DIGITALISATION WORLD

Modern enterprise IT - from the edge to the core to the cloud

AUTUMN 2020

digitalisationworld.com

SPECIAL FOCUS: CYBERSECURITY

enel x

Energy management solutions that deliver commercial and environmental rewards

Global resources, local market knowledge and specialist technological expertise make Enel X the trusted energy management partner for data centres and large scale enterprises all over the world.

Join us as we pave the way for a cleaner, more dynamic future.

enelxuk@enel.com | www.enelx.co.uk

Editor's View

By Phil Alsop

Cybersecurity and the next normal

Cybersecurity in the widest sense has been a major focus in recent times, as many individuals work from home for the first time, governments in the UK, Europe and the US wrestle with various data protection laws, and, more generally, digital transformation throws up all manner of new security threats, opportunities and solutions. So, it seems like now is a good time to see what's going on in the world of cybersecurity, with a particular look to the future.

We've managed to compile a comprehensive supplement, which offers some in-depth content on the security issues surrounding the remote, mobile workforce and zero trust – perhaps the two main hot topics of today – along with a whole range of views and opinions on any and every aspect of cybersecurity as it impacts on end users.

Contents

DIGITALISATION WORLD

Editor
Philip Alsop +44 (0)7786 084559 philip.alsop@angelbc.com

Sales Manager
Peter Davies +44 (0)2476 718970 peter.davies@angelbc.com

Sales Manager
Jessica Harrison +44 (0)2476 718970 jessica.harrison@angelbc.com

Director of Logistics
Sharon Cowley +44 (0)1923 690200 sharon.cowley@angelbc.com

Design & Production Manager
Mitch Gaynor +44 (0)1923 690214 mitch.gaynor@angelbc.com

Publisher
Jackie Cannon +44 (0)1923 690215 jackie.cannon@angelbc.com

Circulation & Subscriptions
+44 (0)1923 690214 circ@angelbc.com

Directors
Stephen Whitehurst – CEO
Scott Adams – Joint - Managing Director
Sukhi Bhadal – Joint - Managing Director

Published by:
Angel Business Communications Ltd, 6 Bow Court, Burnsall Road, Coventry CV5 6SP
T: +44 (0)2476 718970 E: info@angelbc.com

Angel BUSINESS COMMUNICATIONS

recycle When you have finished with this magazine please recycle it.

Digitalisation World is published 12 times a year on a controlled circulation basis in Europe, Middle East and Africa only. Subscription rates on request. All information herein is believed to be correct at time of going to press. The publisher does not accept responsibility for any errors and omissions. The views expressed in this publication are not necessarily those of the publisher. Every effort has been made to obtain copyright permission for the material contained in this publication. Angel Business Communications Ltd will be happy to acknowledge any copyright oversights in a subsequent issue of the publication.

The paper used within this magazine is produced by chain of custody certified manufacturers, guaranteeing sustainable sourcing. ISSN 2396-9016 (Online)

Cybersecurity and the next normal

Over the following articles, we've gathered together a tremendous range and depth of opinion (and topics covered!), as industry experts offer their thoughts on cybersecurity into the future. Part 1.

Cybersecurity innovation and the advancements in its underpinning technologies never rest; it can't because neither do the bad actors who are trying to breach organisations.

BY DAN PITMAN, SENIOR SECURITYARCHITECT, ALERT LOGIC

HACKERS are both innovative and lazy. A successful hacker, like all great engineers, finds efficient and graceful ways of achieving their goal, which drives cybersecurity innovation and is why security is mostly a human challenge, not a technology one.

When we think about the detection of attacks, signature-based detection has primarily run its course and reached a plateau, and it relies on an attacker using a known method to operate successfully. When successful, the penalty for the attacker is usually just an opportunity to try again.

More modern methods based on machine learning, including behavioural analysis for baselining and anomaly detection, can be very successful, bringing technology-based detection closer to human analysis, and allowing security teams to close the gap between the known and the unknown.

But this is only a step forward and not a new paradigm in detection. We're still dependant on what came before, just in a more intelligent way. It takes human understanding and intuition to find the genuinely new.

Ultimately whilst technology underpins security, it is not the deciding factor that allows an organisation to be secure. In the same way, the deciding factor to be successful in digital transformation is not a new technology: It is the culture of integration between business and technology delivery. Security is going through that transformation and to see results–for businesses to be protected–business and security leaders will need tofind a middle ground.

So, the next normal for security is not a new technology, it is not a new silver bullet that can magically stop breaches. It is an improved, business-focused culture in cybersecurity, mirroring the changes we've seen over the past two decades in information technology.

Security's strategy with the business has historically focused on convincing business stakeholders of the risks of inaction or action, but business and security professionals often have different definitions of what constitutes acceptable risk.

The biggest challenge is that, for nearly all companies, security does not provide tangible or easily measurable value. It does not deliver revenue; it is seen as slowing or delaying business results. But with little to no cross over between skills and disciplines with other teams, combined with one of the most competitive job markets and high capital expenditure for new technologies, it's little wonder that business leaders are weary of the topic of security.

When looking for point solutions, organisations find themselves in a fragmented mess of an industry, all seeming to promise the same thing in slightly different ways. Many vendors, managed security services providers (MSSPs) and cybersecurity vendors make the mistake of just lumping anything with security in the name together and trying to deliver on it all.

In the end, only two things matter, are we doing the most we can to reduce the likelihood of attacks and equally importantly, to reduce the impact of attacks-when they happen.

The transformation underway in the security industry today can enable that to happen. The service mentality is shifting away from "all things security, your mess for less" to one focused on breach detection, risk awareness and visibility. This is focusing security expertise where it matters, but organisations need to catch up and ensure security becomes part of their 'business as usual'.

How does cybersecurity relate to the workplace? Asks Jérôme Robert, Managing Director, North America, Alsid.

Considering that the vast majority of data breaches - some reports say as many as 90% - involve at least some element of human error, it's clear that cybersecurity is a human problem requiring a human solution (at least in part). The classic response from cybersecurity professionals is to create awareness campaigns, make colleagues sign agreements about using authorised devices, and even put together some great-looking (or not so great-looking) computer-based security training. The reality though is that most employees largely ignore these measures and get on with their jobs.

To understand cybersecurity we must understand human behaviour. We have to remember that humans are fallible, and even well-intentioned employees will make mistakes on occasion. Cybercriminals are master manipulators with many tools in their arsenal. There is a huge range of sophisticated social engineering scams out there that involve manipulating someone to give away information or take a certain action - such as clicking on a dangerous but seemingly innocuous link. It's also incorrect to presume that it's just junior employees posing the biggest risk. There are plenty of examples of C-level executives being tricked. One alarming case took place last year when fraudsters used AI to mimic a CEO's voice to authorise a cash transfer.

A key point of friction between those tasked with keeping a company secure and employees getting on with their own day-to-day work is that there's a conflict of priorities. Dan Ariely, a professor of psychology and behavioural economics, gave a fascinating insight into his own behaviour with Duke University's online filing system. Frequently abroad, Ariely would find himself seething with rage as he tried to upload his work using the university's file management system and VPN, to

The biggest challenge is that, for nearly all companies, security does not provide tangible or easily measurable value. It does not deliver revenue; it is seen as slowing or delaying business results

no avail. He had a choice: either sit there waiting for the interminable authorised system to work, or use his own unsanctioned, insecure method and get his work done. Exhibiting classic human behaviour, he chose the latter.

The conflict is that the university wants to keep its network and data secure, but Ariely's priority is to get his work done. Although some employers think that they can strong-arm employees into complying with the rules, the reality is that if a system works poorly an employee will find a way to circumvent it. After all, an employee's priority is to get their work done. Everything else is secondary.

But from the IT/security team's perspective, ignoring the rules jeopardises the entire network. As non-IT colleagues see it though, the organisation is putting obstacles in the way of their productivity - their priority. Most people are dedicated to their work and want to get it done. And they'll ignore or work around locked-down operating environments when they get in the way.

According to a recent Forrester report, 96% of organisations in the UK have experienced at least one major cyberattack in the last year. This worrying statistic should send alarm bells ringing for businesses around the country, not least because it's actually unsurprising in this day and age. But, for the reasons outlined above, we need to be cognisant that a locked-down policy may end up not being the most secure option.

Cybersecurity is of course nothing new, but the need for upgraded cybersecurity systems has never been more apparent than it is now, according to Matt Parker, CEO of Babble.

While more and more have been working from home – a trend which is highly likely to continue long-term - cybercrime has been on the rise, as hackers have taken advantage of vulnerable IT systems which were not adapted to non-office based working or the blurring of private and professional lives, which means that employees are accessing work-related information on devices which may have security weaknesses.

Ways of working have been transformed and much more is required to raise employees' awareness of potential cyber threats and personal responsibility whilst working at home.

The new normal means that work and home life is now merged, with personal phones being used for business calls and business data stored on personal devices. Although employees have a personal responsibility to keep business data safe through online safety practices, companies also have a responsibility to create a secure cyber infrastructure for them to work within. Working practices are becoming more fragmented and adopting good online safety polices has never been more important. Organisations must be forward thinking, adopting long term measures, not just short-term practices to adapt to the sudden shift to agile working.

As we move to the next normal, updated user awareness training is vital. Humans make mistakes, forget things and often fall for fraudulent practices. User awareness training involves a formal process of educating employees about how to handle computer security, ensuring that proper procedures are followed, thereby reducing risk and keeping your organisation's data safe.

As the perimeter of our business environment has changed, we must also think about issues surrounding GDPR and compliance. Despite a huge recent overhaul in GDPR regulations, businesses may need to review once again how they are processing data in this new world.

Data protection is more important than ever in the next normal. Devices, both company-owned and personal, are synchronised with corporate networks to gain access to official information. This information needs to be guarded in several ways – mainly through encryption, antivirus and a decent firewall.

Device encryption is the process of scrambling text to render it unreadable to unauthorised users, therefore keeping data safe from cyber criminals. Anti-virus software scans, detects and prevents suspicious files and software infiltrating systems. A firewall acts as a shield between your network and the world wide web. It monitors the incoming and outgoing traffic and prevents suspicious packets from entering the network.

In the next normal, online backups will also become more important to protect business information from theft, fire or other kinds of disaster. Several copies of data in different locations, including cloud storage, provides the assurance that all your information has protection if an unfortunate incident occurs.

We have transformed over 2,000 clients' organisations through cloud-based solutions that are tailored to enhance efficiency, flexibility, security and customer loyalty, and we would always recommend that businesses ask themselves what their next normal is. Business leaders must understand that.

How they want employees to work in the future is essential to build in long-term business resilience through the correct CYBERSECURITY solutions that flex and change in line with your company. In today's world, there is simply no excuse for short term solutions.

INNOVISION2020
DATA CENTRE INSIGHTS + PERSPECTIVES

InnoVision: A very special issue of DCS Magazine dedicated to the data centre industry's visionary leaders and technology innovators

To herald the launch of the all-new Data Centre Solutions digital publication, we have produced a very special first issue, entitled InnoVision – providing an overview of the state of the data centre industry right now.

80+ Vendors from across the supply chain have provided their viewpoint on the future and innovation.

How will the data centre industry evolve over the coming months and years, what will be the major drivers and opportunities?

Read today

https://digitalisationworld.com/magazines

IN ASSOCIATION WITH

DATACENTRE SOLUTIONS

DIGITALISATION WORLD

Cybersecurity and the next normal

Over the following articles, we've gathered together a tremendous range and depth of opinion (and topics covered!), as industry experts offer their thoughts on cybersecurity into the future. Part 2.

Lifting the lockdown: Are consumer-facing sectors sitting on a fraud ticking time bomb?

BY PAUL HAGUE, CEO, BLACK DICE

Andy Barratt, UK managing director at global cybersecurity consultancy Coalfire, unearths an impending danger facing the UK's retail sector as it gets back up and running after weeks on hiatus:

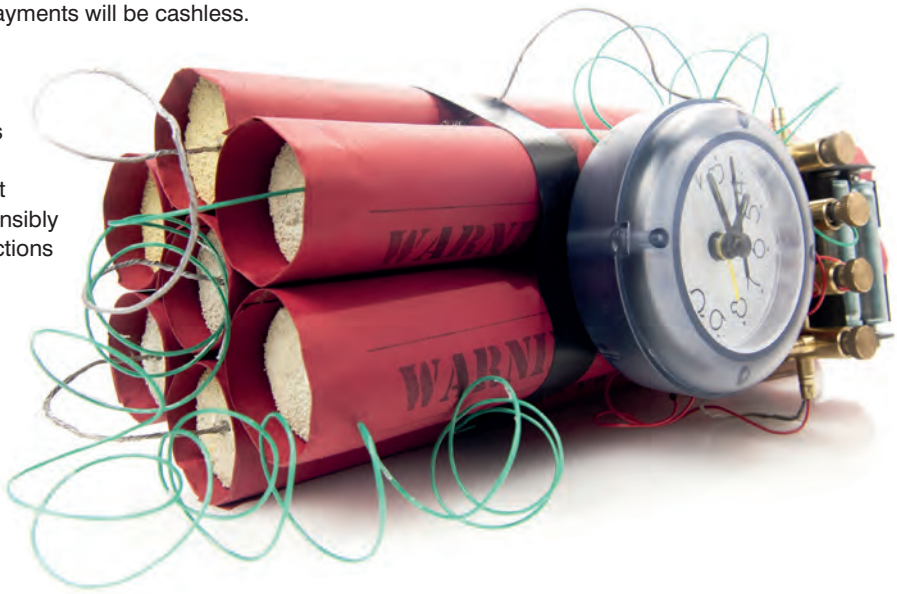
In 2018, people in the UK made just under 40 billion payments, of which some 62% were completed electronically via debit and credit card, contactless or remote banking. By 2028, it is expected that more than nine in every 10 payments will be cashless.

