to configuration management, organisations can prevent drift and provide a stable foundation for their infrastructure, including their applications and systems. By managing configuration drift effectively, businesses can ensure that their estate is futureproofed and prepared for any unforeseen changes in these environments.

SOC 2 Type 2 reports are continuously generated over a period of time rather than a one-off check, therefore monitoring potential configuration drift over time and proving that controls are followed routinely and used effectively making the estate more reliable and secure. This will in turn reduce the likelihood of any unwanted cyber-attacks or threats.

Organisations that adopt SOC 2 Type 2 compliance are taking the necessary steps to ensure their systems are in a secure state and their data is stored safely – protecting both the business and their customers. Monitoring over time can help organisations identify any potential security flaws and make the appropriate changes to mitigate any risks. Through utilising CM tools, businesses avoid potential configuration drift, ensuring that all systems remain in a secure and compliant state. By taking the necessary precautions, organisations can maintain their SOC 2 Type 2 compliance and ensure their data is secure.

While compliance with rules and regulations is one of the more important reasons to keep software and a company's entire IT estate up to date, there are many other reasons to stay ahead of the updates (usability and speed of applications/systems, for example). By putting in the work and protocols before problems arise, organisations are taking active steps to protect themselves and their customers as well as allowing their employees to be more streamlined and efficient. The process of checking for compliance doesn't need to be hard and cumbersome, if done routinely and with the right tools, it should feel like a simple routine check. The ongoing simple checks and implementation where appropriate will save companies time, money and a damaged reputation due to non-compliant software. This type of damage is avoidable with a little foresight and consideration ●

Mat Clothier is CEO and Founder of Cloudhouse.

Configuration management tools play a large part in allowing organisations to monitor possible drifts and plan ahead

TSCM & SECURITY SOLUTIONS

Delivered globally by the world's largest TSCM company

TSCM solutions

- TSCM Inspections & Live Monitoring
- CYBER TSCM
- Equipment Design & Manufacture

  - *Sentinel, BlackLight & Lynx*
- Equipment Supply & Gap Analysis
- Accredited TSCM Training (govt only)
- Physical Security Reviews

Security solutions

- Cyber Forensics
- Drone Forensics
- Cyber Incident Response
- Physical Penetration Testing
- Protective Security Services
- Threat Briefings & Consultancy
- Secure Communications

About QCC

Founded in 1999, QCC has grown to become the world's largest TSCM company with capability unique to QCC. We provide a comprehensive global service to commercial and government clients worldwide.

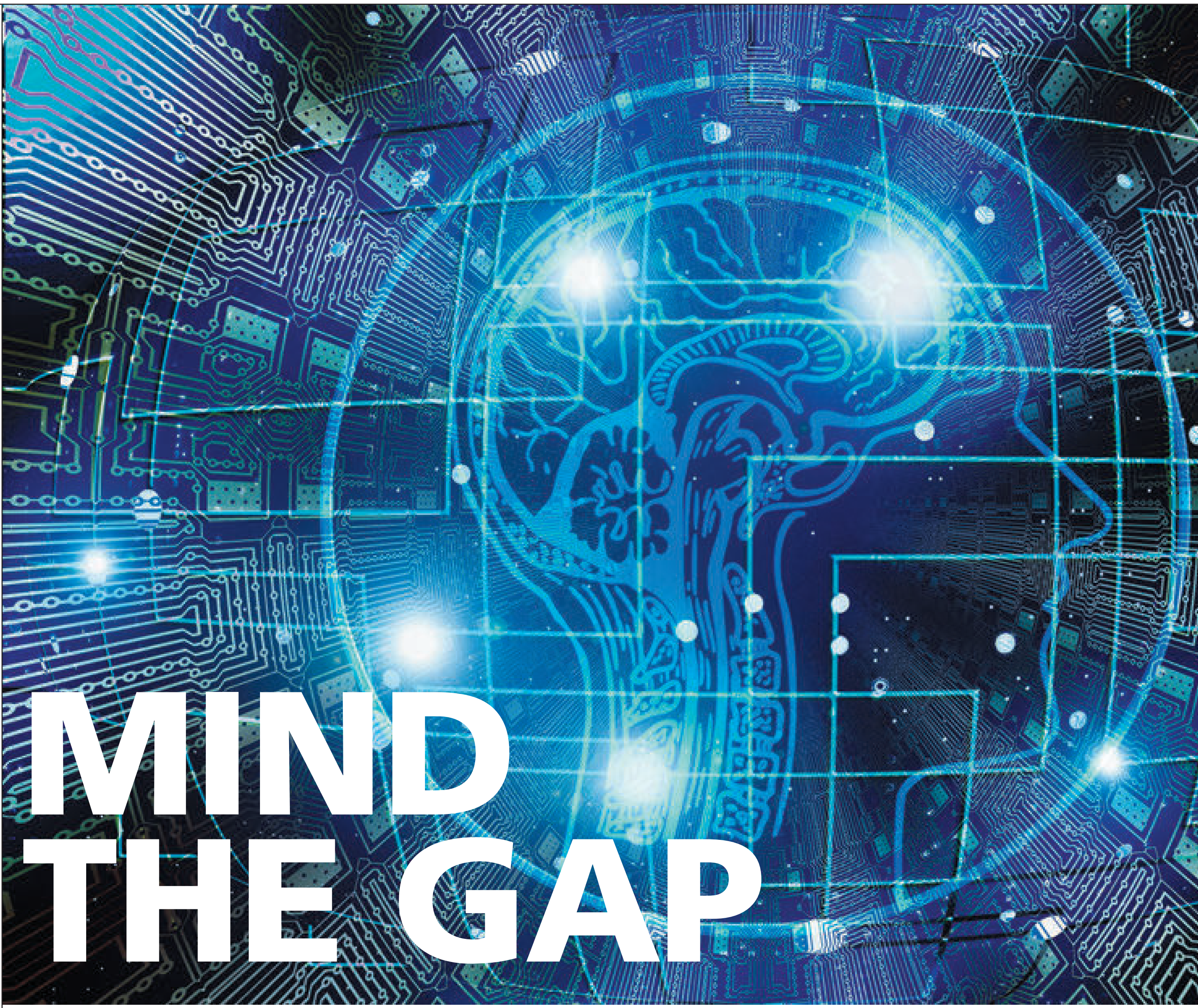
We are serious about what we do, and adopt a partnership approach to directly reduce our clients risk exposure.

LONDON
T: +44 207 205 2100
E: contact@qccglobal.com

SINGAPORE
T: +65 3163 7100
W: www.qccglobal.com

ISO 9001 CERTIFIED · ISO 27001 CERTIFIED · ISO 45001 CERTIFIED · ISO 14001 CERTIFIED · UKAS ISO 17025

Keeping your business, ***your*** business !



MIND THE GAP

Tim Wallen *discusses whether or not technology can plug the cyber skills gap*

Enterprises looking to attract and retain cybersecurity staff have a challenge on their hands in 2023. ISC^2 estimates that the global cybersecurity workforce became 4.7-million strong at the end of 2022, inflating 11.1 percent with the addition of 464,000 newly employed security professionals. However, despite this, the cybersecurity workforce gap actually expanded last year, growing at more than twice the rate of the workforce with a 26.2 percent increase year-over-year.

The industry is now faced with the mountainous task of bridging a worldwide gap of 3.4-million cybersecurity workers if cross-industrial enterprises are to be properly protected from modern cyber threats.

In the UK alone, the Department for Digital, Culture, Media and Sport (DCMS) estimates that approximately 697,000 businesses (51 percent) have a basic skills gap. In other words, the people responsible for cybersecurity within those organisations both lack the confidence to carry out the tasks outlined in the government-endorsed Cyber Essentials scheme and aren't getting adequate support from external security providers.

As you might expect, one impact of these skills shortages is an increased susceptibility to breaches. Fortinet's 2022 Cybersecurity Skills Gap Research Report shows that eight in 10 organisations have suffered from at least one breach that could have been avoided with better cybersecurity skills and/or awareness.

Given the potential impacts of breaches, this is a major problem. IBM's *Cost of a Data Breach Report 2022* shows that the average total cost of a data breach reached an all-time high $4.35-million last year – a figure that tallies up with Fortinet's analysis, which reveals that a staggering 38 percent of enterprises reported breaches that cost them more than a million dollars to remediate.

Unfortunately, the impacts that come with having inadequate cyber skills aren't solely financial. One independent study has shown that more than half of office workers would actually reconsider working for an organisation that had fallen victim to an attack, with only one in three saying they would be unfazed. In this sense, incidents can be so disconcerting that they may exacerbate staff turnover, creating a vicious cycle that sees resource further depleted.