Traditionally, this sheer volume has been one of the banking system's fundamental security challenges. How does it monitor an incomprehensibly large number of transactions and keep its customers safe from fraud and cybercrime – particularly when it is often only a third party to purchases taking place with retailers?

So much of fraud detection comes down to identifying out of character behaviour. It's why many of us have been left high and dry at the hotel bar while on holiday abroad. Unusual purchases – both the location and the product itself – are red flags to the system.

Spotting uncharacteristic behaviour is a skill that one might think of as inherently human. But, when 100 million payments need analysing every day, it has to be done by a machine.

There are two parts to the solution. The first part



is to analyse the behaviour of the consumer for 'unusual' purchasing action and then, secondly, use the aggregation of transactions that are reported as fraudulent or suspicious by the card holder. By doing so, you can then narrow down the locations all those payments have in common and a forensic investigation can be started.

But it is this very quality that, in our current situation, has me and lots of other cybersecurity and fraud experts worried.

Sleeping giant

The UK, following the example set by mainland Europe, went into nationwide lockdown in March to slow the spread of Covid-19. Sectors that rely on footfall – high street retail, hospitality, tourism and leisure – were put on ice, with many forced onto whatever life support was offered to them by the government. The country was temporarily closed for business and the number of transactions went through the floor as a result.

This creates an issue: less transactions equal less fraud. On the surface of it, this sounds great. However, the reported fraud is often the fastest way to determine if a smaller retailer with less security infrastructure has been compromised.

As a result, it is highly likely that a lot of cybercrime has gone undetected during lockdown and that criminals are sitting on locations that would normally only be identified through the common point of purchase analysis. Couple this with furloughed IT staff and other security monitoring costs perhaps being reduced and you have the perfect petri dish for cybercriminals to grow an extensive network of compromised retailers just waiting for them to start trading again.

A few months on and the 'green shoots' of recovery appear to be sprouting as shops are told to reopen – albeit in a much more limited fashion than they are used to. The number of purchases people make will inevitably increase and, as the economy reawakens and other consumer-facing industries are unshackled, transaction numbers will return to normal levels.

It's at this point that the criminals who have been expanding their network of compromised locations will have a quick rise in payment data that they can steal. We won't then know it's gone until fraud using the data is committed further down the line.

In reality, we might not know until Q4 or Q1 next year just how many payment fraudsters slipped under the radar, how many data and system breaches were perpetrated without detection and, perhaps most worryingly, how many cybercriminals snuck into retailers' IT infrastructures while the lights were off. They, like everyone else, are waiting to take advantage of our economic recovery too.

Edge of a precipice

Retailers and their customers are understandably desperate to return to normal. For consumers, a bit of retail therapy will be a welcome antidote to three or four months of relative solitude. For shops, an increase in customers and resultant revenue injection won't have come a moment too soon.
Commerce returning to a relative form of normal is to be celebrated for sure, but it is also a time for those of us whose job it is to police cybercrime and fraud to be incredibly vigilant.

I have no doubt that, while much of the UK's economy was in forced hibernation, cybercriminals and fraudsters were wide awake, plotting how to take advantage in this low-activity environment and positioning themselves in the best possible way to benefit when the tap is turned back on.

John Briar, co-founder & COO, BotRx, focuses on the rise of malicious bot attacks:

The use of automated bots online is increasing every day. From AI chatbots that deliver 24/7 customer service, to shopbots that automate online price comparisons, businesses everywhere are implementing bots to keep operations running smoothly, particularly as effects of the coronavirus pandemic continue. As companies are forced to move more of their business online, this has also exposed them to a greater security threat and organisations everywhere are being impacted by malicious bot attacks trying to take advantage. The problem is that this abrupt shift to a greater level of online activity has drawn attention from fraudsters, who are also looking to implement their own automated bots – bad bots that thrive in a digital-first world.

Indeed, as eCommerce and online purchases grow due to the coronavirus, cyberattacks against the financial sector have also increased by 238%. Health agencies in the US have fallen victim to DDoS attacks with hackers taking advantage of overwhelmed resources. There's also been an 820% increase in e-gift card bot attacks since the coronavirus lockdown began, and bots are even being used to spread

Covid-19 misinformation on Twitter

As these fraudsters continue to take advantage of the new virtual landscape, so too must cybersecurity evolve. A new level of awareness must be reached so that organisations can better protect their customers and their ever-increasing dependence on online business.

Remaining resilient against bot attacks in the new normal

Bad bots employ artificial intelligence and a host of

automated tools to masquerade as humans, stealing critical content, breaking into user accounts, and committing other forms of fraud. Traditional, reactive security solutions don't cut the muster when it comes to today's ever-evolving bot attacks. Passive solutions that follow action-reaction security by identifying an attack after it has happened, then deploying a counter measure fix, will struggle to keep pace with threat actors who never stop proactively seeking changes and advances in their attack methods.

Instead, organisations need to look towards implementing more proactive security measures. Moving from passive to proactive security can seem like an insurmountable hurdle, yet there are solutions out there that can help even small or resourced-strapped businesses to protect their assets. Moving Target Defense (MTD) has surfaced as just such an approach.

A term coined by the US Department of Homeland Security, MTD dynamically changes the attack surface to deflect attackers. By making the attributes of the network dynamic rather than static, MTD obscures the attack surface, much like attackers do to ensure bots go undetected. By hiding entry points and vulnerabilities, MTD reduces an attacker's window of opportunity and raises the costs of their probing and attack efforts.

Levelling the playing field

Remote access to our accounts like banks, shopping and travel are here to stay, and as malicious actors continue to take advantage of the security vulnerabilities created by it, MTD is a much-needed tool to level the playing field between defenders and attackers. In an increasingly virtual world, adding the proactive approach of MTD to traditional defence mechanisms is crucial to ensuring organisations remain resilient against malicious bot attacks now and in the future.

Rapid adoption of alternate operating models by companies in response to the challenges they faced this year has resulted in changes to internal, supplier, and customer processes and interactions, explains Paul Hague, CEO, Blackdice:

Many of these changes are set to remain in place as "the new normal" either by necessity or perhaps through resulting benefits, sometimes unexpected. CYBERSECURITY is more important than ever before as we emerge from lockdown and discover what new normal looks like for businesses and employees.

There will be an increase in the number of employees working from home and using unsecured devices to access sensitive business information. This has to be urgently addressed by companies. The attack surface is so much larger when employees are spread out. "Cybercriminals will always seek to capitalise on the latest trends to try and boost the success rates of attacks, and the coronavirus pandemic has created a perfect storm of a global news event together with dramatic changes in working practices and the technologies used by organizations," said Rafi Kretchmer, head of product marketing for Check Point.

As hackers and others leverage the wider attack surfaces and find vulnerabilities to gain access to networks, they don't usually attack the devices themselves as the data associated potentially has little monetary value

There are many serious vulnerabilities in our connected world, such as operating system flaws, no patching capability to name a couple. Most of these will use open source software with no time given to add adequate security to the code, its often just used as found.

As hackers and others leverage the wider attack surfaces and find vulnerabilities to gain access to networks, they don't usually attack the devices themselves as the data associated potentially has little monetary value. Unless it's connected to intellectual property theft. It's what the devices connect to that is important. Once they have access to a device, they can have access to the network to use the malware payload to connect to command and control servers. Then they can go on from there to exploit other vulnerabilities and the organisation's network.

With cyber-attacks now on the increase, it is more important than ever for organisations and individuals to be vigilant and not leave private data open to third parties. In the meantime, it is important to be educated on all the facts surrounding data privacy to limit the risks.

DIGITAL CHANGE MANAGEMENT SUMMIT

25.11 2020

www.dcmsummit.com

How Managed Service Providers and Cloud Service Providers can help SMEs on the road to digital transformation

A unique online event to connect MSPs, VARs and System Integrators with their target market

Cybersecurity and the next normal

Over the following articles, we've gathered together a tremendous range and depth of opinion (and topics covered!), as industry experts offer their thoughts on cybersecurity into the future. Part 3.

Securing the hybrid workforce begins with three crucial steps, according to Rick Vanover, Senior Director of Product Strategy, Veeam:

The days of everyone working from the office are gone for now. As businesses face this reality, a new era of work will emerge: the hybrid workforce, split between office and remote environments. While this transition brings opportunity, it also gives threat actors a chance to capitalise on the added strain that IT departments have been put under.

Amongst the array of cyber threats, ransomware continues to be the most prominent risk to organisations, with a 41% increase in 2019 alone. It's important they acknowledge this threat and deploy strategies to prepare, defend, and repair incidents before adapting to a hybrid workforce model. This process will prevent them from falling victim to attacks where data loss or ransomware a real risk.

Focus on education first, avoid reactive approaches to threats later

Education is the first step towards resilience. To avoid being caught by an incident, it's important to understand the three main mechanisms for entry: remote access, phishing attacks and software vulnerabilities. IT administration should isolate RDP servers with backup components, integrate tools to assess the threat of phishing attacks to help spot them and respond correctly, and force updates of critical software and firmware.

Implement backup solutions that maintain business continuity

An important part of ransomware resiliency is making sure that backups are easily accessible, but are set up so that they don't become a target. Requiring two-factor authentication for remote desktops or limiting shared account access can help. Backups with an air-gapped, offline or immutable copy of data paired with the 3-2-1 rule will provide one of the most critical defences against ransomware, insider threats and accidental deletion.

Detecting a ransomware threat as early as possible also gives IT teams a significant advantage. This requires tools in place to flag possible threat activity. For endpoint devices displaced remotely, backup repositories that are set up to identify risks will help to do this. Another option is encrypting backups wherever possible for an additional layer of protection, as it reduces the value of the data to threat actors threatening to leak it. When it comes to a ransomware incident, there are many options to recover, so explore and implement them properly.

Prepare to remediate an incident in advance

Even if prevention has been taken, organisations should still be prepared to tackle a threat if it's discovered. Have a list of contacts and a pre-approved decision chain in place. Organisations should know who to turn to quickly. If conditions are ready to restore, IT should be familiar with their recovery options, and be making additional checks before putting systems back online, such as antivirus scanning and forcing password changes.

Ransomware is a real threat. While no one can predict an attack, a strong defence and response strategy can mitigate the effects. Organisations must be as resilient as possible to protect their customers, data and reputation – now more than ever.

Cloud services, remote learning, self-service and IoT come under the spotlight, courtesy of Joerg Borchert, Trusted Computing Group's President:

The last few months have brought a period of unprecedented circumstances leading to drastic changes in our day-to-day lives. With this new

normal, we have had to adjust to a rapidly changing environment and new technology challenges.
The acceleration of cloud service adoption
Adopting cloud services was already being considered by organizations worldwide but the Covid-19 pandemic has drastically increased the need for remote services. Cloud initiatives are expected to account for 70 percent of tech spending this year, with Information as a Service (IaaS) set to reach $72.4 billion worldwide in 2020.

This trend was already growing, but the uncertainty of 2020 has accelerated this, with 84 percent of enterprises now running on a multi-cloud strategy. With cloud adoption showing no signs of slowing down, cybersecurity must be considered.
As the number of cloud-connected devices rises within the enterprise environment, Trusted Computing Group technologies will play a vital part in safeguarding personal data from inception and networks from attack. A security-first approach and building on essential principals of updating, protection and resilience, will benefit billions of IoT and cloud systems, providing a safe, secure future despite a growing cybersecurity risk in our increasingly connected world.

Remote learning

Remote learning has become a necessity during the ongoing pandemic and is likely to stay. Teachers and students have become accustomed to remote learning environments and are presenting content in innovative ways to make it interesting, exciting and inventive, ensuring students can still learn despite the unusual circumstances.

With traditional and online learning elements, remote learning offers teachers an integrated learning tool environment and an infrastructure for scheduling, registration, attendance and reporting. However, remote learning solution developers need to ensure mobile user friendliness as the form factors will be very diverse depending on different hardware, software, and application platforms such as MacOS, Windows, WinCE, and Linux.

Self-service portals

Self-service is now essential to provide a positive customer experience, with 70 percent of customers now expecting a company's website to include a self-service application. As call centers experience astronomical call volumes, organizations have adopted self-service portals to ease the strain. However, just like remote learning solutions, self-service portals will require mobile user friendliness based on the hardware, software, and application platforms used. If an enterprise's self-service portal is not mobile friendly, then customers are less likely to use it. Solution developers will need to incorporate cyber resiliency technologies to guarantee remote recovery and capability to avoid customer frustration at the point of interaction.

Challenge of distributed IoT devices

With more than 21 billion IoT devices expected by 2025, and with little or no security hardware on these devices, more must be done to create a safe and secure digital ecosystem. IoT devices often act as a bridge between the virtual and physical world, supplying a rare opportunity for hackers to interact remotely, providing almost limitless opportunities to compromise devices.

IoT devices need power, sensors, and microcontrollers to compute and feedback to a controller or processor. The main challenge in the distributed device scenario is the protection of network sensor nodes. The integrity of the network endpoints needs to be measured and constantly monitored to avoid endpoint compromises. As the threat landscape becomes more complex, device manufacturers should leverage Trusted Computing technologies to provide more agility and speed of deployment – safe in the knowledge that all layers of security are implemented to protect against the growing sophistication of threats.

Jonathan Sander, Security Field CTO, Snowflake, focuses on Cloud Data Security: the importance of trust:

The significant growth of cloud platforms as a means of storing and utilising data in recent years has introduced new security challenges.

A common challenge for cloud platform providers is customers not fully understanding what it means to operate in the cloud, which means they attempt to map older security models to new platforms instead

of making the most of all that the cloud has to offer. Cloud scale and elasticity is often seen as a security challenge rather than something which enables them to securely share and acquire live data.

One of the most effective ways to ensure their understanding of security features is by closely partnering with customers on their use of the platform and the positive impact this could be having on security. If customers can see the secure nature of the platform first-hand and understand the specific benefit to their business, they are more likely to invest further in cloud architecture and incorporate this into their data analytics strategies.

The recent shift in working from home has made these advantages all the more apparent. Remote working has had a significant impact on data security and has made it more important for companies to adopt secure data storage systems. This in turn gives vendors a new opportunity to educate customers on the benefits of a secure cloud platform.

Working from home has changed the dynamics of how companies address security policy, as it can no longer be built around on-premise solutions or physical resources. Data security instead must be able to work remotely too, and cloud platforms are built to be able to guarantee secure data storage wherever the workforce is located. This is an acceleration of changes that were already happening, but companies are now forced to consider remote data storage as a necessity rather than a luxury.

For cloud platform providers, it is vital to ensure security takes a more prominent role in discussions around data storage on the cloud so that customers know and trust the built in security protections of the platforms that they're working with.

Moves toward automating the Security Operations Centre gain surprising boost from Coronavirus, writes SIRP Labs Co-Founder & CEO Faiz Shuja:

Security-tool sprawl in Security Operations Centres (SOCs) has led to rooms filled with multiple banks of screens. It is not unusual for a security analyst to pivot their chair continuously between screens as they strive to keep a watchful eye over the many hundreds, sometimes thousands, of security alerts every day.

Cybersecurity incident response has always leaned heavily on manual processes. A new study from SIRP Labs reveals more than half of security analysts view time spent on mundane tasks as the worst part of working in a SOC and a major factor behind why staff churn is an enduring problem.

The pressure on in-house SOCs is amplified by a rising tide of threat alerts emerging from Security Information and Event Management (SIEM) platforms. The average SIEM at a mid-sized enterprise can produce several thousand alerts each day, far too many to resolve manually. According to the SIRP research almost a third (29%) of security analysts believe missed alerts due to high volumes are a significant, even serious, problem.

Security analysts are also hampered by having to use upwards of 12 different security tools in their day to day roles. Pivoting between each one, sometimes on different machines is another drain on their already limited time, especially when staff have been laid off or reassigned because of the pandemic.

For all its disruption and global inconvenience, it is starting to emerge that the pandemic has a surprising upside. Technological advances that were undergoing cautious adoption in the pre-Covid world - from digital transformation to Cloud collaboration and from robotics to process automation - have accelerated. In its recent report Forrester Research notes that the economic recovery when it comes will be a jobless recovery that will include an increase in automation investments.

The SOC is no exception. Highly automated SOCs are becoming a reality. As the flood of security threats increases, new tools are needed to manage the rising tide of alert data. Many SOC teams rely on Security Orchestration and Response (SOAR) platforms to provide them with actionable information.

However, these tools often fall short by failing to incorporate sufficient threat intelligence and context tied to the organization's risk. What they are crying out for is something that gives them a clear view of the nature and severity of alerts. Armed with this intelligence they are better able to make informed decisions about incident response priorities.

Due to the pandemic we are seeing growing interest in automation platforms that tie threat intelligence and context to an organization's individually tailored risk profile. Unifying the output from multiple security solutions into one easy to use interface saves security analysts from constantly switching their attention from platform to platform when tracking down and mitigating potential security risks.

Finally, they have a clear view of the nature and severity of threat alerts helping them make fast, informed decisions about incident response priorities. Here at least, automation is helping to ease some of the pressures of the job.

Angel
BUSINESS COMMUNICATIONS

WEBINARS

Specialists with 30 year+ pedigree and in-depth knowledge in these overlapping sectors:

Expertise: Moderators, Markets, 30 Years + Pedigree
Reach: Specialist vertical databases
Branding: Message delivery to high level influencers via various in house established magazines, web sites, events and social media

Semiconductor (Silicon/Compound)
Publications include: Compound Semiconductor, Silicon Semiconductor, CS China, SiS China

Power Electronics
Publications include: Power Electronics World

Future Mobility
Publications include: TaaS Technology, TaaS News

Data Centres
Publications include: DCS Europe, DCS UK, SNS International

SmartSolar UK & Ireland
Publications include: Solar and Power Management, Solar UK and Ireland

Sensors
Publications include: Sensor Solutions Magazine, Sensor Solutions International

Digitalisation
Publications include: Digitalisation World, Information Security Solutions, Managed Services

Photonics
Publications include: PIC Magazine, PIC Conference

Expert Moderators

Dedicated technical and time-served experts/editors

MARK ANDREWS
Mark Andrews is technical editor of Silicon Semiconductor, PIC Magazine, Solar+Power Management, and Power Electronics World. His experience focuses on RF and photonic solutions for infrastructure, mobile device, aerospace, aviation and defence industries

PHIL ALSOP
Journalist and editor in the business to business publishing sector for more than 30 years currently focusing on intelligent automation, DevOps, Big Data and analytics, alongside the IT staples of computing, networks and storage

JACKIE CANNON
Director of Solar/IC Publishing, with over 15 years experience of Solar, Silicon and Power Electronics, Jackie can help moderate your webinar, field questions and make the overal experience very professional

DR RICHARD STEVENSON
Dr Richard Stevenson is a seasoned science and technology journalist with valuable experience in industry and academia. For almost a decade, he has been the editor of Compound Semiconductor magazine, as well as the programme manager for the CS International Conference

For more information contact:

Jackie Cannon **T:** 01923 690205 **E:** jackie@angelwebinar.co.uk **W:** www.angelwebinar.co.uk
6 Bow Court, Burnsall Road, Coventry, CV5 6SP. UK
T: +44(0)2476 718 970 **E:** info@angelbc.com **W:** www.angelbc.com

Cybersecurity and the next normal

Over the following articles, we've gathered together a tremendous range and depth of opinion (and topics covered!), as industry experts offer their thoughts on cybersecurity into the future. Part 4.

Why unified storage is key to protecting your business with modern IT

BY WES VAN DEN BERG, VP & GM UKI, PURE STORAGE.

The COVID-19 pandemic has caused a huge amount of disruption for businesses. The majority of workforces have had to suddenly work remotely, and while this has been a necessity, it has created new opportunities for hackers looking to exploit new vulnerabilities with insecure home systems and networks.

It's therefore unsurprising that COVID-19 has created a surge in ransomware attacks, and as such many security firms are offering advice and new protective measures to customers. However, one area that is not discussed so frequently in relation to ransomware is the vital role that storage can play in mitigating the risk.

Prevention is no longer enough

In the vast majority of cases, once a business has been infected with ransomware it's already too late

to stop it. Therefore, anti-intrusion systems alone are not enough. If everyone agrees that the ransom should not be paid, the data, once encrypted, is unrecoverable. IT teams then have the responsibility of restoring data from backups, which may be out of date and result in data loss.

This approach also assumes that backups are available and haven't been encrypted or deleted by the ransomware attack itself.
Recently, attackers have increasingly targeted backups with the goal of deleting them,

acknowledging backups as an organization's last line of defence. Data recovery is then impossible, forcing companies to pay a ransom or resign themselves to the loss of data, which could do irreparable damage. Even if a ransom is paid it doesn't guarantee recovery of data or protection from future attack and extortion.

Using snapshots to combat ransomware

This is where advanced snapshots come in. Snapshots are designed to protect data in the same way as backups, but with the goal of minimizing data loss and restoration times. They serve as a detailed index and protect metadata which acts as a guide for restoring an organisation's systems, speeding up the process dramatically.

What's more, the concept can be taken further with our FlashBlade unified fast file and object storage platform via SafeMode snapshots. These unique, read-only snapshots are immutable and prevent ransomware attackers from deleting backups stored on FlashBlade, our cloud-optimised file and object storage. After being enabled, automated FlashBlade-wide snapshots are kept for a customer-specified period of time and cannot be deleted by the customer or even anyone with admin access to the FlashBlade system or backup software.

Restore speed – the underappreciated difference-maker

Even with immutable snapshots in place, organisations will be limited by the speed at which they can restore data to get them up and running again in today's fast-paced business environment. Imagine a major online retailer being down for even one hour, it could cost them many thousands or even millions in revenue. If hit with ransomware, that retailer will want to restore its secure data as rapidly as possible.

Organisations should insist on a backup solution that can restore data at a rate of hundreds of terabytes per hour for maximum speed to resolution, and near complete peace of mind against ransomware attacks.

With a solid cybersecurity strategy reinforced with advanced snapshots and a rapid restore solution, the restoration phase after a ransomware attack can be reduced from several weeks to just a few hours.

So far this year, we've seen an enormous rise in cyberattacks and the internet is currently drowning in malware and phishing scams as hackers attempt to exploit the general public for their own criminal gains, writes Tom Lysemose Hansen, CTO at Promon:

"As was to be expected, in the first half of 2020, there was an inundation of COVID-19-related phishing attacks, many of which aimed to trick victims into handing over login credentials and even their hard-earned cash. Unfortunately, it is not uncommon for malicious attacks to be tied to current affairs to ensure their scams are far-reaching and timely. Emails often appear to come from trustworthy organisations, or those in senior positions from within the likes of the World Health Organisation, or company directors. These have plausible subject lines to increase the chance of them being opened and the call to action being acted upon by recipients.

Beyond this, many of the attacks being observed in the wild have come about due to a rise in vulnerabilities found in both Android and iOS operating systems. In recent months, there have been a number discovered that allow attackers to gain unauthorised access to personally identifiable information, such as names, email addresses, and even credit card information. Some are even able to hijack security-sensitive apps such as banking and cryptocurrency apps.

With the ever-present and increasing threat of state hacking on the rise, these types of 'hidden' attack are, more than ever, a major and very dangerous concern for both companies and the wider public, particularly as it isn't immediately obvious that the end-user device is compromised. They also predominantly occur when a user unknowingly downloads malware onto their smartphone. Recent examples of which include the Cerberus banking trojan, or StrandHogg and StrandHogg 2.0, which are Android vulnerabilities that enable malware to masquerade as legitimate apps, all the while enabling attackers to steal information such as banking passwords and credit card information. While this is, of course, awful for anyone that might fall victim, the consequences for businesses are far more severe. Unlike with attacks on personal devices, successful attacks on business devices can result in enormous data breaches and compromised corporate networks.

As mobile devices are increasingly used for security-sensitive activities, such as online banking and mobile payments, the significant rise in these attacks has also become a major concern for app developers, who have to ensure that their apps uphold the highest security standards without delaying releases, or compromising the functionality of the apps themselves.

As far as the new normal goes, many companies have had to adapt to this new wave of app-based attacks, with one of the most common mitigations being the use of in-app protection tools, which have paved the way for developers to mitigate against the devastating consequences that cyber attacks targeting these apps can have. These tools aim to impede attackers' attempts to reverse-engineer and modify sensitive apps, while also monitoring a mobile app's runtime behavior and protecting against mobile malware.

In these instances, when in-app protection tools detect malicious activity, a protected app can modify its behavior in real-time to interrupt potential attacks. Response actions might include things like blocking the execution of injected code, notifying security administrators, and even terminating the infected app to stop the execution of a compromised application.

In these instances, when in-app protection tools detect malicious activity, a protected app can modify its behavior in real-time to interrupt potential attacks.

Ultimately, when it comes to in-app protection, it cannot be understated how detrimental the consequences can be if developers don't take the time to ensure their apps are meeting the highest possible security standards. Tackling the multi-faceted challenge of developing a successful mobile banking or cryptocurrency app is no easy feat, and developers have to contend with pressures from every direction. The demands to get an app built, tested, and published as quickly as possible are only going to increase. However, in the rush to market, app protection and security cannot be overlooked, and ensuring security on end-user devices should be a top priority if the rise of app-based attacks is to be successfully mitigated against."

Nigel Thorpe, technical director at SecureAge looks at cybersecurity in the new Wild West:

Being unable to control the security of remote home workers is significant. While employees sit at home connecting to business servers and applications through VPNs, remote desktops or the cloud all managed by the IT department, other processes running on laptops, connected to insecure home Wi-Fi networks makes the environment like the cyber Wild West. At the same time, hackers have upped their game, with a massive growth in the quantity and sophistication of phishing, malware and user account compromises.

We must assume remote network environments are hostile and employees are deliberately or unwittingly potential threats. Staff, now working from home and unobserved, are more likely to have fewer scruples about stealing data. Many organisations believe in full disk encryption as a solution, but once employees' laptops are running, the door is open to malware and accessing files, fully decrypted. And while the Zero Trust approach is important, it's evident it's no longer adequate and for the 'next future'. Driving security deep into the network itself is the only way.

Traditional approaches to security assume you can keep attackers out. Not true, so there needs to be another way of protecting data. IT Security must prioritise a 'data centric' approach, where security is built into data itself, using file encryption. If data is stolen, it remains protected and useless to the thief - even if extracted by staff.

Modern PKI-based file encryption is designed to work seamlessly so legitimate users aren't aware of the security functions' activity. This is the only way to ensure data is 100% secure in use, in transit and while stored, and no matter where it's copied.

Another assumption is differentiating between legitimate and illegitimate activity. . For each successful intrusion, a new rule is written so the attack, or data extraction, can't be repeated. As we see a multitude of ransomware attacks and data breaches daily, this is also mistaken. A deny-first approach must be taken.

For users working from home, security must be an inherent property, invisible from those generating and using it daily. PKI-based encryption enables Asymmetric Encryption, using two keys: a public key to encrypt and a private key to decrypt, allowing simple and natural file sharing across user groups, networks and in the cloud.

Encryption processes working at the file system level so humans aren't aware they're going on is paramount. Additionally, tightly binding authentication with encryption of data files ensures if information falls into the wrong hands – accidently, via insider theft or by malware - it remains encrypted and useless. Lax attitudes towards data protection, alleged Russian antics and Twitter's woes illustrate data remains vulnerable. Insecure, uncontrolled home environment networks mean there's a recipe for data theft by both cybercriminals and rogue employees. If security is built into the data itself, it won't matter where or when information is stolen - it will remain useless.