While AI isn't likely to fully replace cybersecurity workers, automating consistent and repeatable processes can free them up to focus on higher value tasks

These financial and mental strains are only expected to worsen moving forward. At present, we're not seeing the flow through required to tackle the cyber skills gap effectively. According to the DCMS, there were 4,400 core cyber security postings each month in 2021 – an uptick of 58 percent on 2020 averages. And while there have been roughly 7,500 new entrants into the cyber security labour market each year, there have also been about 4,600 people leaving the profession. For this reason, it is estimated that we're currently experiencing an annual shortfall in cyber security personnel of more than 14,000 in the UK alone.

Any idea that we can simply "ride out" the skills gap is unrealistic. Something needs to change – without action, the current skills crisis will only continue to get worse and worse year after year, placing ever greater strains on already limited cyber resources.

Organisations should therefore work to support their security teams wherever they can, enhancing their toolkits and empowering them to work in the most effective and efficient manner possible. Here, technologies can help. While AI isn't likely to take the place of cybersecurity workers any time soon, automating consistent and repeatable processes can free up workers to focus on higher value tasks.

With the right solutions, firms can take the pressure off security teams, helping them work more productively while improving their overall employee experience. Not only will this make it easier to retain talent, but it can also serve to reduce staffing shortages without requiring additional staff.

So, exactly where and how should enterprises leverage automation to the benefit of security? This is a question to which the answer must be very carefully considered. While it can be tempting to acquire every shiny new solution under the sun, such an approach can do more harm than good.

More doesn't always mean better. An expansive range of automated solutions will cost a lot, and that's not going to be desirable or sustainable for many firms given the current economic climate. Equally, it can make the lives of security professionals that need to learn to navigate all these various applications more complex. Furthermore, many solutions can become redundant, duplicating capabilities, while the need to manage multiple platforms will contribute to alert fatigue.

Instead, organisations should work to optimise their security support network by ensuring the logical convergence of technologies that accelerate detection and response by fusing telemetry and automating responses across the enterprise technology stack.

Security professionals need to be supported with platforms that provide efficiencies of scale to help build defensive capabilities. Any technologies should therefore empower them by providing a comprehensive overview from which cyber threats can be managed and business risk reduced.

That might be achieved by surfacing high-value true positives and providing threat context to prioritised cases, or by providing data to optimise the efficacy of the broader security infrastructure. Above all, these solutions need to be easy to use, freeing up security personnel to focus on solving genuine cyber security issues.

There are several technologies that should form central pillars of the automated technology stack, user and entity behaviour analytics (UEBA) being a prime example.

Using advanced machine learning, UEBA works by building baselines for normal behaviour for every user, peer group, and entity in a corporate network, instead of applying predefined rules for standard behaviours. In doing so, UEBA is then able to identify activity that strays away from these baselines to detect abnormal and risky behaviours which may not be immediately obvious otherwise.

It is a technology capable of providing tailored detection to each user, so that analysts can spot, prioritise and manage anomalies easier. Indeed, with UEBA, analysts are able to accelerate threat hunting with capabilities that serve to reduce alert fatigue and drive professionals to focus on those threats that genuinely require remediation. As a result, UEBA can provide vital support in mitigating risks, damages and data loss incidents by eliminating false positives and cutting down response times significantly.

THE INDUSTRY NEEDS TO BRIDGE A WORLDWIDE GAP OF 3.4-MILLION CYBERSECURITY WORKERS

Alongside UEBA, security operations centres should also tap into threat intelligence to add context to alerts and improve outcomes.

Successful security relies upon the ability of organisations to understand their vulnerabilities and deploy adequate knowledge and intelligence to mitigate potential threats. While indicators of real risk are often difficult to identify, and preparation for every single new threat is impossible, making the best use out of the intelligence sources that are available can help security professionals to prioritise threats and broaden their armouries.

Threat intelligence automation can be used to achieve this, enabling organisations to collect and analyse data on the latest threats. Be it security vendors, intelligence groups or other connections, leveraging information from a wide range of sources can help in proactively identifying trends and initiating security activities to stop malicious behaviour and avoid incidents.

It is a means of logically informing security decision making. By combining intelligence and previous experiences from many organisations into a single, central feed, security teams can make better strategic choices to help mitigate attacks.

Of course, manually trying to identify threats within large volumes of collected information can feel like finding a needle in a haystack. For this reason, automation is key. Analysts should automate event interrogation, screening hundreds of thousands of indicators of compromise (IOCs) across a variety of internal and external intelligence feeds to evaluate the data based on known attacks. In doing so, they can benefit from an accelerated ability to correlate multiple threat indicators generated inside their perimeter with external threat IOCs.

In addition, security teams should also look to embrace security orchestration, automation and response (SOAR). SOAR is all about alert aggregation and prioritisation. It's an incident detection and response technology centred around workflow and playbook

▶

automation that accelerates threat investigation and remediation by guiding analysts towards consistent and optimal responses.

By automatically pulling all cyber incidents and supporting data together in one place, it can provide structured workflows for day-to-day security analyst tasks, serving to decrease response times and helping analysts identify and resolve incidents fast. Through correlating and analysing data, SOAR can present all contextual information and intelligence, allowing security teams to react more efficiently and effectively. Not only can this help to improve productivity, with SOAR capable of recommending a response so analysts can simply approve or execute a decision, but it can also reduce alert fatigue and information overload.

8 IN 10 ORGANISATIONS HAVE SUFFERED FROM A BREACH THAT COULD HAVE BEEN AVOIDED

Without question, solutions such as UEBA, threat intelligence automation and SOAR can help organisations to bridge the cyber skills gaps by empowering security professionals and in the process freeing them up to focus on additional high-value tasks.

Encouragingly, organisations are beginning to recognise these merits. Indeed, automation is becoming increasingly prevalent in cyber security, with 57 percent of firms having already adopted it and an additional 26 percent planning to do so in the future. However, businesses planning to invest in such technologies must plan wisely, particularly in light of current economic conditions.

According to Gartner's 2022 Board of Directors Survey, business leaders now acknowledge that security incidents can have significant impacts on an organisation – so much so, that 88 percent of boards now consider cybersecurity a business risk, this up from 58 percent five years ago. This is positive, but professionals must still invest wisely. Any strategic failures could serve to undermine this newfound appreciation of security, so firms need to be cost-effective in their methods while also improving performance – ideally with no mistakes.

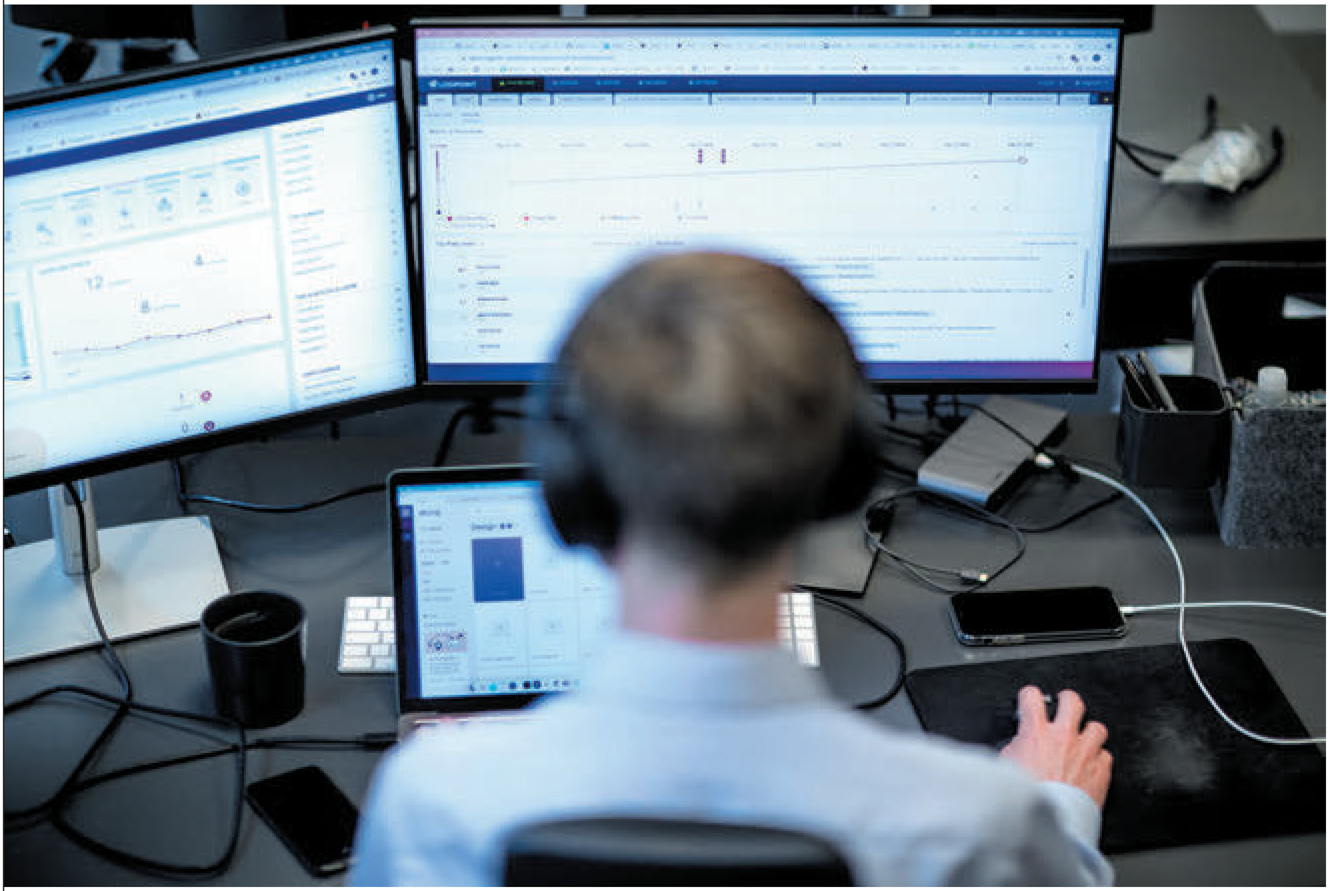
With this context and the needs of modern security professionals in mind, embracing a converged security solution makes sense. Enabling organisations to combine multiple tools into one platform, converged solutions can reduce the number of point solutions and vendors that security teams need to manage. This is key, as complexity in IT departments is typically driven by integrations, technology evolution and changes to scope. Therefore, selecting a solution with a broad set of features limits complexity, cost and friction.