AIOPS SOLUTIONS ONLINE SUMMIT

ENABLING APPLICATION OPTIMISATION

The importance of proactive performance monitoring and analysis in an increasingly complex IT landscape.

29 October 2020

aiopssolutions.com

Cybersecurity and the next normal

Over the following articles, we've gathered together a tremendous range and depth of opinion (and topics covered!), as industry experts offer their thoughts on cybersecurity into the future. Part 5.

Andrew Hollister, senior director at LogRhythm Labs, on how cybersecurity will develop into the future:

When talking about the future of cybersecurity, we have to talk about working practices – I don't believe in the demise of the office, but I do think a significant digital transformation has taken place, which will impact where work is done in the long term. In order to facilitate that, some sacrifices to security were made, and organisations really need to review what their overall cybersecurity strategy looks like, and if it's predominantly aligned to on premise working, then it will need to pivot to support a more remote workforce.

The workforce being remote signals a change in visibility – you are no longer traversing the company firewall to access public services for example; we cannot monitor data being transferred across that choke point any more in many cases. This will lead to more innovation on the endpoint, device-side to claw back the visibility lost by endpoints leaving the corporate fold. It's along the lines of we used to try to secure the castle, now we need to secure lots of little enclaves and the communications between them.

The data privacy angle is also interesting, since no account seems to have been taken of this in many of the pandemic responses. It's difficult enough to protect data when you are trying to follow GDPR, but ignoring that requirement altogether is not a strategy. It does just demonstrate that there is more work to be done in the secure by design, and security being seen as an enabler, and a key part of the development lifecycle, not as an add-on or an afterthought, which appears to be the case here.

The privacy shield being struck down, could be seen as more political than technical, but it does underline the point that in an increasingly digital world, a harmonised approach to data privacy is not easy to come by. Some organisations dealt with GDPR by saying that they will not allow EU citizens to access their offerings, which is one way of looking at it, but it's

a bit limiting for your online business if you can only operate in your own jurisdiction – plus it is not trivial to enforce that either.

Ultimately, users will continue to be part of the security strategy, and we need to find effective ways to help users to operate information technology securely. The human mind is endlessly inventive, and ultimately will always find an easier, quicker or shorter route – often that can result in things designed to keep data secure being bypassed, and educating users to know when that's the case would help secure organisation data, as well as the individual. There can perhaps be a bit too much emphasis on phishing training, and testing etc, whereas there is a much broader mindset that could be taught, and the school education system could be a good place to start that.

Watch out for enterprise-like marketplaces, warns Mark Greenwood, Head of Data Science at Netacea:

The advance of anonymisation tools and the Dark Web have meant that marketplaces can operate more openly than ever before and users with bad intent can browse freely, without the fear of being identified. This has led to a growing sophistication of cybercrime marketplaces where billions of credentials are up for sale.

One of the reasons behind the proliferation of these marketplaces is the adoption of the 'as-a-service' business model. This has allowed the specialisation for services offered, but also the creation of sophisticated business models for cybercriminals where end-to-end specialised knowledge is no longer required.

Beyond primary activities, meaning carrying out the attacks or selling digital fingerprints or access to hacked accounts or servers, marketplaces for supporting services are also on the rise. They are, for instance, providing access to platforms for webstores fronting cybercrime services and products, job opportunities and training tips. A good example is OnionIRC, a school for hacktivists on the dark web that was launched in 2016 by members of the hacker collective Anonymous for teaching hacking and coding techniques and encryption mechanisms. The service was an internet relay chat forum, allowing users to remain anonymous through encrypted communications over the Tor network.

Indeed, people that are purchasing the products and services available on these marketplaces have an expectation of professionalism which means providing on-going support is a key requirement for standing out and selling more. As part of our recent work into the Genesis market, we discovered that browser profiles that were gathered from victims' computers and sold on in this marketplace were then periodically updated as new updates were received from the compromised machine. Similarly, tools and services sold have customer service contact points and money-back guarantees attached to the usability of the software or data sold. Open-source tools, previously shared openly by developers on platforms such as GitHub, have also been commoditised and monetised through SaaS models, with ongoing support offered to customers.

All of this is driving a lower barrier to entry for carrying out attacks, or acquiring or making use of ill-gotten gains. Anyone who's interested in launching a cybercrime business today or capitalising on an identified opportunity can easily find partners and required tools online.

The way cybercrime marketplaces are evolving in terms of complexity and organisational capacity make them, under many aspects, work exactly as a major enterprise. This means we're likely to see many more of them pop up in the near future and become part of the "new normality".

Professor Pamela Briggs from Northumbria University says that people still aren't sure who the trusted guardians for cybersecurity are:

In recent years people have lost trust in the data giants (Google, Facebook) but have also lost trust in government (Test and Trace, plus if we go back a few years the refusal to accept the national identity card) and so where does that leave us? One answer is that cybersecurity governance is gradually getting better. In the UK we now have a National Cybersecurity Centre which – unlike the GCHQ of the past – is much more focussed on giving good advice to citizens and businesses and acting as a responsible reporting point. They are offering certification services ('Cyber Essentials') for businesses of various sizes.

In tandem with this, cyberinsurance is starting to get off the ground. At the moment this is a bit of a messy business as the insurers don't really have all the actuarial data they need, and it has been a bit of a race to the bottom, but cyberinsurers could work as a force for good as they will gradually insist on businesses improving their cybersecurity posture in order to get good insurance deals and therefore offset liability. So I think the picture for businesses could improve, but I'm less sure about the picture for individual citizens who have been recently exposed as never before (through the massive change in digital habits arising from COVID-19).

Authentication methods need to be more secure to enhance the customer experience, says Keiron Dalton, VP at Payfone:

The coronavirus pandemic has affected all aspects of society, from socialising to the way we work. With high-street stores closed during lockdown the public became accustomed to shopping and banking online. With more people now using their smartphones or tablet to open bank accounts and to make transactions, it is imperative companies work to build the same sense of trust amongst their customers that they would when interacting face to face. The best way to do this is to reduce friction in the customer experience, without having to compromise on security. While online has now become the new norm, in terms of banking and shopping, there still remains a layer of uncertainty for some users, especially those who have just been introduced to the faceless interaction. For many, the prospect of banking online remains daunting. It's important the financial services sector provides the necessary support to those customers taking their first steps.

Recreating a secure, familiar experience

Building trust between business and customer is vital and maintaining a positive customer experience is key to making this happen. A user should be able to make a transaction or sign up for a bank account with as little disruption, but they also need the reassurance their information is secure. It's all about recreating the human experience as best as possible, allowing customers to have a seamless, easy, and secure experience online.

SMS One Time Passcodes (OTP) has generally been an efficient technique to achieve this, as it provides heightened security and reduces reliance on outdated methods such as static passwords. However, as fraud methods have become more complex over the years there are now ways to bypass OTP, for instance through SIM swapping. There's also an element of friction to their use, which is something that should be reduced where possible, while guarding data from the latest threats.

Outdated techniques need to be replaced

With online interactions set to dominate, organisations need to introduce new ways to verify customers without the need to go into a bank branch, while still providing the same, if not better, standard of security and familiarity.

Banks are able to verify a customer's account is authentic by analysing insights from the behaviour attached to a user's phone number. Techniques like this can be employed in areas such as auto form pre-fill, which pre-fills online application forms with verified information from authoritative sources, which in turn builds trust by guarding against fraud while avoiding making the customer experience too cumbersome. With technology innovating at a considerably fast rate, we will likely enter a new era of customer identification.

The last few months has seen most organisations adapt their operations quickly. However, now is the time to implement the long-term changes that will future-proof businesses. Building and maintaining customer trust needs to be done in a different but secure way, and those taking the leap by developing new approaches will be the ones to flourish.

CELEBRATING 10 YEARS OF SUCCESS

The 2020 DCS Awards feature 31 categories across FOUR groups.

THE DCS AWARDS are now firmly established as the data centre industry's premier annual celebration of all that is great and good. End user projects, product innovation and individual excellence are all recognised in an evening that pays more than lip service to the idea of data centre and IT convergence. So, the award categories cover both the facilities and IT aspects of the data centre, recognising the achievements of vendors, their business partners, their staff and their customers.

Getting involved with the DCS Awards couldn't be easier. Take a look at the award categories, and make sure to nominate your company, a customer, or maybe an individual – better still all three (!) – for a chance to be recognised for outstanding achievement when it comes to projects, product innovations and individual contributions within the data centre industry.

Once you've made your nominations, make sure to book a table for the Awards night. You wouldn't want to win an award and not be there to collect it! (And even if you don't win an award on the night, there's a cocktail reception, three course meal and a top comedian to entertain you – we have a track record of booking individuals on their way to the top of the comedy circuit).

To 'We look forward to welcoming you to the Awards night in December.

NOW, GET NOMINATING!

WHY ENTER?

MAXIMISE VISIBILITY
Free PR opportunities with 5 months of marketing utilising the Digitalisation World portfolio.

POSITIONING
Position your product or service as an innovator in your field.

INCREASED CREDIBILITY
An award win, shortlisting or nomination acts as a 3rd party endorsement.

NETWORKING
Over 300 industry leaders attend the gala awards evening.

COMPETITIVE ADVANTAGE
Gain an advantage on your competitors.

NOMINATION IS FREE OF CHARGE

The DCS Awards panel will validate entries and announce the final shortlist to be forwarded for voting by the readership of the Digitalisation World stable of publications in October 2020.

The winners will be announced at a gala evening at the LEONARDO ROYAL ST. PAUL'S HOTEL, London on 10 December 2020.

DCS AWARDS 2020

www.dcsawards.com

Supported by

dca The data centre trade association

Cybersecurity and the next normal

Over the following articles, we've gathered together a tremendous range and depth of opinion (and topics covered!), as industry experts offer their thoughts on cybersecurity into the future. Part 6.

Cybersecurity after lockdown: the new risks and how to stay secure

BY RICH ORANGE, HEAD OF UK&IRE AT FORESCOUT

DURING LOCKDOWN, organisations were faced with the challenge of ensuring business continuity in a world where lockdown measures were a necessity. While many were quick to enable remote working, and as a result saw many benefits for employees and employers, it also created hidden CYBERSECURITY risks. The implementation of additional IoT devices, VPNs and cloud solutions has quickly mobilised a remote workforce, but it has likewise created new routes for malicious actors to find their way into the corporate network.

With restrictions lifting and many organisations looking towards a return to work, cybercriminals are preparing for the same. With this in mind, here are three tips to reduce the risk of a cybersecurity incident after lockdown:

Knowing what you've got

Knowing where threats are coming from is a gamechanger. Achieving the nirvana of a complete asset inventory (or CMDB) is hard but imagine having 100% visibility of all your connected devices and software, what a game changer that could be. A great range of devices and software go undetected within organisations today and this has been further complicated recently by employees accessing

the network remotely. New kit such as laptops have been procured at a rapid pace to enable employees to do their jobs effectively from home, which also means a greater number of devices to gain visibility over. Without this, they could function as a backdoor into the network, with IT teams none the wiser as to where the attack originated.

Assess cybersecurity hygiene

Once all of the devices have been discovered, it's important to assess their cybersecurity posture and exert controls from there. Not all devices were made equal and that means some are less secure than others. This is where solutions which can not only discover and monitor but can assess their security posture come into their own. Understanding the latest patches and whether devices are running on the most up to date systems is essential to keep a business's cyber hygiene in check. Security teams can then implement another essential security measure - a 'zero trust' policy.

This approach centralises around the idea that no device should ever receive automatic access to a network and should have to verify itself to get that privilege, which is particularly important if personal devices are now being used to do professional work.

A digital quarantine

We have seen in recent months that limiting unnecessary interactions prevents the spread of coronavirus. The same is true of cybersecurity, where isolating individual elements of a system can prevent a breach from becoming a catastrophic incident. Segmenting a network into its distinct components stops malicious actors from laterally moving across an organisation's network following a breach. Just as a hospital protects patients from quarantining different sections from each other, so too can the network prevent a single breach becoming widespread.

Many businesses have been under more strain than ever since the onset of COVID-19, and the return to offices proving yet another hurdle to overcome. However, with the right solutions and procedures in place, organisations can protect themselves and their networks from a fully-fledged cyber attack and further business disruption - at a time when ability to survive is most needed.

Safi Raza, Director of CYBERSECURITY at Fusion Risk Management, offers the following comments:

The events of 2020 have drastically changed the work environment for years to come. An estimated 42% of the US labor force is working from home during the pandemic, with little hope to be back in the office by January 2021. The organizations that were early adopters of digitisation and cloud migrations were able to swiftly resume operations remotely, while organizations that maintained most of their technology stack on-prem had difficulties returning to normal. For instance, many organizations had to quickly provision VPN connectivity, upgrade infrastructure, add firewalls, and routers to handle multiple-fold increase in usage.

The billions of financial transactions that once occurred behind fortified infrastructures are now being conducted from fragile home networks – which is a nightmare for CTOs. As a result, they are exploring multiple venues from employee training to new technology deployment. Remote employees are sharing their home network with smart TV, phones, tablets, and various IoT devices that are not adequately secured.

Wardriving

Wi-Fi is ubiquitous, but its ease and convenience make Wi-Fi hot spots a target. Wardriving is the act of discovering and exploiting connections to wireless local area networks while driving around a city or elsewhere. With most employees connected to corporate networks remotely, the odds of successful cyberattacks are in hackers' favor. Wardriving attempts are expected to increase during the pandemic.

Deep fakes - When Seeing is not believing

Deep Fake is a type of artificial intelligence used to create convincing images, audio, and video hoaxes. Businesses are spending more on security awareness training, phishing, and ransomware protection. Although phishing attempts make up 90% of Social Engineering attacks, bad actors are slowly migrating their social engineering efforts to Deep Fakes.

In March of this year, criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 ($243,000).

These AI applications are getting more sophisticated and widely available to purchase. Users can download the software and appear as someone else during a Zoom meeting. Security experts have raised significant concerns about the potential damages of this technology.

Hackers'R'us

Hacking services have always been available to purchase on the Dark Web. However, these services are increasing. Dark web users can browse through a variety of hacking tools that offer Ransomware as a service, phishing as a service, and more. Cybercriminals who lack the knowledge and skill to conduct sophisticated attacks can buy a hacking toolkit to easily execute a cyber-attack.

CYBERSECURITY skill shortage

Many colleges and universities have begun to offer Cybersecurity degrees to help reduce shortages in the InfoSec field. However, these graduates will still require 3-5 years to develop cybersecurity proficiency in the real world. This lack of skill is a significant threat to our data, and unfortunately, is a problem that won't be subsiding soon.

The attacks on critical infrastructure, election meddling, and attacks on local governments will continue to rise through 2020 and 2021.

Overall security spending has already increased for this year. And businesses will continue to increase their technology and security expenses in 2021.

No anonymity, privacy, security or sleep, warns Peter Bassill, Founder of Hedgehog CYBERSECURITY:

The world has changed. At the close of 2019, something happened and the world as we knew it went to hell in a handbasket. Anonymity and security of information have always been a diminishing commodity, but the last six months has eroded it to extinction. Welcome to the next near-norm. I have never felt more sorry for my colleagues on support desks.

The global Corona pandemic has changed the state of anonymity forever. In the UK, and many other countries, Track and Trace programs have been half thought out and implemented in a rush. For the criminal-minded, dumpster diving is back. And it is so rewarding. Finding a worthy target is as simple of buying a coffee and giving up a fake name and phone number. Watch the staff write it onto a sheet of paper. Guess where that paper ends up? The majority of the time, it is not a crosscut shredder. In one dumpster dive earlier this month I netted more than 200 names and phone numbers.

The Track and Trace initiatives have also starting nailing shut the coffin on anonymity too. Only last week my favourite coffee shop stopped taking cash. It is card payment only. So if you are trying to stay "off-grid" using cash for payments is getting harder and harder.

It isn't only the populace that is affected. Businesses are taking a hammering too. With reduced movements and increased remote working, the challenges for securing the flow of information have increased, and the workloads on overburdened IT departments skyrocketed. Rapid implementations of remote operations, VPN's, webmail, home printing and the like has started to take its toll on security. Two out of five businesses that we reviewed in the last month had critical security flaws in their remote working deployment. Some of these were as simple as providing staff with a secure shredding pickup server. Some were more sinister. One company had all its data encrypted after allowing employees to use their own devices on the remote network.

The typical answer we see businesses adopting is "buy more flashing lights". Vendors have been quick to ram "solutions" into clients, and while I agree that the right appliance will help, it is merely not addressing the overburdened IT teams. You can have the best technology at your fingertips, but if your IT team are reaching near exhaustion, or are already exhausted, then you are close to the dreaded breach.

When you think the new near-norm couldn't get any worse, the EU weighed in and killed the EU-US Privacy Sheild agreement. Sensible businesses are now scrambling to cover all their documents, contracts and such into a form that can demonstrate compliance with the SCC, or Standard Contractual Clauses. CIOs and CISOs now have to work to identify which suppliers and vendors operate on the privacy by design principle and which do not. For the vendors that do not, customers will be slipping through their fingers and moving to suppliers who can.

Data Sovereignty has become a new business horror phrase. The principle is that data should physically remain in national or regional jurisdiction, ensuring that that region's laws and practices are the ultimate authority. Adhering with Data Sovereignty is going to be hard. For predominantly Software as a Service operated businesses, this may mean changing entire suppliers and frameworks.

What does the new near-norm hold for us?

An increase in government-sanctioned surveillance and monitoring is a given. With that comes a step increase in phishing attacks as consumer information is more readily available. Along with the increase in Phishing will be an increase in information and identity theft.

Homeworking is more normality over office working, and while some businesses will return to the office environment, some will embrace home working and the cost savings that come with it. For staff, this may mean a better or worse situation.

Cross border data exchanges will still happen, but the paperwork surrounding them will become more burdensome.

Cyber attacks will start focusing more on the end-user. For businesses that have adopted the home working model, there is a greater chance of compromising the end user now. Businesses attack surfaces have increased exponentially.

Cybersecurity and the next normal

Over the following articles, we've gathered together a tremendous range and depth of opinion (and topics covered!), as industry experts offer their thoughts on cybersecurity into the future. Part 7.

Following the mass migration from office to remote working for many organisations, cybersecurity has never been so critical, says Jim Shook, Director, Cybersecurity and Compliance Practice at Dell Technologies:

As Europe enters an extended transition period of social distancing measures, and we continue to adapt to a workforce that primarily works from home, the scale of the surface vulnerable to attack has significantly expanded. The increased level of risk is being acknowledged across industries, with Europol warning that they expect the number of cyber-attacks to increase, placing cyber-crime as one of the top four crime categories. IT decision-makers must have a trusted partner to turn to who can give some much-needed clarity when faced with these challenges. Today that clarity comes in a shift of tack: instead of committing all efforts to prevent an attack, organisations must also ensure they have the right data protection and recovery measures in place for when that attack happens.

A consequence of having so many employees working from home is the increased number of endpoints that are now vulnerable to attack, along with the potential for less control over those endpoints. Organisations already had to move away from perimeter-based protection. But now, almost overnight, they have to manage and protect thousands of new endpoints in varied work-from-home locations. And at the same time as securing against attacks, they must continually enable their teams to be productive.

Of course, it is never a case of "one size fits all" when it comes to an organisation's approach to security. Every security team needs to properly understand its particular business, risk appetite, threats and the regulatory environment to properly align with the most likely problems they will face. Regardless, recognising the importance and place for cyber resiliency will pay dividends for the future, across the entire sector spectrum.

Building cyber resiliency is a layered approach. To start, executives need to ensure they understand the complex threat landscape for their business and sector. The crucial next step is for teams to identify the businesses' most critical applications and data, and, as part of a comprehensive risk management programme, embed a technology solution to protect that most precious cargo. It is here that data vaulting comes into play.

Deploying secure infrastructure to store the business's crucial data, and supported by an analytics platform to detect malicious activity, data vaulting is a must-have strategy, ensuring that a business can recover its most essential data in the event of an attack.

In the face of current (and future) cyber threats, I believe that a secure data vaulting strategy must be at the heart of a business' security plan. Security chiefs must implement and sustain a recovery solution in addition to protection capabilities. This is not a pessimistic view for the future, but a realistic one - the massive increase in destructive cyberthreats and attacks cannot be overlooked, and businesses must be prepared.

Neville Armstrong, Service Strategist, Fordway, explains why understanding your organisation's Risk Appetite is vital for effective security:

In a digital world, it is more important than ever to provide assurance that data is secure, maintain customer trust and protect reputation. To address this, organisations need to understand the risks they face and assess them in the light of their own Risk Appetite. They can then put appropriate governance and compliance in place to manage the most critical risks.

Risk Appetite can be difficult to quantify. It requires a full understanding of assets, threats and vulnerabilities

i.e. the impact on an organisation's activities if a risk was realised, such as if an unprotected mobile device was lost or a ransomware attack was successful. This means considering three factors:

- the organisation's ethical stance and culture
- the legal and potentially moral frameworks it operates in, which vary greatly across jurisdictions and even within 'standardised' trading blocs such as the EU
- the organisation's security operations and requirements, which will depend to some extent on the sector in which it operates. This includes technical architecture along with formal policies, processes and procedures

A measure of an organisation's Risk Appetite could be the threshold value above which it treats each of the risks identified as a potential disruptor to operations, or the approval mechanisms in its change management.

When organisations understand their Risk Appetite, decision-making becomes simpler because leaders understand the parameters within which they operate. This enables them to make informed choices about where to invest to protect against the most critical risks to their business and where, with respect to security, they can realise value. For example, patching is a key aspect of protecting against cyber risk, but should it be done weekly, or is monthly sufficient? Does a weekly process provide significantly greater benefit for the additional cost and time required? Each organisation will have a different answer, depending on its Risk Appetite and which threats it has identified as the most critical.

Being averse to risk can be extremely costly, as overbearing restrictions mean a slow response to changing situations. Some risk can be a positive thing. Organisations need to innovate, so may actively incur calculated risks as they grow their business into new areas. However, taking this too far can be even more costly and put their future in jeopardy.

The impact of getting risk management wrong include:

- damage to reputation – how the outside world and its staff view the organisation
- loss of trust, resulting in loss of market and customer confidence
- financial loss: both primary commercial impact through fines and penalties and secondary impact due to loss of reputation after a compliance breach. There may also be contractual penalties and the cost of insurance to transfer risk

- loss of competitiveness, due to restricted access to markets and potentially loss of business
- loss of productivity, if the operating environment is barred or services are suspended.
- staff retention, due to the stress within the working environment.

Once an organisation has assessed its Risk Appetite, it can develop policies to manage the most critical risks. These might address both corporate values and behaviours, which frame how staff operate, and the processes required to carry out day-to-day operations. In developing policies, organisations need to assess how their users work and how digital technology can be aligned to organisational strategy without compromising security. The ITIL framework for service management can assist here; version 4 has been designed for the digital world and will help organisations make change at pace while maintaining integrity. They can then apply governance to review compliance to their policies.

The organisation's chosen stance should be reflected in tailored management systems. An approach that well managed organisations have implemented to streamline governance and compliance is to consolidate security, quality, environmental and service management systems (ISO27000, ISO9001, ISO14001, and ISO20000). This means that, in certain areas, they have single policies to manage instead of multiple policies across different systems. A streamlined environment with no or minimal non-conformance means less spend on remediation.

A new normal needs a new cybersecurity approach, according to Nick Offin, Head of Sales, Marketing and Operations, Dynabook Northern Europe:

As lockdowns ease and economies slowly begin to wake up, business leaders are starting to think about the lessons learnt during this period and how they can be used to re-shape the future of work. An after-effect of the pandemic for many organisations has been that employees can continue to work effectively, no matter where their location is. Those who once shied away from remote working programmes are now re-imagining their operational strategies to include them. However, the rise of remote workers doesn't come without its challenges and, unsurprisingly, security concerns have topped the list.

COVID-19 has undoubtedly put a strain on organisations bottom lines. Many may be considering making cuts or reducing investment in certain areas of the business that are viewed as non-critical. It's fundamental that cybersecurity isn't part of these cutbacks as this short-term outlook can have a detrimental effect on the long-term protection of a business.

In fact, this new post-pandemic operational environment has created a need for businesses to rethink their cybersecurity position altogether. Updating staff education According to research, almost 90% of data breaches are caused by human error. It's well known that passwords are merely a speed bump for today's sophisticated cyber criminals, and all it takes is for one wrong click on a fraudulent link or a laptop left on a train to compromise business or employee-sensitive data.

The current climate has seen cybercriminals looking to capitalise on the hysteria surrounding COVID-19. In the first quarter of this year, there was an increase in phishing-related email cyber attacks by over 600%. Many used COVID-19 related themes to create urgency and anxiety. According to the National CYBERSECURITY Centre (NCSC), its newly launched suspicious email reporting service which launched in April receives an average of 16,500 emails a day.

With this in mind, team training and education around cybersecurity has never been more important. After all, your employees are your first line of defence against cybercriminals. Organisations need to educate their staff on the new CYBERSECURITY landscape post COVID-19, including how to handle sensitive information correctly when working outside of the office. Part of this training should cover why and how certain security solutions are deployed and their own responsibility to carry out good cybersecurity practices.

Investing in the right tools

Although, it's not just down to staff being extra vigilant. Technology budgets may shrink as businesses enter post-COVID recovery, however, hardware and specifically laptops – remain an integral part of employee protection whilst working remotely and should not be ignored. Devices with facial or fingerprint recognition and hardware-based credential storage capabilities provide a secure initial defence against cybercriminals, reducing the risk of unsolicited login to the device.

Other defences include zero client solutions, these go a step further to ensure devices themselves do not retain sensitive information. Instead, information is stored on a central, cloud-based system so if a device is lost or stolen, this information remains secure. According to a recent Gartner poll, 48% of employees will likely work remotely at least part of the time after COVID-19, versus 30% before the pandemic. With remote working at scale here to stay, security will remain the most important challenge that many organisations will not have come across before. Staff education and technology that is up to the job should be the foundation of any business cybersecurity strategy in the "new normal."

CELEBRATING 11 YEARS OF SUCCESS

Announcing the 11th edition of the premier IT awards: The Storage, Digitalisation + Cloud Awards 2020.

In what has been, and continues to be, extraordinary times for the business world, it seems doubly important to recognise the projects, innovations and individuals which have made such a huge difference during 2020. Almost overnight, employees switched from office working to working from home, and the new, or next, normal, means that, into the future, what might be called a 'hybrid work' model looks set to evolve, with flexible working very much the order of the day. What was already becoming a trend as part of many organisations' digital transformation programmes, has been accelerated.

The SDC Awards 2020 will celebrate the achievements of end users and the IT community as they have innovated like never before to ensure business continuity in these challenging times. This year more than any other, please do make sure that you enter our SDC Awards. There's no limit to the number of entries, all of which are free of charge, and we'll be promoting all the short-listed entries via Digitalisation World's multi-media platform over the coming months, ahead of the awards ceremony. We really do want to celebrate and recognise the many amazing achievements which have come about in response to the coronavirus.

WHY ENTER?

MAXIMISE VISIBILITY
Free PR opportunities with 5 months of marketing utilising the Digitalisation World portfolio.

POSITIONING
Position your product or service as an innovator in your field.

INCREASED CREDIBILITY
An award win, shortlisting or nomination acts as a 3rd party endorsement.

NETWORKING
Over 300 industry leaders attend the gala awards evening.

COMPETITIVE ADVANTAGE
Gain an advantage on your competitors.