Performance can improve too. By combining SIEM centralised monitoring with automation, workflows and a case management system, all in one tool, security teams can benefit from all the necessary data to support better outcomes.

Not only does this cover all bases to give peace of mind, but it also offers transparency into total cost of ownership. A sound converged security setup will offer a predictable licensing model that is dependent on factors that are within the customer's control, so they know exactly what they are getting for their money. Looking ahead, it's this convergence that promises to be the real gamechanger in helping businesses navigate the cyber skills gap ●

Tim Wallen is Regional Director for the UK&I at LogPoint. With almost 20 years of cybersecurity experience, he has held senior sales and management positions within both high-growth and established vendors, including FireMon, ForeScout, Check Point, McAfee and IBM.

The Department for Digital, Culture, Media and Sport estimates that 51 percent of UK businesses have a basic skills gap



Picture credit: Logpoint

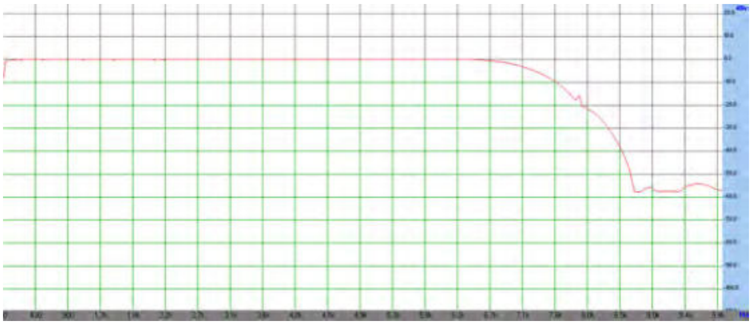
MGT SST-33

DATA SHEET

STEREOPHONIC DIGITAL RECORDABLE STETHOSCOPE - WITH PERSPEX DUST COVER

OVERVIEW

MGT-SST-33 is the best choice when you need to hear through the walls. It processes the audio signal using the greatest stereo digital audio technologies, which have been adapted to this market as a high-reliability DSP system.



To improve the characteristics of all audio paths, high-quality DAC and ADC sample the audio signal at a very high frequency (over-sampling approach).

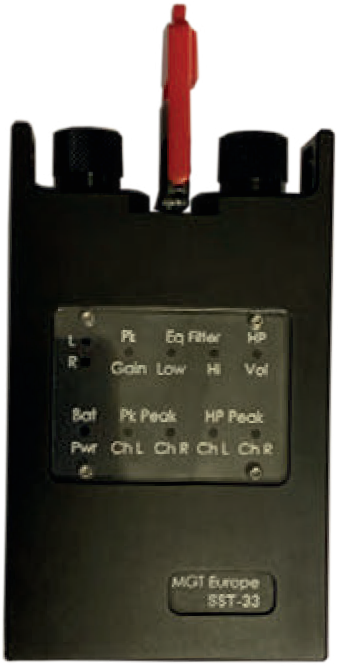
An incredible five-band equalisation technology gives you a crystal-clear audio experience.

All you need to set up the device is the two knobs and the frontal led.

The Host Full-Speed USB Port allows you to plug in a memory stick and record all audio in an uncompressed format.

The MGT-SST-33 has a perspex dust cover and high-quality connectors for the best connections.

TECHNICAL SPECIFICATIONS



Input	2 balanced channels
Bandwitdh	50Hz - 8KHz
Sample Frequency	16KHz
Microphone Gain	59.5db
Microphone AGC	Yes
Line Out Gain	0 ~ 40db
Headphone Gain	0 ~ 40db
Equalizer Bands	5
Gain Each Bands	+/-12 db
Audio Output	Stereo Headphones
Stereo Separation	-70db
DAC	16 bit DAC ADC input sensitivity 0.707 vrms
USB File System	FAT 16 or 32
Compression	None
Power Voltage	3.0V~5.0 V DC
Power Consumption	280mW (70mA at 4V)
Battery	3.7v 1100 ma Li-Ion battery
Size	75mm x 125mm x 20mm

Picture credit: Towfiqu Barbhuiya

A HOLISTIC APPROACH

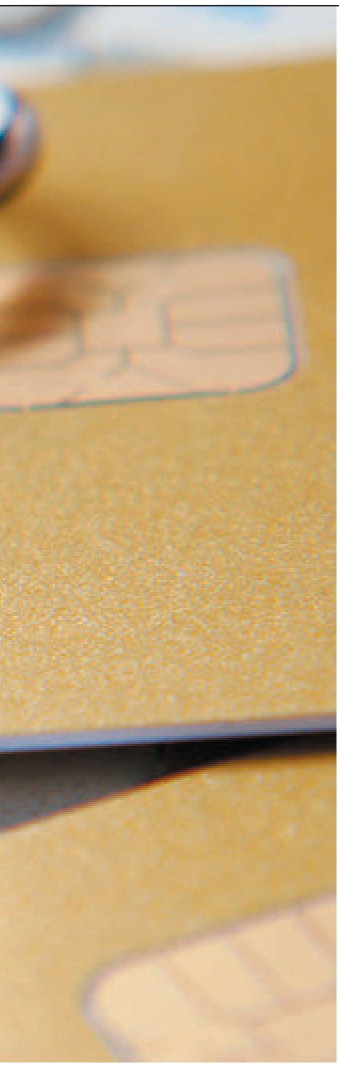
Dylan Border *explains why creating an organisation-wide culture of defence holds the key to strong security performance*

Results of a recent pwc survey reveal that 27 percent of global CFOs have experienced a data breach in the past three years, costing their organisation more than $1 million. Companies are under increased pressure to protect their business from threats that could cause extensive financial and reputational damage. Cybersecurity is no longer a 'nice-to-have' – it's business critical. As a result, more customers are interested in how their content and data are being secured. And while many are making progress, some are still playing catch up.

Organisations are facing threats that are constantly evolving and becoming increasingly sophisticated. Hackers are relentless in their search for any gap in a company's security armour. Unfortunately, security is only as strong as its weakest link, and it only takes one insider threat to jeopardise everything. No longer just a passive focus for an IT department, cybersecurity requires organisations to create a defensive and scalable model to managing their policies and technologies that is applied holistically across the whole organisation.

The trend towards remote work has been replaced by a hybrid model, in which many employees work from home part of the time. This has ushered in the rise of bring your own device (BYOD), which means employees need to be more savvy about security.

At the same time, workers are faced with managing an ever-growing variety and volume of content – from office documents to images and videos. With users



CSPs enable users to store, access and share their sensitive data and content, adding extra layers of security across the enterprise

often struggling to find internal tools that are up to the task and that fit their work styles, it's only natural that their own device might fill this void.