NOMINATION IS FREE OF CHARGE AND VOTING IS DONE BY THE READERSHIP OF THE DIGITALISATION WORLD STABLE OF PUBLICATIONS.

SDC AWARDS 2020

www.sdcawards.com

Cybersecurity and the next normal

Over the following articles, we've gathered together a tremendous range and depth of opinion (and topics covered!), as industry experts offer their thoughts on cybersecurity into the future. Part 8.

According to **ANURAG KAHOL, CTO at BITGLASS**, for most businesses, securing the remote workforce has been a growing priority for some time, but the unexpected emergence of COVID-19 has propelled it up the corporate agenda in a way that few could ever have imagined:

THE RAPID SHIFT from office-based work to home-based work, combined with a lack of adequate forward planning, has made the transition a painful one for many. Simply finding a workable remote solution has been challenging enough, let alone one that meets all the same stringent data protection measures typically found in an on-premises setup.

And all the while organisations are considering their options when it comes to more permanent remote work, misconfigurations of cloud databases continue to plague enterprises around the world and be a leading cause of data breaches.

Cloud adoption is clearly outpacing the adoption of the tools and expertise needed to properly protect data in cloud environments; this is supported by the fact that 99% of cloud security failures will be the customer's fault through 2025, according to Gartner. Misconfigurations will continue to be a leading cause of data leakage across all verticals.

In addition, highly niche cloud tools provided by second-tier cloud service providers are making their way into enterprises. While services that cater specifically to individual industries or company departments are gaining traction, they do not typically have the same native security measures that mainstream cloud services do. Regardless, companies are gaining confidence - even if it's a false sense of confidence - in their ability to utilise the cloud and are adopting these second-tier and long-tail cloud apps without considering all of the security ramifications. Enterprises will need visibility and control into all of their cloud footprint, including niche services, in order to proactively mitigate any vulnerabilities and properly secure data in the cloud.

Finally, threat actors continue to enhance their current tactics, techniques, and procedures (TTPs) as well as create new ones in order to infiltrate businesses and steal data, implant ransomware, and more. One technique that will continue to gain traction is lateral phishing. This scheme involves a threat actor launching a phishing attack from a corporate email address that was already previously compromised.

Even the savviest security-minded folks can be lulled into a false sense of security when they receive an email asking for sensitive information from an internal source – particularly from a C-level executive.

With the increasing number of enterprises storing sensitive customer, employee, and business-critical data in the cloud, it is essential to rethink the way that cybersecurity is to be enforced. Fortunately, by implementing a proactive cybersecurity strategy that detects and responds to new threats and vulnerabilities as they arise, organizations can feel empowered and secure as they enhance their operations and scale their businesses with cloud technologies.

We will continue to see the impact on security from the shift to a remote workforce, in particular the concern surrounding data egress and USB control, saysTim Bandos, VP Cybersecurity at Digital Guardian:

While portable USB drives and devices are seen as a quick, convenient way to transport or store data by employees, they often present a major headache for security professionals.

According to new research, there has been a 123% increase in the volume of data downloaded to USB media by employees since the onset of COVID-19, suggesting many have used such devices to take large volumes of data home with them. As a result, there's hundreds of terabytes of potentially sensitive, unencrypted corporate data floating around at any given time, greatly increasing the risk of serious data loss.

As we've seen a significant increase in employees syncing this data locally now that they are working from home. It's critical to continue security awareness training and re-enforce company policies related to the proper handling of sensitive business information. Fortunately, implementing USB control and encryption solutions can greatly improve the tools at a security team's disposal to deal with such challenges and ensure both the network and sensitive company data remains protected at all times.

Now, that said it is people who are (and likely always will be) the biggest security risk. For that reason, employers should never underestimate the power of properly educating their people. Not only is it significantly cheaper than the latest CYBERSECURITY solution, but in the majority of scenarios it is also much more effective. Well trained, well informed employees can easily spot phishing or social engineering tactics and even identify insider threats, helping to stop attacks much faster than any technology solution can.

Looking more broadly, geopolitical relationships around the world have increasingly become strained and uncertain with direction and we will continue to see state-sponsored attacks being carried out much more. There have been a number of attempts and even successful attacks against these types of systems but for the most part they've all been isolated

incidents. One can only wonder though if these attacks were merely conducted to set up backdoor functionality for a future panic button push to cripple the target's systems. Not to mention the considerable adoption of IoT devices connecting once-segregated Operations Technology (OT) environments; which only further widens the attack landscape. The security in these environments need to be fully assessed and controls need to be put in place as soon as possible in order to mitigate against future attacks. It's only a matter of time.

The rapid onset of Covid-19 has by no doubt changed the world we work and live in, says Jay Ryerse, CISSP, VP Cybersecurity Initiatives at ConnectWise:

So much so, that many organisations who were skeptical of employees working remotely, have now successfully adapted and are now completely changing their ongoing procedures to include a remote working culture - in the new normal.

As many countries ease lockdowns, organisations are now in the process of returning to their office, however it clearly won't be the same as before, for example not being able to walk to your colleague or manager's desk to discuss ideas. Many of these organisations will need to consider how they can not only bring people back to a shared working environment safely, but also consider how they can continue to protect their organisation from potential cyber threats, while many employees will continue to work from home. Here are three things to consider:

Document the transition to remote working
It's important to firstly take a step back and understand what you've learnt from going into lockdown. Documenting the manner in which moving an office-based workforce to remote-based will be required for any future lockdowns that may occur from a second wave, and understanding what mistakes were made first time round, so they're not repeated.

Having this record is also crucial to uncovering potential cybersecurity vulnerabilities that may have left the organisation exposed. It's crucial to understand how these existing or new security vulnerabilities can be diminished. Organisations will need to ensure that they have strategies in place to manage cybersecurity, disaster recovery and backup, which can function no matter where the staff are located.

Prepare staff with security awareness training
Security awareness training is a must for organisations in this day and age, especially with employees working remotely, they are a vulnerable entry into your organisation's IT system, especially if they use their own devices which may not have the appropriate security tools in place. Online education is an easy-to-access resource that staff are able to undertake, no matter where they are. Organisations should be using this online training and investing time to educate employees on the best practices of IT such as not clicking on suspicious links, using 2FA and preventing cyber attacks from taking place.

Have an agile workforce

Moving the entire workforce overnight when lockdown happened was clearly no easy feat, so it's important to ensure your organisation has the capability and the right tools to quickly and securely make this happen when required. Embedding not just flexibility but cybersecurity into the tech infrastructure is a necessity. Before the pandemic, most organisations were not prepared for the mass home working situation that took place globally, however, if a second wave or a pandemic should ever take place again, then the majority will trust that organisations will be able to seamlessly adapt and continue meeting their customer needs.

While working in the new normal may be a challenging process, putting processes in place will allow organisations to reopen shared office spaces that's secure for employees and technology alike.

Moving the entire workforce overnight when lockdown happened was clearly no easy feat, so it's important to ensure your organisation has the capability and the right tools to quickly and securely make this happen when required. Embedding not just flexibility but cybersecurity into the tech infrastructure is a necessity

Angel
BUSINESS COMMUNICATIONS

WEBINARS

Specialists with 30 year+ pedigree and in-depth knowledge in these overlapping sectors:

Expertise: Moderators, Markets, 30 Years + Pedigree
Reach: Specialist vertical databases
Branding: Message delivery to high level influencers via various in house established magazines, web sites, events and social media

Semiconductor (Silicon/Compound)
Publications include: Compound Semiconductor, Silicon Semiconductor, CS China, SiS China

Power Electronics
Publications include: Power Electronics World

Future Mobility
Publications include: TaaS Technology, TaaS News

Data Centres
Publications include: DCS Europe, DCS UK, SNS International

SmartSolar UK & Ireland
Publications include: Solar and Power Management, Solar UK and Ireland

Sensors
Publications include: Sensor Solutions Magazine, Sensor Solutions International

Digitalisation
Publications include: Digitalisation World, Information Security Solutions, Managed Services

Photonics
Publications include: PIC Magazine, PIC Conference

Expert Moderators

Dedicated technical and time-served experts/editors

MARK ANDREWS
Mark Andrews is technical editor of Silicon Semiconductor, PIC Magazine, Solar+Power Management, and Power Electronics World. His experience focuses on RF and photonic solutions for infrastructure, mobile device, aerospace, aviation and defence industries

PHIL ALSOP
Journalist and editor in the business to business publishing sector for more than 30 years currently focusing on intelligent automation, DevOps, Big Data and analytics, alongside the IT staples of computing, networks and storage

JACKIE CANNON
Director of Solar/IC Publishing, with over 15 years experience of Solar, Silicon and Power Electronics, Jackie can help moderate your webinar, field questions and make the overal experience very professional

DR RICHARD STEVENSON
Dr Richard Stevenson is a seasoned science and technology journalist with valuable experience in industry and academia. For almost a decade, he has been the editor of Compound Semiconductor magazine, as well as the programme manager for the CS International Conference

For more information contact:

Jackie Cannon **T:** 01923 690205 **E:** jackie@angelwebinar.co.uk **W:** www.angelwebinar.co.uk
6 Bow Court, Burnsall Road, Coventry, CV5 6SP. UK
T: +44(0)2476 718 970 **E:** info@angelbc.com **W:** www.angelbc.com

Cybersecurity and the next normal

Over the following articles, we've gathered together a tremendous range and depth of opinion (and topics covered!), as industry experts offer their thoughts on cybersecurity into the future. Part 9.

The average enterprise has millions of vulnerabilities, states Stephen Roostan, VP EMEA at Kenna Security:

NO ORGANISATION, no matter how well resourced or efficient, can possibly fix them all. The good news is that no organisation really needs to. That's because not every vulnerability an organisation finds in its environment poses a risk to its own specific assets or business.

In most enterprises, fewer than 4% of vulnerabilities and weaknesses pose a legitimate risk. Typical vulnerability scanners and application assessment tools are useful for finding potential exposures, but spitting out a massive list that is hundreds of pages long is little help to an already time-strapped team. IT and development can't fix all of them, so which vulnerabilities should they address first? How will they know which flaws pose the greatest risk to your particular organisation? The truth is, without the right insights, they can't.

This is why risk-based vulnerability management (RBVM) is the future of cybersecurity. RBVM is changing rules of the game by making it easier for organisations to dramatically improve their security stance by reducing the relentless and constant pressure to monitor, track and fix vulnerabilities and protect the organisation from a potential cyberattack. By adopting a risk-based approach to vulnerability management organisations are able to identify – and remediate – the small subset of vulnerabilities that are most prone to exploitation by cyber attackers.
As digital methods and new ways of working continue to increase, vulnerability and threat management are quickly climbing up the enterprise agenda. Today's highly adaptive RBVM platforms make it possible for enterprises to apply meaningful metrics to evaluate their specific exposure to potential risk factors, sorting the 'wheat from the chaff' to rapidly prioritise remediation actions.

Utilising predictive data science modelling and real-time threat intelligence feeds, RBVM platforms enable security teams to gauge exactly how critical each threat is to the organisation's real-world specific environment. Unlike CVSS (Common Vulnerability Scoring System) tools that blanket-score high volumes of vulnerabilities as 'high risk', RBVM solutions provide the evidence-based guidance intelligence teams need to identify only those most critical vulnerabilities that represent a true risk to the enterprise stack.

The days of blindly, manually chasing vulnerabilities are over. The future of cybersecurity will be increasingly defined by meaningful prioritisation and

metrics business leaders can understand. What's more, a modern vulnerability management operation shaped by metrics will benefit business leaders in multiple ways including helping you become a more strategic and effective force in the C-Suite.

The technical skills gap in cybersecurity was well reported and many security teams were running lean before the pandemic, warns Richard Cassidy, Sr Director Security Strategy at Exabeam:

The impact of this cannot be overstated. When you add in the fact that many organisations will have deferred planned critical technology updates, the impact on security in the long run will be significant.
As we move through the pandemic and the most severe restrictions are lifted, organisations should prioritise reinvesting in their security teams. The 'new normal' we are beginning to craft will need a far greater focus on security and the already limited supply of security professionals tasked with ensuring this will need our full and comprehensive support - from ensuring they have the right tools, to approaching productivity, mental health, and collaboration and a more sophisticated way.

For years now, we have lived in an age of alert overload, with security, risk, compliance, and response teams overwhelmed by the data points they receive. All too often in the news, we see the result of critical alerts and events slipping through the defensive net. As we plan for a new normal, we need to consider how we can better support our security teams and automate as much of the more time intensive and mundane tasks as possible.

This will help security professionals better protect their organisations, and will help more junior analysts do more to support their team. But we also need to rethink security operations centre (SOC) practices - the attack surface is far greater now and IoT security is a bigger risk vector than ever before. Organisations need to cast their net of inspection far wider now.

The home office is the new corporate cubicle, and security teams will need to detect anomalies from home networks, users and devices - sources that are far easier to compromise, because they inherently lack security capabilities.

Security leaders need to make sure remote teams can work securely, applying best practice despite the unprecedented changes. On one hand, the security organisation needs to ensure remote employees remain vigilant and maintain sufficient cybersecurity awareness. However, security teams themselves will need to place more focus on email security and deploying threat intelligence solutions that can help identify new campaigns. The key to this is a foundation of behavioural analytics that can help detect attacks and automate incident response.

This frees up security teams enormously by using existing datasets to detect anomalies across the entire estate and monitor critical assets to find early signs of suspicious activity. When presented with the most critical information and with all of the necessary context, security teams can better respond, mitigate, and remediate the many threats they are faced with. We are all still adjusting to the 'new normal', however, taking the steps now to ensure your security teams are prepared and remote employees are clued-up for the changing cyberthreat landscape will be crucial in the coming months.

If there's one thing you can say for cybercriminals, they rarely miss an opportunity, says Andy Swift, Head of Offensive Security at Six Degrees:

The coronavirus pandemic has offered cybercriminals a myriad of opportunities to exploit victims' fears and uncertainties, sow seeds of false hope, and persistently cause disarray in the aid of compromising data and making money. I don't expect this to change as we transition towards a post-pandemic world.

Many organisations throughout the world are fighting to remain operational, and cybercriminals know this. They will continue to proactively target organisations that are struggling as a result of the coronavirus pandemic, as they recognise that budgets for IT and CYBERSECURITY resources may well have been reduced - making them easier targets for phishing and ransomware attacks.

Many of the coronavirus-related cyber-attacks we've seen to date have not progressed technically. It's the methods of infiltration that have – those earlier steps in the malware kill chain that entice victims and gain initial footholds. PHaaS and RaaS (phishing as a service and ransomware as a service) have both seen significant uptake throughout the coronavirus pandemic, and I believe this 'as a service' way of working will continue to rise.

Post-pandemic, I can see a lot of organisations realising the benefits of mobilising a remote workforce and transitioning to a more flexible, hybrid operational model. I expect to see a continued increase in the targeting of conferencing tools moving forward, both through continued phishing campaigns and exploits identified following more in-depth research in the area. My advice to anyone reading this is to keep CYBERSECURITY high on your agenda throughout the coronavirus pandemic and beyond; doing so will minimise your exposure to data breach and enhance your ability to remain efficient and operational.

Cybersecurity and the next normal

Over the following articles, we've gathered together a tremendous range and depth of opinion (and topics covered!), as industry experts offer their thoughts on cybersecurity into the future. Part 10.

BY JOHAN PELLICAAN, VP & MANAGING DIRECTOR AT SCALE COMPUTING EMEA, OFFERS SOME THOUGHTS ON BUSINESS RESILIENCE:

For many businesses around the world, the upheaval caused by COVID-19 has been nothing short of chaotic. Deploying a work-from-home strategy smoothly and securely, as well as the enormous spike in ransomware attacks during recent months, have been the root of concern among many business owners, governments, and schools. The focus for all organisations right now, and into the next normal, must be business resilience. A rethink of IT systems to ensure the distributed workforce can work securely and effectively – and that critical enterprise systems remain both protected and highly available – is important. This must include considering taking a deeper look into cybersecurity.

It was evident from the news cycle that cyber criminals were quick to take advantage of COVID-19. Organisations, governments, research establishments, healthcare agencies, and schools experienced a rapid uptick in ransomware attacks. According to Reuters, ransomware attacks jumped by 148% in March as online threat actors targeted vulnerable remote users. As a large number of companies discovered at their cost, utilising traditional VPN connections to enable remote workers opened up enterprise networks to cyber-attacks that entered through employee home networks. To eliminate this risk, IT leaders will need to deploy active protection tools across the entire extended network and initiate advanced built-in back-up, disaster recovery and cloud storage to enable fast and granular object-level recovery in the event of an attack.

The recent emergence of edge computing in combination with hyperconverged infrastructure (HCI) has made VDI a highly practical option for IT teams that need to be confident they can both enable a large number of users to work remotely at the drop of a hat, and do so securely. As many organisations discovered, these solutions make it possible to set up a remote user in under an hour, but moreover today's modern VDI solutions can simplify how IT teams are able to maintain the security stance of the extended enterprise.

Using multifactor authentication to give users access to their email, files and applications, IT teams can remotely monitor user profiles, log users out and receive automated alerts on potentially suspicious activities. Plus, sensitive data always stays within the corporate network as it is never exposed to employees' private networks through a VPN connection. Similarly, these solutions make BYOD strategies that eliminate any need to deploy IT to home-based employees a risk-free option. Users can securely connect to their personalised desktop using any device they choose.

While it may feel we are still in the midst of the chaos, and perhaps irrelevant or even a waste of time to think longer term about business resilience, failing to plan is planning to fail. The potential for many organisations to keep a vast majority of their workforce working remotely, even as we begin to come out of the other side of COVID-19, is high. The savings on the cost

of an office space and for employees commuting (amongst others) are making remote work long-term ever more attractive to employers. This means it would be wise for organisations to consider investing in solutions and processes that are simple to implement, manage, and maintain remotely. Solutions that have built-in backup and DR will allow users to work remotely, safely, and securely – and provide protection from ransomware – are becoming increasingly important in the new and uncertain times we are living through.

During the first week of April 2020, Google reported it had blocked more than 18 million COVID-19 related phishing emails every single day, says Gijsbert Janssen Van Doorn, Director Technical Marketing at Zerto:

Ransomware has long been the tool of choice for cyber criminals, so it is hardly surprising they are taking advantage of the pandemic to execute attacks. Many organisations, especially those in healthcare or public sector, face enormous pressures to keep systems up and running. The likelihood of a payout increases with the urgency of the need for patient/ customer data to be secure.

Ransomware attacks are not a new phenomenon and they aren't uncommon; they will continue to be prevalent long after this global pandemic. But one thing many businesses have become more aware of over the pandemic, is the importance of a modernised data protection strategy to safeguard their valuable and sensitive data. And they are not wrong – for an unprepared organisation, just a single employee clicking a malicious link in their emails could mean paying a ransom is the only way the business can recover encrypted data - and this is far from guaranteed.

Cyber criminals often exploit vulnerabilities in employee emails, so it is crucial to have the right cyber defences in place to avoid a disaster where critical data could be at risk – especially when it comes to government or healthcare organisations. Having appropriate role-based access controls and an extensive tiered security model will help minimise this risk. But, the attack itself is only half of the problem - without sufficient recovery tools, the resulting outage will cause loss of data, as well as financial and reputational damage.

Over the coming months, it is important that we see more organisations utilising tools that allow them to roll back and recover all of their systems to a point in time just before an attack. This level of IT resilience will prove to be paramount. Email will undoubtedly continue to exist at the core of most organisations - but this remains a standing target for ever-sophisticated cyber criminals, whether in the middle of a pandemic, or not.

Beyond this, and taking a broader look ahead to the future of cyber resilience for businesses, cyber resilience is about maintaining security as you grow. With operations shifting to accommodate the 'new normal' we will inevitably start to see business pick up across the board. As your business evolves, so does your need for data protection. This requires a more robust, enterprise-class infrastructure complete with storage, compute, networking and other services like security. It's often the case that only the largest of companies can afford to keep this kind of infrastructure in-house, as the cost gets simply unmanageable, let alone the footprint.

With a disaster recovery as a service (DRaaS) provider, you're leveraging their infrastructure and services, providing the benefits of scale, but without the normal cost. Additionally, this removes the cost of keeping a DR environment going 24/7, just in case it's needed. The majority of DRaaS vendors utilise OpEx-based cloud billing, giving your IT team valuable time to focus on more strategic, business-benefiting initiatives.

Cyber resilience has never been more vital amidst the turbulent pandemic environment, but the truth is that it always was and always will be an absolutely critical factor in the success of any business. This will remain the case far beyond the unprecedented upheaval businesses are facing now."

Ransomware attacks are not a new phenomenon and they aren't uncommon; they will continue to be prevalent long after this global pandemic. But one thing many businesses have become more aware of over the pandemic, is the importance of a modernised data protection strategy to safeguard their valuable and sensitive data

Will lockdown necessity change our cultural perception of remote working?

The world we live in is currently undergoing a seismic change. Previous patterns of working and living have been forcibly modified. One of the most foundational of these movements are the instructions to stay at home, which are in place for many countries across the world: employees, no matter their industry or profession, have had to come to grips with working from home for long periods of time.

BY MIKE KISER, SENIOR IDENTITY STRATEGIST, SAILPOINT.

THE CONCEPT of working from home is not a novel. With the adoption of mobile devices and the increase in broadband availability both in private and public areas, a small segment of the workforce had already adopted this model. However, it was a secondary option, and its cultural impact was limited.

The spectrum of work has now shifted. Directives to work from home if possible have forced a global workforce to adapt to the home office. What had been an alternative mode of work has now become the primary – all within a few short months, if not weeks. Remote work is one of the biggest trends of 2020, and it is likely here to stay. Once a new norm arrives, innovation and investment can create entirely new industries, and the forced adoption of this new mode of work will force a similar shift. With the realisation that a different way of working doesn't have to mean a dip in productivity, comes for many a change in perspective on what is required to advance in a way that is 'normal' or 'optimal'.

In the wake of this transformation, the cultural impact of this shift awaits. In short order, can we expect remote working to become associated with health, power, and affluence – at least in sectors where it is a practical option?

Certainly, from a business perspective, the value of this new way of working is already evident, particularly for organisations that have already developed the infrastructure to accommodate a pattern of remote work. This does not just mean an installation of IT services such as a VPN, but also requires reconsideration of the established security mindset. While many of them may not have the scale to handle a complete and immediate transition to home-based employees, their transition to this brave new world will be smoother due to their pre-emptive investment in a revised security strategy.

This new approach to securing resources deemphasises perimeter defence and elevates the role of identity. Various systems and names have been introduced (or reintroduced) to facilitate the practical development of these systems; zero trust and CARTA are a few strategies among many that attempt to translate this vision into a practical reality.

Businesses that have already begun this shift are likely to be less impacted by the maelstrom of change; while none welcome this new reality, organisations well-equipped for this new cultural value will be healthier in both the short and long term. Fewer disruptions in their business and continuity in their economic model will mean that they have a stronger chance of not just surviving, but thriving as the crisis transitions into a different, hopefully milder, phase.

Even organisations with a solid security strategy, however, are subject to market forces. It is possible that the new dominance of remote work will alter the

landscape of enterprise. Just as the rapid proliferation of the internet drove some organisations into the stratosphere and left others behind to languish in the "brick and mortar" mindset (the easiest example of this dichotomy is Amazon and local booksellers), working from home at this sort of scale has the potential to divide enterprises into winners and losers. As a result, remote work may become semantically linked with health and with power – or their business-speak equivalents "profitable" and "innovative".

But the more profound potential for the cultural impact of working from home centres around individuals. In just a few short weeks, lockdown has shone a bright light on existing inequalities that are all-too-easily ignored.

The pandemic is revealing a caste system, one of whose demarcation lines is the ability to work from home. This flexibility is primarily dictated by both the availability of reliable broadband access and the specific occupation in question.

Rural residents with limited network access, or those in specific sectors: the service industry, shipping and transport, food distributors, and government officials often have no viable option to work from a remote location – to say nothing of the healthcare workers who find themselves thrust to the front line of the pandemic.

For others, the ability to continue to work while staying home confers a wide range of benefits. The first is obvious: steady employment. With unemployment rapidly escalating, the pandemic is already having an effect on economies worldwide. If working from home means retaining a job, this primary benefit lays the foundation for the others that follow. The second advantage lent by remote work may be a bit more hidden: continued education for their children. Schools in 130 countries have closed, disrupting the learning of over 1.2 billion students.

The same reliable network access which allows them to continue working also provides for the continued education of their children and puts those pupils at an advantage to their peers. Finally, the most striking benefit that working from home while in lockdown bestows is a better health outcome. If the point of stay at home orders is to prevent interaction with outsiders, preventing the spread of COVID-19, then by complying with these guidelines and working from their homes ensures that those individuals and their family are less likely to fall ill.

These are not minor benefits: affluence, education, and health. And if the pandemic and working from home are revealing an existing caste system, it is also reinforcing it. Those with the ability to work from home are finding their wealth protected, their children keeping pace academically, and their expected health outcomes confirmed.

After only a few short weeks of lockdown, both businesses and individuals are already associating a work from home model and increased health, power, and influence. After a long period in relative obscurity, benefits and requirements of remote working have been brought to the fore. As the quarantine continues, that connection will only strengthen. COVID-19 has transformed remote work from a relatively unused mode of employment to the only viable option, and the benefits that that model currently conveys will ensure its association as not just a possibility, but as a preferred way to work for many.

Security considerations for remote workers, courtesy of Pete Watson, CEO of Atlas Cloud:
Remote working is here to stay and, having adopted this way of working, has made many workers reluctant to leave their home offices. Technology is going to be an important part of this new normal as it will be held accountable for the shift in permanent home working. In order to move forward, businesses should learn from the past and apply this new learning into future solutions.

With systems under more pressure than ever as they are performing tasks out of the office, companies must consider what security tools they have in place to keep both their people and sensitive data safe from cyber threats. IT and network managers are facing new challenges and in order to overcome these they will need to find ways to implement effective security solutions. This also includes protecting hardware from security threats whilst left unattended and enabling solutions to BYOD approaches. In order to stay on top, businesses should be proactive in their approach with cybersecurity and act quickly.

So, how prepared are homeworkers for cybersecurity threats? In our recent study, 26.5% of employees have used self-service guidance level of training and support on the cybersecurity risks associated with home working as opposed to 10.15% who have received comprehensive training and support. Without educating workers on cybersecurity, companies could face a number of significant risks. Organisations are placing a large amount of trust on their employees to make sure they are working safely and efficiently and, in many cases are relying on them to have anti-virus software installed on their devices to protect their networks and files from being compromised. In fact, only 35.4% have updated antivirus software, and worryingly 20% of home workers have done nothing to mitigate potential cybersecurity threats. Overall, businesses should take more responsibility in educating their staff in order to safeguard them and also their sensitive data.

Moving to cloud-based security solutions to support remote working

The time to review cybersecurity is now. Here are some solutions to implement in your business to be in control of security. Cloud-connected solutions can eliminate many of today's remote working security concerns. Hosted technologies are on an upward trajectory and are being used as a vehicle for secure flexibility. With data always held in one off-site secure hosted environment, security is maximised as data is never downloaded to an individual device, therefore reducing any risks.

Adopting a standard cloud solution like Hosted Desktops can keep your business safe. Even when you adopt a BYOD policy, your data is protected within the perimeter of the server and no data is stored on devices. You, therefore, don't need to rely on the security of the user's device and all security patching and updates can be controlled centrally and applied to all users simultaneously.