So, while remote working provides greater flexibility, its impact has some negative implications. Introducing hundreds, of employee-owned devices into a company's network drastically increases the risk of a cyber-attack and inadvertent insider threats.

Employees are often using their own devices out of convenience and habit, rather than with any malice in mind. They are simply seeking a work experience equal to the one they have in their day-to-day lives.

It's clear that education is key when it comes to ensuring workers are savvy about the risks. Gartner predicts that: "by 2025, lack of talent or human failure will be responsible for over half of significant cyber incidents." Even with the best of intentions, it is impossible for an organisation's IT team to defend against all variables, all of the time. Cybersecurity measures must extend beyond the realm of the IT department and reach every employee in the business – regardless of where they and their connected devices are working from. So, what does this actually look like?

An organisation must ensure that staff are up to speed with best practice security measures and threats. Many organisations we work with are constantly playbooking and running tabletop exercises to address security vectors, while some also offer bug bounty programmes to help cover as many angles as possible, using resources beyond their internal teams. However, the variables of breaches and exploits are endless.

The key to strong security performance is to develop an organisation-wide culture of defence in which all employees are invested and take a proactive role. From the marketing team to the finance department, employees must understand not only why cybersecurity tools and processes are essential, but also how to identify a potential threat and what action to take. This shift heralds a culture change that requires constant and consistent training and education, as well as support and investment at the most senior levels.

Cybersecurity is a careful balancing act. If implemented improperly, it can be incredibly disruptive to a business. Too many security controls can prevent employees from carrying out their role effectively. However, too little security can spell disaster.

Above all else, IT leadership must consider what security approach works best for their organisation. Zero Trust may be too limiting for some organisations, either through the resources required to truly implement it or the management of it once in place. First and foremost, senior leadership must both understand and agree on the organisation's overall approach to security. They must determine what the structure will look like, and how it will be managed. Then, adequate cybersecurity budgets must be allocated not only to developing and onboarding the right technology, but also towards running continuous training programmes across the organisation.

Over the last few years, organisations have invested in content services platforms (CSPs) to enable employees to collaborate effectively whether they are office-based or working from home. CSPs enable users to store, access and share their sensitive data and content, while also boosting productivity. They also add extra layers of security across the enterprise.

CSPs employ several tactics to keep data secure from the moment it enters your organisation, to the moment you decide that you no longer need access to it. For example, automated processes can be set up based on predetermined rules to mask, delete, encrypt or archive records and therefore protect them from unnecessary exposure. Businesses can enable workflow automation to significantly reduce the number of human contacts data points are exposed to, thus improving both accuracy as well as security. And redundant configurations can mitigate the potential impact of ransomware attacks.

Essentially, CSPs allow businesses to automate and secure internal data and documents, by giving the right people access to the right records, with historical monitoring to help audit this access, if it's ever needed.

In order for cybersecurity to stay top of mind, organisations must develop training programmes that employees engage with regularly. In doing so, staff will always have fresh, up-to-date knowledge on the importance of security, as well as a robust understanding of the types of new attacks out there. In 2023, we are seeing a focus on ransomware and supply chain attacks, as well as the ongoing prevalence of phishing attempts. Unfortunately, security is never a case of 'once and done' – attacks are constantly evolving, and team members' knowledge must develop at the same rate.

IT LEADERSHIP MUST CONSIDER WHAT SECURITY APPROACH WORKS BEST FOR THEIR ORGANISATION

Ideally, training should extend beyond the hypothetical, to include realistic attack examples. For example, in best-in-class organisations, non-technical teams are exposed to simulated attacks in order to find out how employees would deal with a real-life scenario, such as a phishing attempt. These 'drills' prepare a user for a genuine attack, and they also offer security professionals invaluable insights into weak points across the business. This information should be used to inform future training programmes, to ensure that they are as robust and up-to-date as possible.

As part of the training, trainers must make it clear how to properly report suspected attacks. The company's incident response plan should include expected timeframes for reporting a potential threat, as well as any details required to assess the risk level. Employees should be made aware of their legal obligations to report a threat, such as a suspected data breach, within a timely manner.

In order for employees to take security seriously, and feel accountable for maintaining appropriate standards, many businesses include employees' cybersecurity obligations within their job descriptions. This sends a clear signal that security is their responsibility, and they must take a proactive approach upholding the business's security agenda.

These requirements generally cover password protocol; adhering to multi-factor authentication policies and following any other digital hygiene measures that are described in the company's cybersecurity guidelines. It is also likely to include a requirement to follow cybersecurity training and education courses regularly.

For organisations enabling BYOD, employees should also be made aware of the organisation's BYOD policy as part of their onboarding. These policies will likely cover device maintenance; approved access to applications and functions; sharing of company documents; installation and regular updates of antivirus software; use of firewalls and what constitutes appropriate personal use of the device.

> THE KEY TO STRONG SECURITY IS TO DEVELOP AN ORGANISATION-WIDE CULTURE OF DEFENCE

Beyond continued training for non-technical staff, it is also crucial to ensure that your cybersecurity team always has access to timely information about the changing security landscape. As well as new types of attacks emerging, security teams must keep a pulse on the latest external validation points that may be required by customers, such as ISO standards and HITRUST compliance.

Cybersecurity is a rapidly evolving industry, with new trends and technologies constantly emerging. In 2023, hot topics are AI and the vast security opportunities it affords, continuing to secure remote workers and how to best secure this model into the future, as well as Zero Trust. Without deep knowledge of these concepts, it can be difficult for security teams to advise the business on where to invest, and what is even possible to achieve within their specific organisational framework.

Technical teams must keep their knowledge updated to be able to advocate for the most appropriate course of action for their business. Security professionals should be encouraged to attend conferences and undertake relevant courses and certifications.

In 2023, almost half (48 percent) of UK organisations say a "catastrophic cyber-attack" is the top risk scenario within their business. Every day, cyber threats are growing in severity and frequency. It is therefore unsurprising that cyber security budgets have increased in recent years, as senior leadership becomes more aware of the risks posed by failing to invest in security. Within my work, we are seeing an increasing number of companies placing security at the top of their agenda – and for good reason.

While a rise in interest in this area is a positive step, we must also acknowledge that creating a strong cybersecurity defence takes time. Some leaders are under the impression that simply hiring in new and experienced team members means they can take their eye off the ball. However, without proper continued support and contextual guidance, new security staff can be limited in their understanding of the organisation's software, system and processes. Even the most talented teams cannot secure what they do not understand.

For these reasons, an organisation-wide approach to cybersecurity is essential. Senior leadership must not only allocate budget to the programme, but they must also enable their IT teams to work collaboratively with the entire business. By implementing effective CSPs, they are able to ensure that content and data is protected throughout its life within the organisation's estate. Finally, they must empower staff to play their crucial role in securing the enterprise. For organisations yet to embrace this holistic way of working, there has never been a better time to start ●

Dylan Border is Hyland's Director of Cyber Security. He is responsible for leading the Cyber Security Operations and Governance, Risk & Compliance teams, which facilitate the secure operations of Hyland's enterprise networks, systems, and business processes.

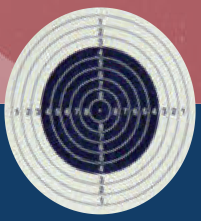
The increase in working from locations outside of the office has intensified the need for employees to remain savvy about security

Picture credit: Glenn Carstens Peters

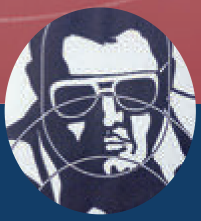
MCQUEEN TARGETS

LIVE FIREARMS TRAINING TARGETRY

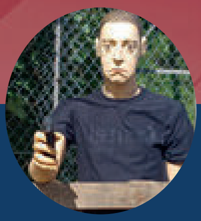
AIM FOR THE BEST.


CIVILAIN TARGETS

MILITARY TARGETS


POLICE TARGETS

THREAT ASSESSMENT


3-D FOAM TARGETS

3-D FOAM ACCESSORIES

Hit the mark every time with

MCQUEEN TARGETS

GALASHIELS, SCOTLAND

targets.ukgal@sykes.com

+44 (0)1896 664269

mcqueentargets.com

INCIDENT BRIEF

Europe

2 May, London – UK

A man was arrested outside Buckingham Palace after allegedly throwing items – suspected to be shotgun cartridges – into the palace grounds.

3 May, Belgrade – Serbia

A 13-year-old boy opened fire in a classroom in an apparently planned attack that killed eight children and a school security guard and injured a further six pupils as well as his teacher.

4 May, Belgrade – Serbia

Eight people were killed and 14 wounded in a second mass shooting in the Balkans in as many days as a 21-year-old with an automatic weapon carried out a drive-by assault.

9 May, Ghent, Roeselare, Menen, Ostend and Wevelgem – Belgium

Belgian police arrested seven people suspected of supporting Islamic State and plotting a terrorist attack. Almost all of the suspects were ethnic Chechens and three possessed Belgian nationality, prosecutors said in a statement.

11 May, Saint-Brevin-les-Pins – France

The mayor of the Western seaside town resigned following death threats and an arson attack on his home as far-right groups protested over an asylum-seeker centre in the town.

16 May, Orio – Spain

A man and a woman were killed by an explosion near a children's playground in the North of the country. Authorities suspect the blast was linked to "gender-based violence".

Americas

6 May, Allen – USA

A gunman killed eight people and wounded seven others at a shopping mall outside Dallas, Texas. He was shot dead by police.

8 May, Brownsville – USA

Eight people were killed and 10 others injured after a car ploughed into a crowd outside a shelter serving migrants and homeless people in the Texas town. Investigators believe the attack was intentional.

9 May, Bloomfield Township – USA

A man in Michigan was the target of hackers who stole six figures worth of Bitcoin cryptocurrency by hacking his cellphone through a SIM card swap.

13 May, Riverside – USA

Police in California, are searching for a man who attacked a homeless person with a sword and cut off his hand.

14 May, Philadelphia – USA

The *Philadelphia Inquirer* was targeted in a cyber-attack, forcing it to cancel its Sunday issue and delay online stories. The attack triggered the worst disruption to the newspaper in decades.

15 May, Farmington – USA

At least three people were killed and multiple people injured after a shooting in New Mexico. Police killed the suspected 18-year-old gunman.

15 May, Virginia – USA

A man with a metal baseball bat walked into the district office of a Democratic congressman and struck two of his workers – including an intern in her first day – with the bat.

Asia

2 May, Damghan – Iran
An explosion struck a base belonging to the country's paramilitary Revolutionary Guard, killing two workers in the Northern Semnan province.

7 May, Melbourne – Australia
The homicide squad is investigating the death of a man who was found with critical injuries inside a car with a large bullet hole through the windscreen in the North-West of the city.

9 May, Gaza – Israel
Israeli airstrikes targeting the militant group Palestinian Islamic Jihad killed three senior operatives and at least nine civilians, including three children.

9 May, Islamabad – Pakistan
Internet services were suspended across the country after violence erupted as former prime minister, Imran Khan, was arrested and dragged into an armoured vehicle by scores of security forces in riot gear.

9 May, Perth – Australia
Authorities regained control of the Banksia Hill Detention Centre after dozens of rioting juveniles burned buildings, threatened staff and tried to escape the troubled facility.

10 May, Karachi – Pakistan
A suicide bomb attack on Chinese shipyard workers in Port Qasim was foiled by police following an intelligence tip-off.

16 May, Wellington – New Zealand
A fire at the Loafers Lodge hostel in Newtown, in the capital's South,left at least six people dead and 11 others missing. Police suspect arson and have opened a homicide investigation.

16 May, Bandarban – Bangladesh
Two soldiers of the Bangladesh Army were killed and two officers injured as members of Kuki-Chin National Army detonated an improvised explosive device and opened fire on army personnel.

16 May, Pushp Vihar – India
A school in South Delhi received a bomb threat via email in the early hours of the day. A team of Delhi Police searched the premises, but were unable to find anything.

Africa

1 May, Toffo – Benin
Ten soldiers were injured in an explosion in an ammunition bay at an officer training school in the South of the country.

6 May – Djibouti
Journalist Gobeze Sisay is facing a terrorism investigation in Ethiopia after arrest in the neighbouring country. He is accused of terrorism and leading the media propaganda wing of an unnamed extremist group.

8 May, Kaduna State – Nigeria
Terrorists stormed the Emir's palace and abducted nine children and the Emir of Kagarko's youngest wife (who later escaped). The gunmen also killed a herdsman in Kuchimi village and looted seven shops in Janjala village.

9 May, Djerba – Tunisia
A police officer shot a colleague and seized his ammunition before heading towards the Ghriba synagogue where he killed three other police and two visitors.

11 May, Mouhoun province – Burkina Faso
At least 33 people were killed when gunmen opened fire on vegetable farmers in the jihadist-hit village of Youlou in the department of Cheriba.

14 May, Lake Chad – UK
Troops of the Multinational Joint Task Force (MNJTF) operating in the region killed "a number" of suspected Boko Haram militants and recovered "heavy weapons".

14 May, Maiduguri – Nigeria
Three soldiers from Nigeria and Niger were killed and at least 12 others were injured when their vehicle set off an improvised explosive device while pursuing insurgents.

16 May, Anambra state – Nigeria
Gunmen attacked a US diplomatic convoy in the South-East of the country, killing four people and abducting three others.

19 May, Djibo – Burkina Faso
Doctor Ken Elliott, the Australian who was kidnapped by an al-Qaida-linked group in Africa in 2016, was released.

NEWS

Europe

Educational institutions are top of hackers' shopping lists

Over three-quarters (78 percent) of UK schools have experienced at least one type of cyber-incident, according to a recent National Cyber Security Centre (NCSC) and National Grid for Learning (LGfL) audit. Cyberattacks on educational institutions have been on the rise for some time. In early January 2023, it was reported that confidential data from 14 UK schools was leaked online by the threat actor Vice Society after they refused to pay the group's ransom demands. In early May, the UK's largest state boarding school Wymondham College announced it had been hit by a cyber-attack and while it is yet to confirm if any sensitive data has been accessed, it did confess to anticipate ongoing disruption over the coming weeks. Simon Bain, founder and CEO at OmniIndex, has called on educational institutions to take steps to improve their defences against cyber criminals looking for an easy target: "One of the biggest challenges in educational data use today is preventing data misuse. Educational institutions are frequently targeted by cyber criminals as they regularly collect and store huge amounts of highly sensitive, confidential and regulated information. With this comes huge risks and privacy concerns. While collection of data is a crucial part of the education system and can be utilised to support improved educational outcomes by identifying areas where students and schools may need additional support and facilities, when mismanaged, educational institutions can face large fines and reputational damage that can have long-term effects on their success."

Ministers consider body-worn facial recognition for UK police

Ministers are calling for facial recognition technology to be "embedded" in everyday policing, including potentially linking it to the body-worn cameras UK officers use as they patrol streets. Until now, use of live facial recognition in England and Wales has been limited to special operations such as football matches or the coronation. The government's intentions were revealed in a document produced for the surveillance camera commissioner, discussing changes to the oversight of technology and surveillance. It said: "This issue is made more pressing given the policing minister [Chris Philp] expressed his desire to embed facial recognition technology in policing and is considering what more the government can do to support the police on this. Such embedding is extremely likely to include exploring integration of this technology with police body-worn video." Body-worn cameras can currently capture video in high definition and it is technically possible to link them to live facial recognition (LFR), a system that matches the biometrics of people's faces against those held on a watchlist.

UK ringleaders jailed over scam providing fake passports

The ringleaders of a gang that specialised in supplying fake passports to high-level criminals allowing them to evade arrest and identification have been jailed. Anthony Beard, 61, paid individuals for expired passports and applied for renewals using photographs of criminals who paid up to £20,000 to start new lives in Dubai, Portugal and Spain. In mid-May he was sentenced to six years and eight months at Reading crown court and jailed after admitting conspiracy to pervert the course of justice and conspiracy to make a false instrument with intent. "This was the golden ticket for the organised crime networks in order that they could evade arrest, evade identification by local law enforcement either internationally or at home in the UK," said Craig Turner, deputy director of investigations at the National Crime Agency (NCA).

AARONIA AG opens new drone detection location in Austria

The world leader in drone detection systems, AARONIA AG has opened its subsidiary in Austria at Vienna – Vöslau Airport. Stephan Kraschansky, former officer and expert in drone defence in the Austrian Armed Forces, will lead the company as Managing Director. With the foundation of a subsidiary in Austria and the opening of the new location, AARONIA AG is reacting to the constantly growing demand for its products. In both the military and civil sectors, the need for reliable systems to detect and defend against drones is constantly increasing. "The site offers ideal training and demonstration conditions thanks to numerous civil transmitters and flight movements," explained Kraschansky.

EU told it needs to tighten spyware safeguards

The EU needs tighter regulation of the spyware industry, a European parliament special committee has said, after concluding that Hungary and Poland used surveillance software to illegally monitor journalists, politicians and activists. A special European parliament committee voted in early May for a temporary ban on the sale, acquisition and use of spyware while the bloc draws up common EU standards based on international law. The moratorium would be lifted only on strict conditions, including independent investigations into the abuse of spyware in the EU. The report found that Hungary and Poland's nationalist governments had: "weakened and eliminated" safeguards on spyware, "effectively leaving victims without any meaningful remedy". MEPs also raised questions about the use of the spyware in Spain and Greece, while voicing concern that many European Union member states had created a: "safe haven for the spyware industry, often in violation of union laws and standards".

NEWS

Americas

Biden: white supremacy is biggest terrorist threat

President Biden has declared white supremacy as: "the most dangerous terrorist threat" to the American homeland, using a speech to graduating students at a historically Black university to elevate a debate that has already become central to his campaign for a second term. Recounting the story of how he initially decided to run for the White House after seeing white supremacists marching in Charlottesville in 2017, the president said the country continues to be in a "battle" against "sinister forces" that are determined to turn the clock back to more divisive times. "I don't have to tell you that progress towards justice often meets ferocious pushback from the oldest and most sinister of forces," Biden said, after quoting former president Donald Trump's equivocating response to the 2017 rally. "That's because hate never goes away." His address came as many leading Republicans, including those currently vying for the GOP presidential nomination, argue that the nation's focus on racial injustice has gone too far. Florida Gov. Ron DeSantis and others have attacked critical race theory, which examines how race is embedded in society and criticised the push for diversity, equity and inclusion embraced by many institutions. They argue that such initiatives portray America as evil and tar all white people as racist.

Post-9/11 wars have contributed to 4.5-million deaths

Brown University researchers have draw on UN data and expert analyses to attempt to calculate the minimum number of excess deaths attributable to the war on terrorism – across conflicts in Afghanistan, Pakistan, Iraq, Syria, Libya, Somalia and Yemen – post 9/11. The accounting, so far as it can be measured, has puts the toll at between 4.5 and 4.6-million. Of those fatalities, the report estimates, some 3.6 to 3.7-million were: "'indirect deaths" caused by the deterioration of economic, environmental, psychological and health conditions. More than 7,000 US troops were killed in Iraq and Afghanistan, along with more than 8,000 contractors, according to Brown's Costs of War project. And US forces have suffered cascading effects of their own, including rates of suicide among veterans outpacing the general population. But the vast majority of those killed in the fighting were locals: more than 177,000 uniformed Afghans, Pakistanis and Iraqis and Syrian allies died as of 2019 alongside a vast count of opposing combatants and a disputed civilian toll. "There are reverberating costs, the human cost of war, that people for the most part in the United States don't really know enough about or think about," said Stephanie Savell, the paper's author and co-director of the Costs of War project. "We talk about it being over now that the US has left Afghanistan, but one significant way that these wars are continuing," she said, is that: "the people in the war zones are continuing to suffer the consequences".

SEC issues largest-ever whistleblower award

The US Securities and Exchange Commission has announced the largest-ever award, nearly $279-million, was given to a whistleblower whose information and assistance led to the successful enforcement of SEC and related actions. This is the highest award in the SEC's whistleblower programme's history, more than doubling the $114-million award the SEC issued in October 2020. "The size of today's award not only incentivises whistleblowers to come forward with accurate information about potential securities law violations, but also reflects the tremendous success of our programme," said Gurbir S Grewal, Director of the SEC's Division of Enforcement. "This success directly benefits investors, as whistleblower tips have contributed to enforcement actions resulting in orders requiring bad actors to disgorge more than $4-billion in ill-gotten gains and interest. As this award shows, there is a significant incentive for whistleblowers to come forward with accurate information about potential securities law violations."

CI cybersecurity spend to reach $236-billion by 2027

Following the impact of COVID-19 on cybersecurity spending budgets behind industrial sectors, worldwide investments in Critical Infrastructure (CI) cybersecurity will display robust growth rates in all sectors, according to global technology intelligence firm ABI Research. The global cybersecurity market was estimated at $213-billion in 2022 and is projected to be more than $380-billion by 2027. CI cybersecurity spending will stand at around $236-billion by 2027, displaying a healthy Compound Annual Growth Rate of 14 percent. The pandemic hindered cybersecurity spending in some sectors while boosting spending in others. "For example, cyber spending in the transport sector was significantly affected during the first few fiscal quarters of the pandemic, when many sectors grounded to a halt (most notably the aviation industry). On the contrary, the healthcare sector saw an uptick in cybersecurity spending at the start of the COVID-19 pandemic as healthcare operations ramped up significantly. Spending in healthcare is expected to slow post-2023 as the effects of the pandemic start to level out. At the same time, transportation cybersecurity spending will return to normal," explains Michael Amiri, Senior Industrial Cybersecurity Analyst at ABI Research. The defence sector has the highest spending among all eight sectors in ABI Research's report and is predicted to reach more than $52-billion in 2027.

NEWS

Asia

Syria's main insurgent group distances itself from al-Qaida

The leader of the Hayat Tahrir al Sham (HTS), which rules much of North-West Syria and rose to notoriety carrying out deadly bombings and dispatching Islamist religious police to crack down on women deemed to be immodestly dressed, is attempting to distance his group from its al-Qaida origins, spreading a message of pluralism and religious tolerance. As part of the rebranding, Abu Mohammed al-Golani has cracked down on extremist factions and dissolved the notorious religious police. Al-Golani told a gathering of religious and local officials that Islamic law should not be imposed by force. "We don't want the society to become hypocritical so that they pray when they see us and don't once we leave," he said, pointing to Saudi Arabia, which has relaxed its social controls in recent years after decades of strict Islamic rule. The pivot comes at a time when HTS is increasingly isolated. Countries that had once backed insurgents in Syria's uprising-turned-civil-war are restoring relations with Syrian President Bashar Assad. The United States still considers HTS a terrorist group and has offered a $10-million reward for information on al-Golani's whereabouts. The United Nations also designates it a terrorist organisation.

North Korea unveils first military spy satellite

Kim Jong-un has inspected North Korea's first military spy satellite and given the go-ahead for its "future action plan", according to state media. Jong-un met the "non-permanent satellite launch preparatory committee" in mid-May before viewing the satellite, the Korean Central News Agency (KCNA) said. In April, Kim said construction of the satellite was completed and gave the green light for its launch. That report came about a week after Pyongyang launched what it said was a new solid-fuel intercontinental ballistic missile, marking a major breakthrough in its banned weapons programmes. ICBMs and space launch capabilities use shared technologies. The satellite appeared to be a polygonal cylinder, covered in gold insulating foil and fitted with solar panels. The photographs were partly blurred for obvious reasons. Jong-un has accused the US and South Korea of escalating what he calls: "confrontational moves" against the North and said his country will exercise its right to self-defence.

Crypto thefts target Japan, Vietnam and Hong Kong

North Korea is using cyberattacks to target Japanese cryptocurrency assets. Hacker groups affiliated with North Korea have stolen $721-million from Japan since 2017, according to a study by UK-based compliance specialist Elliptic. The amount is understood to be equal to 30 percent of the total of such losses worldwide. Pyongyang is believed to have targeted the crypto assets of other countries to obtain the foreign currency that it uses for its missile programme. This could, in turn, threaten the security of Asia. In a joint statement adopted by the Group of Seven finance ministers and central bank governors in mid-May in Japan, top officials acknowledged the "growing threat from illicit activities by state actors" such as the theft of cryptocurrencies, with North Korea's repeated missile launches in mind. According to a report released in April by a UN Security Council panel of experts, North Korea stole between $600-million and $1-billion in cryptocurrency in 2022, double the previous year's total. Elliptic estimates the figure at $640-million for 2022.

New APT targets South and South-East Asia

APT group Lancefly is using a custom-written backdoor in attacks targeting government, aviation, education and telecom organisations in South and South-East Asia in an activity that has been ongoing for the past five years, according to Symantec. The group has been seen carrying out the activity with the motive of intelligence gathering. Lancefly has been deploying the Merdoor backdoor in highly targeted attacks since 2018 to establish persistence, execute commands and perform keylogging on corporate networks. "Lancefly's custom malware, which we have dubbed Merdoor, is a powerful backdoor that appears to have existed since 2018," Symantec said in the blog, adding that researchers observed it being used in activity in 2020, 2021 and this more recent campaign, which continued into the first quarter of 2023. The backdoor is highly targeted and used selectively. "This recent Lancefly activity is of note due to its use of the Merdoor backdoor, but also the low prevalence of this backdoor and the seemingly highly targeted nature of these attacks," the blog said.

China jails US citizen for life on espionage charges

A Chinese court sentenced a 78-year-old US citizen to life in prison on espionage charges. John Shing Wan Leung, a Hong Kong permanent resident, was detained in April 2021 by Chinese security services. His sentence was announced in mid-May by the Suzhou intermediate people's court on its public WeChat account. No further information about his trial or charges were listed. Leung's sentence also included deprivation of political rights for life and confiscation of personal property in the amount of 500,000 yuan. There are no previous reports or notices of Leung's arrest or trial. Espionage cases in China are treated with almost no transparency, with trials often conducted in secret and long delays between convictions and sentencing. This month, amendments to China's anti-espionage law came into force, broadening its scope and increasing the risk to foreign individuals and organisations operating in the country.

3DX-RAY

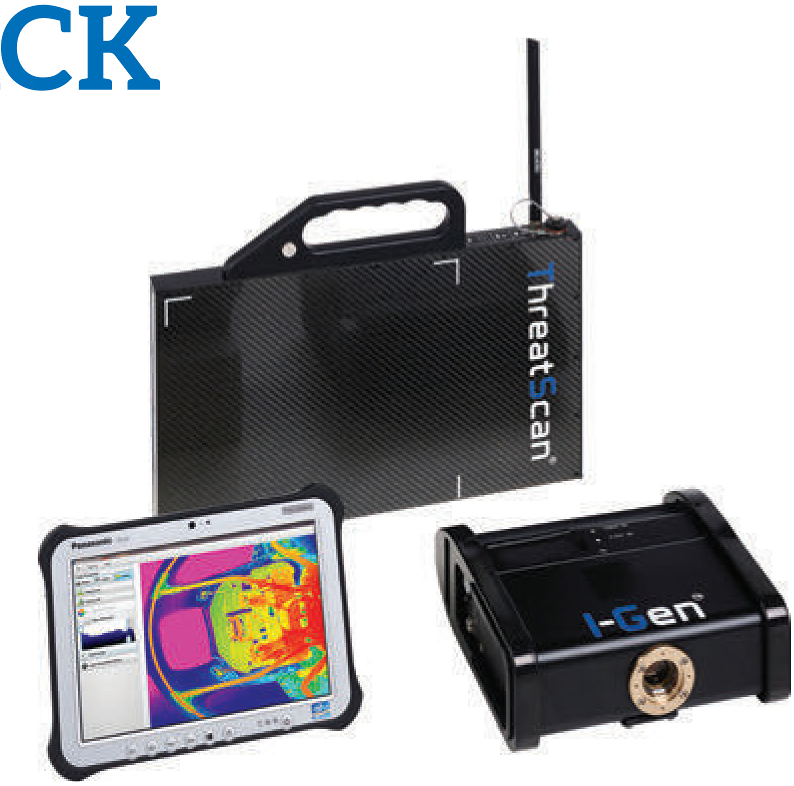
INSIGHT WHERE IT MATTERS

SECURITY IN A BACKPACK

Rapid deployment.
High quality images.
Fast decisions.

Introducing the new, robust and powerful **ThreatScan®-LS3**. Designed in collaboration with first responders, this is a small, lightweight and compact unit that's designed to be rapidly deployed.

High quality, real-time X-ray images (305 x 256mm), materials discrimination, pan, zoom, DeepFocus™, 3D Emboss, measurement and annotation all enable rapid and accurate decision-making.



Optional tablet PC shown.

The complete system fits in a backpack.

www.3dx-ray.com

An **IMAGE SCAN** company

NEWS

Africa

US urges Mali to investigate horrific Moura attack

In mid-May the United States urged Mali's transitional government to pursue an: "independent, impartial, efficient, exhaustive and transparent investigation" to hold accountable those responsible for the execution of hundreds of people in the South-Central village of Moura. "The United States is appalled by the disregard for human life exhibited by elements of the Malian Armed Forces in cooperation with the Kremlin-backed Wagner Group," US State Department spokesperson Matthew Miller said after Malian soldiers and unidentified "armed white men" executed at least 500 people and sexually assaulted or tortured dozens of others during a five-day operation last year. Though the identity of the white men was not clear, Western countries have raised concerns over the Russian private military contractor Wagner Group's activities in the region since late 2021. Mali, whose leaders seized power in a 2021 coup, and Russia have previously maintained that Russian forces there are not mercenaries but trainers helping local troops with equipment bought from Russia.

Cyber attacks in South Africa, Kenya and Nigeria increase

Anti-virus company Kaspersky has revealed that for the first quarter of 2023 the share of users attacked with spyware in South Africa, Kenya and Nigeria increased steadily. The company recorded an increase of 18.8 percent in South Africa, 12.9 percent in Kenya and 14.6 percent in Nigeria from Q4 2022 to Q1 2023. Spyware continues to be a threat to users of different types of devices, including thin clients. Thin clients are used in corporate networks around the world to set up workspaces at a much lower cost than when using traditional laptop or desktop computers. A thin client on a traditional operating system (OS), Linux or Windows-based, could potentially be targeted by different types of attacks, including spyware. A compromised thin client could serve as an entry point to the corporate network and could be used to gain access to confidential data, take control over other machines on the network, or run malicious software, etc. According to the company, there are over 60 vulnerabilities in thin clients that could be used by cybercriminals.

Sahel needs help to fight violent extremism and stop its spread

A senior UN official has warned that without greater international support and regional cooperation the instability in Africa's Sahel region will expand toward West African coastal countries. "Resolute advances in the fight against terrorism, violent extremism and organised crime in the Sahel desperately need to be made," UN Assistant Secretary-General for Africa Martha Pobee told a UN Security Council meeting in mid-May. The counterterrorism force, now comprised of Burkina Faso, Chad, Mauritania and Niger, lost Mali a year ago when its ruling junta decided to pull out. Pobee said the force hasn't conducted any major military operations since January adding that the force is adjusting to new realities: France moving its counterterrorism force from Mali to Niger due to tensions with the junta and Mali's decision to allow Russian mercenaries from Wagner to deploy on its territory. Pobee criticised the international community, saying a lack of consensus among donors and partners has left the joint force without sufficient funding and other needed support to become fully operational and autonomous so it can have the capacity it needs to help stabilise the Sahel region.

Germany to pull troops out of Mali by May 2024

The German government has decided to end its participation in the UN mission in Mali by next May over problems with the ruling junta. Chancellor Olaf Scholz's cabinet said Berlin would pull its 1,110 troops in the UN mission MINUSMA out of the West African country over the next year and pivot towards more humanitarian and development aid for the region. "We are reorganising our engagement in the region and will let our participation in MINUSMA run out in a structured fashion over the next 12 months," Foreign Minister Annalena Baerbock said in a statement. Defence Minister Boris Pistorius said Berlin's goal was to: "foster the growing responsibility of Africans for security and stability on their own continent".

Kenya urged to step up cybersecurity

The growth of cyber risk insurance, once touted as the next big thing in the Kenyan insurance industry, is being hampered mainly by insurers' processes and premium-related concerns. Lack of personnel to analyse risks, financial capacity and underwriting challenges are some of the issues that have forced local insurers to pass off the underwriting capacity to foreign firms more familiar with the concept. The Association of Kenya Insurers (AKI) has admitted in the past that local insurance industry players lack the capacity to price and offer indemnity covers for cyber insurance. As cyber threats continue growing in the country, insurers will have to partner with cyber specialists to develop products that focus more on providing security solutions to minimise risks of exposure. The Kenya Computer Incident Response Team, a multi-agency collaboration framework responsible for the national coordination of cyber security, identifies ransomware, malware, and phishing attacks as the most common cybersecurity risks in the country with financial institutions the biggest targets. Check Point Research placed Kenya among high-risk countries in its cyber threat risk analysis for 2022.

DIARY DATES

2023 Conference and Exhibition planner

26-27 July India Homeland Security Expo 2023

New Delhi, India
Organiser: Nexgen Exhibition
Tel: +91-11-4153699info@
homelandsecurityexpo.in
www.homelandsecurityexpo.in

11-13 September GSX 2023

Dallas, Texas
Organiser: ASIS International Tel: +1
703.519.6200
Email: asis@asisonline.org
www.gsx.org

12-15 September DSEI 2023

Excel, London
Organiser: Clarion Defence. Tel: + 44 (0)330
912 1213
Email: enquiries@dsei.co.uk
www.dsei.co.uk

19-20 September International Security Expo 2023

Olympia, London
Organiser: Nineteen.Group Tel: +44 (0)20
8947 9177
Email: info@internationalsecurityexpo.com
www.internationalsecurityexpo.com

26-27 September DSEI 2023

Excel, London
Organiser: Clarion Defence. Tel: + 44 (0)330
912 1213
Email: enquiries@dsei.co.uk
www.dsei.co.uk

14-17 November Milipol Paris 2023

Paris, France
Organiser: Comexposium
Email: visit@milipol.com
https://en.milipol.com/

15-17 November Sicurezza 2023

Milan, Italy
Organiser: Fiera Milano S.p.A. Tel: +39 02
4997.7238
https://www.sicurezza.it

16-18 January Intersec 2024

Dubai, UAE
Organiser: Messe Frankfurt Exhibition
Tel: +971 4 3894 500
Email: intersec@uae.messefrankfurt.com
www.intersecexpo.com

19-21 November MAST Australia 2024

Adelaide, Australia
Organiser: MAST. Tel: +44 7411 732978
Email:admin@mastconfex.org.
mastconfex.com

YOUR MOBILITY SPECIALIST FOR ARMOURED VEHICLES

- Flat tyres? **Keep on driving**
- Punctured fuel tank? **No leakage**
- Enclosed in armour? **Barrier free communication**
- Heavy armouring? **Extra braking power**
- Blast threat? **Shock mitigation**

TSS International official distributor for:

RODGARD HUTCHINSON®

TSS HEAVY DUTY WHEELS SEMA WORLD ANTI-TERRORISM SAFETY FEATURES Téléflow

MOV'IT ProtecTank TSS

B&G electronics SKYDEX

TSS®

TSS INTERNATIONAL BV ZUIDEINDE 30-34, 2991LK BARENDRECHT. THE NETHERLANDS.
PHONE: +31 (0)180-618 922 FAX: +31 (0)180-611 326 EMAIL: SALES@TSSH.COM **WWW.TSSH.COM**

NEW TECHNOLOGY SHOWCASE

Rheinmetall and Elbit self-propelled howitzer

Rheinmetall and Elbit Systems have successfully conducted a live fire demonstration of an automated 155mm L52 wheeled self-propelled howitzer. The demonstration of the new system took place at the Shivta firing range in Southern Israel and was attended by high-ranking officials of the armed forces of the United Kingdom, Germany, the Netherlands and Hungary. The two companies signed a cooperation agreement last year to develop, manufacture and market an automated European 155mm wheeled self-propelled howitzer system. The cooperation between Rheinmetall and Elbit builds on the fully automated wheeled self-propelled howitzer procurement programmes that Elbit has signed with Israel and additional customers. As a result, a technically mature system is already available, enabling the integration of a Rheinmetall gun into the unmanned, fully robotic artillery turret of the Elbit system. The integration is currently in an advanced phase of the verification process. This will help reduce development risks and enable faster realisation of operational readiness.

ADT two-way audio camera with theft deterrent system

Security expert ADT has released a brand new outdoor wi-fi camera, which provides two-way audio and crystal-clear imagery. Michele Bennett, General Manager at ADT UK&I Subscriber explains: "Our brand new security camera not only allows for surveillance of your home and surrounding areas, it also allows homeowners to warn off potential intruders". The camera is also fully integrated with the ADT Smart Services app, which means customers are informed 24/7 – ensuring they feel safe and secure at all times. The new ADT Outdoor Wifi Camera is available as part of ADT's Smart Home security system and has a range of features which include: HD video footage in full colour, as well as night vision capacity; two-way audio; recorded clips which include audio; two additional memory cards allow for 24/7 footage in high-definition; live and recorded footage is available in the ADT Smart Services app and online portal; smart video analytics that can distinguish between people, vehicles and animals; and perimeter guard, which works by emitting a loud whistle and flashing red light to let unwanted visitors know they have been recorded.

IAI and Atlas Elektronik BlueWhale unmanned submarine

Israel Aerospace Industries (IAI) and Atlas Elektronik (AE) launched their latest joint development for advanced anti-submarine warfare missions at Undersea Defence Technology in Rostock, Germany, in a ceremony at ELTA's exhibition booth. Based on ELTA's sophisticated BlueWhale autonomous underwater multi-mission platform (a large unmanned underwater vehicle with a wide range of advanced sensor systems), the system incorporates AE's unique, towed passive sonar triplet array. Unlike existing towed sonars, the combined system can function at depths traditionally exploited by submarines to avoid detection. An AE transmitter, deployed from an autonomous (or manned) surface vessel, enables BlueWhale to perform bi-static location and tracking of submarine targets. BlueWhale has been successfully tested for thousands of diving hours, performing a wide range of missions, including ISR, EW/ESM and MCM. During the BlueWhale presentation, Michael Ozegowski, Chief Executive Officer of AE, explained: "The joint development of the BlueWhale ASW demonstrates once again the long-standing and trusting cooperation between German and Israel naval industry partners. In close collaboration with ELTA, we developed a state-of-the-art system solution enabling high impact ASW operations with minimum infrastructure requirements."

Teledyne FLIR Boson+ thermal camera

Teledyne FLIR has announced the first Boson+ thermal camera module with its factory-integrated, high-performance 14mm to 75mm continuous zoom (CZ) lens. With seamless optomechanical integration, the new Boson+ CZ 14-75 reduces development and operational risk and costs, all with an industry-first warranty that is not available when using multiple suppliers. The reliable Boson+ CZ 14-75 is ideal for unmanned aerial vehicles, perimeter surveillance, light armoured vehicle situational awareness and targeting, and soldier sighting systems. "The Boson+ CZ 14-75 camera and lens are factory-designed and integrated to optimise performance and reliability," said Dan Walker, vice president, product management, OEM cores, Teledyne FLIR. "Thanks to flexible and advanced lens control electronics, industry-leading 20mK thermal sensitivity, and US-based integration support, the Boson+ CZ 14-75 streamlines development for applications requiring high-performance infrared zoom capability."

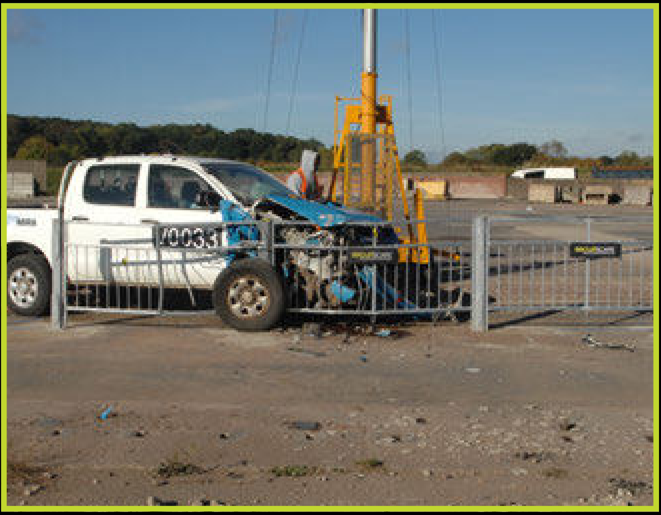
Saab supplies Seaeye Leopard to Spanish Navy

A multi-million-pound complete Saab Seaeye Leopard system has been supplied to the Spanish Navy for submarine escape and rescue, and underwater intervention. The NATO Support and Procurement Agency (NSPA) acquired the Seaeye Leopard electric remotely operated robotic vehicle system for the Spanish Navy to fulfil the responsibilities of the International Submarine Escape and Rescue Liaison Office and provide diving support. It is the first codification by NATO for a remotely operated vehicle meeting its standards. The Leopard also met the Spanish Navy's full ISO/IEE 15288 standards for remotely operated vehicles, along with standards for the control cabin. The Leopard can locate and survey a distressed submarine using its array of sonar systems and cameras to provide both colour zoom and low-light black and white video images for rescue planners. In urgent rescue situations the Leopard can work 24 hours a day, for days on end in challenging conditions. According to the information provided by the Spanish Navy through NSPA, the Leopard will also contribute enormously to the Spanish Navy underwater intervention capability, especially in the areas of underwater search and reconnaissance and diving support activities.

GUARD RAIL

Described as a game-changer for the security industry, our IWA-14-rated HVM pedestrian guardrails offer full roadside protection and can withstand a deliberate or accidental impact, unlike regular pedestrian guardrails, which are not designed to protect and so crumple when hit. Perfect for preventing death and injuries outside schools, local government buildings and other locations

- Crash-tested and capable of withstanding the impact with a 2.5 tonne vehicle travelling at 40mph - without significant bending or buckling
- Available as the standard HVM Guardrail, HVM Socketed Guardrail and even our HVM Guardrail Ultra systems
- Uses Securiscape's Smartpost technology in conjunction with fence panels for a flexible security solution
- Manufactured in the heart of the UK from high quality materials and can even be used on road bridges



All Securiscape Products have been tested to **PAS68** or **Iwa** and have **full certification**