Solutions such as Citrix Workspace can also support users in putting security first, by securing files, desktops and even SaaS applications through two-factor authentication, sophisticated access controls and disaster recovery for optimal data protection. This allows for centralised monitoring and control of all user interactions. When it comes to securing email, investing in software such as Mimecast can vastly reduce the number of malicious emails making it to inboxes. Providing threat awareness training to employees is also an essential step.

Some cloud-based collaboration tools can also offer another layer of security by design. For example, Microsoft Teams offers a unified set of tools that comes as part of the Microsoft 365 suite (formally Office 365), which not only allow for collaboration on documents but prevent siloed data for enterprise-level security.

With systems under more pressure than ever as they are performing tasks out of the office, companies must consider what security tools they have in place to keep both their people and sensitive data safe from cyber threats

INNOVISION2020
DATA CENTRE INSIGHTS + PERSPECTIVES

InnoVision: A very special issue of DCS Magazine dedicated to the data centre industry's visionary leaders and technology innovators

To herald the launch of the all-new Data Centre Solutions digital publication, we have produced a very special first issue, entitled InnoVision – providing an overview of the state of the data centre industry right now.

80+ Vendors from across the supply chain have provided their viewpoint on the future and innovation.

How will the data centre industry evolve over the coming months and years, what will be the major drivers and opportunities?

Read today

https://digitalisationworld.com/magazines

IN ASSOCIATION WITH

DATACENTRE SOLUTIONS

DIGITALISATION WORLD

Online, but not insecure:

Securing the remote workforce

Some thoughts from Mark Weir, Director of CYBERSECURITY at Cisco UK & Ireland.

THE OFFICE IS NO MORE. For now at least. Many of us are now working from home, and in the battle to maintain business continuity in these circumstances, collaboration tools have become a lifeline. But with staff dispersed, and accessing sensitive company data remotely, security has become an even bigger challenge than usual.

Malicious individuals are taking advantage, focusing even more on phishing attempts and interfering with video conferencing. While quick workarounds like sharing passwords and making files public might feel harmless, it's important to not trade-off security in favour of convenience. The last thing businesses need is a data theft or breach.

This pressure can seem relentless. But there's a great deal of guidance and support available which will remain useful after things return to normal.

More than just one password

Security around granting remote access is a good place to start. IT teams should consider implementing multi-factor authentication for all users– meaning identity must be confirmed using a second device before access is given. This can help prevent against network snooping and data theft.

As entire workforces connect to VPNs, network monitoring is even more important. Security tools can help in alert to suspicious or unusual activity. Many vendors are helping, and Cisco is playing its part – we've added more than 15.3 million users of our security products since free support started in March.

Racing to address remote working needs can be tempting, but things like remote access, if not adequately secured, can be a huge open door to entire internal networks and confidential file systems.

Take stock of users and devices

The influx of new devices accessing corporate networks makes keeping tabs on those devices more important. This can help shed light on how widespread personal device usage is, as well as any possible threats involved. Physical entry points to sensitive company data and networks, through offices and data centres shouldn't be forgotten. Some malicious actors aren't afraid to cause trouble in the real world, and unauthorised access could have serious.

Emergency preparedness

With situations changing so quickly, quick contact is key. An up-to-date accessible phone tree or contact list is a must.

IT leaders can do a lot from their senior positions, but employees also have an important role to play. They're on the front lines, and susceptible to direct contact and influence that IT might not hear about until it's too late. They should remain critical and vigilant of any communications.

Data hygiene

Employees should also keep their devices and software up-to-date, applying patches when requested. Keeping work activity on authorised devices also helps reduce possible entry points and the amount of data spread. When it comes to video conferencing, employees should also take care to not re-use meeting codes and set passwords. Stay aware of what is being displayed when screen sharing – information can inadvertently be on display.

Legions of workers are now working completely online. Businesses are doing all they can to maintain their operations and service customers. In this scramble, security can't afford to take a back seat. Whether it's smarter use of monitoring tools, or encouraging a more security-conscious workforce, there's a lot businesses can do. Offices might be closed, but threat actors never rest. By making use of available tools, and encouraging employees to play their vital role, businesses can reduce the risk of cyber attackers. Now is the perfect time to secure that remote workforce.

The increase in cyber-threats during the COVID-19 crisis, as well as the adoption of remote working as a standard, as par to the new normal organisations are likely to implement changes from a cybersecurity perspective. What can we expect? Asks* Simon Eyre, *Director, Drawbridge.

Investment in secure remote working tools

The coronavirus pandemic necessitated a rise in remote working, as companies sought to protect their employees, customers, and partners from the virus. However, while many companies are planning for a return to the office, this is unlikely to look the same as before the pandemic. COVID-19 has shown many business leaders that remote working does not necessarily mean a decline in productivity and comes with its own benefits. As experts are predicting that remote working is here to stay, even if it is a few days of the week – this comes with cybersecurity challenges. As part of the new normal, we can expect organisations to invest in secure remote work tools and emphasis on multi-factor authentication.

Strengthening cybersecurity training and awareness programs for employees

With a large percentage of employees working remotely, cybersecurity training will become an even greater priority. We can expect organizations to bolster their cybersecurity awareness programs to ensure that employees understand the nature of cybersecurity risks, how they threaten the company's security, and what steps they should take in the case they encounter a threat. In the new normal for the remote workplace, cybersecurity should be more than ticking an annual checkbox - training should be done regularly, so employees are aware of the latest cyberthreats.

Bolster ransomware protection and continuous vulnerability management programs

Remote working can increase the risk of a successful ransomware attack significantly. One example of this was the increase in COVID-19 related ransomware attacks during the height of the pandemic. To protect valuable data, organizations should invest in increased ransomware protection and continuous vulnerability management. As part of the new normal, organizations will strengthen their vulnerability management programs and seek patch weaknesses before hackers exploit them.

From a technology and business perspective, senior management must understand the importance of protecting the business from cyber criminals, to protect critical information assets, keep the business operating and protect its reputation as a safe partner to do business with

More cyber-committed CEOs and senior leadership

With the rise in cyberthreats, cybersecurity has become every leader's job – it is no longer only the concern of the IT team, or the third-party security provider. From a technology and business perspective, senior management must understand the importance of protecting the business from cyber criminals, to protect critical information assets, keep the business operating and protect its reputation as a safe partner to do business with. Beyond understanding the issue, as part of the new normal, senior leaders will seek to effectively address the cyberthreat through series of structural and organizational changes.

Third-party due diligence as a necessity

Even with a comprehensive, robust security program, an organization's defenses are only as secure as the weakest third party with access to their data. This is why it's important to understand the company's cyber and confidential data risk both inside and outside of the organization's walls and ensure third parties and their cybersecurity practices meet the organization's and industry standards. While we can already see this happening, the new normal means that the oversight of third parties who have access to sensitive data is not only best practice but is expected by regulators, business partners and customers.

Over the last six months, as the COVID-19 pandemic swept across the world, IT departments worked 24/7 to ensure critical business continuity. Quickly and securely they had to enable a remote workforce, as well as ensuring their organisation could conduct business with customers securely online. Xavier Coemelck, EMEA VP, Entrust Datacard, writes:

As we settle into a new normal, the world of work looks like it will be changed forever. In a recent Entrust Datacard customer survey, 84% of respondents said they expect the recent shift to a more significant remote workforce to be a permanent change.

A remote workforce makes the perimeter security concept more dated than ever and adds to the challenge of securing employee identities. During the pandemic, we saw that phishing continues to be the 'attack of choice' because it's very effective. For IT departments to quickly and securely onboard remote workers en masse, it came down to authentication - verifying the identity of remote workers anytime, anywhere, from any device.

Not surprisingly, workforce authentication has now become a top priority for IT leaders, which also means it now has C-level visibility and support. The risk of getting authentication wrong is huge because the vast majority of today's breaches are due to compromised credentials. As the threat landscape continues to intensify, employee passwords, especially in less secure home environments, are likely to be the single largest vulnerability.

Accelerating the shift to passwordless authentication It's way past the accepted time to do away with passwords, but a passwordless experience is not the same as passwordless authentication. Simply replacing the password with another authenticator like FaceID on a smart phone still means a single point of exposure. Credential-based passwordless authentication, on the other hand, provisions a digital certificate onto the worker's mobile device, which is then unlocked by the phone's biometrics, transforming it into their trusted workplace identity – regardless of physical location.

A credential-based passwordless solution provides both a friction-free passwordless user experience and secure passwordless user authentication. We expect to see an accelerated shift to passwordless authentication, as home working or a hybrid of home/office/anywhere working becomes the new norm.

Moving towards a touchless enterprise

With COVID-19, we have also learned that people are, for very good reasons, reluctant to 'touch' or perform tasks with their fingers - especially where this could be done without any contact.

The spike in usage of contactless payment cards is well known, but this same trend is now extending to accessing buildings or accounts on computers or other devices. Typing a User ID and password on a keyboard requires frequent cleaning to respect the new hygiene rules. By allowing us to unlock our devices, accounts or access to buildings just by having a phone in our pocket means the smartphone becomes the new smartcard - using the Bluetooth capability you can login to your computer account without typing anything. What a revolution indeed.

AIOPS SOLUTIONS ONLINE SUMMIT

ENABLING APPLICATION OPTIMISATION

The importance of proactive performance monitoring and analysis in an increasingly complex IT landscape.

29 October 2020

aiopssolutions.com

The four security pillars of a remote working world

BY DANIEL HUREL, VICE PRESIDENT WESTCON EMEA – CYBERSECURITY & NEXT GENERATION SOLUTIONS.

WITH BUSINESSES WORLDWIDE turning to remote working as a long-term solution, employees are forced to connect to external networks and use unmanaged devices. Many companies have faced increased vulnerability as this process has created additional attack points and have realised the need to undergo further digital transformation to support this. However, with cyber attacks on the rise, companies need to find a solution that facilitates the transition safely.

With the rapid adoption of cloud apps, services and mobile devices and the introduction of increasingly complex network systems, the attack surface is increasing. Furthermore, the nature of working and collaborating remotely - where there is a heightened volume of shared data - makes it difficult to keep information safe.

These factors accumulate to create vulnerability, with multiple potential attack vectors. Companies maneuvering towards long-term remote working need to remain secure without affecting business performance. To combat this challenge, there are four key solution pillars that companies must consider: Zero Trust Access, Next Generation SOC, Cloud Security and IoT security.

Zero trust access

Zero Trust Access dictates that security measures should 'never trust, always verify' and keep assets and data safe wherever they live. Never trust users, even if they have been previously given access or are already inside in the network perimeter. It is also important to remember that even trusted users could be compromised when they connect to infected websites, so isolating their web browser traffic in a next-generation secure web gateway will avoid any malicious code hitting their system, drastically improving an organisation's exposure.

Next generation SOC

It's crucial for organisations to have detection and response capabilities to detect attacks and breaches early. This can be provided by an internal or external Security Operations Centre (SOC) where a team of security analysts will use advanced monitoring, detection and response tools augmented by AI and machine learning to reduce noise and detect meaningful security alerts. This automated approach

is crucial in the face of exploding threat volumes and sophistication.

Cloud security

As the usage of cloud applications accelerates, securing the cloud is becoming an important part of security strategy. Unsanctioned SaaS applications can cause accidental data exposure, malware propagation and compliance issues, while configuration errors in public cloud infrastructure have been responsible for significant data breaches. Cloud workloads running in containers or serverless environments can be misused by crypto miners or used to compromise other systems if not sufficiently protected. A cloud delivered security solution that provides visibility, granular control and enforcement is crucial to mitigate these risks.

IoT security

A new attack vector that is on the rise is the exploitation of IoT devices both at home and in corporate environments. Considering that many IoT devices are manufactured without proper security measures, every IoT device becomes a potential entry point for malicious hackers. It is crucial for CYBERSECURITY teams to have visibility on their IoT device estate and monitor the behavior of those systems to block malicious communication in the corporate firewall or isolate them from the company network.

To keep companies, employees and data safe, security teams must address all four solution pillars. Particularly in this new era of remote working, security teams are facing constantly evolving threats, but by utilising a consistent and modern approach organisations can manage and prevent future attacks.

The impact that global crises have on the security policies of the future
By Paul Anderson, Regional Director UK & I at Fortinet.

The shift to remote work has taken place almost overnight for many companies, forcing business leaders to make quick-fix decisions in order to secure the widely distributed workforce. But as lockdown measures begin to lift, the world is entering a volatile and unstable new phase. Scientists are increasingly confident that the COVID-19 pandemic threat will persist, possibly for years, which begs the question: is remote working here to stay? And if so, how must organisations adapt and structure their CYBERSECURITY strategy in a post-crisis world?

Empowering employees to defend against cybercrime

Some of the security needs of a remote workforce are relatively obvious, but businesses also need to understand the impact of losing the physical security of the normal office environment. Controls no longer exist for accessing the building or logging onto a specific computer, and the new 'hyper-agile' business model makes it much more difficult for IT teams to implement controls. The rise in COVID-19 related phishing attacks serves as a reminder that any organisation is only as secure as the most vulnerable device or user in the network, and yet many of today's remote workers are novices. For business administrators and employees who typically conduct daily business affairs in-office, the security requirements of working from home are something very new. Remote work tools, such as conferencing platforms, generally put access to your internal network into the hands of users and devices that may not stand up to your security standards.

For this reason, organisations must devise a plan for delivering online training to those users who need to learn how to access systems remotely and securely. Some cybersecurity vendors have responded to this demand, offering free online training programmes to help bring remote workers up to speed on essential security topics, such as how to identify malicious websites or ways to prevent phishing attacks. Training these users to recognise red flags will not only protect the widely distributed network now, it will also serve as a wise investment for the future security of the business.

The right tool for the job

As we settle into remote working for the long haul, many organisations are still facing severe issues with performance and reliability. The challenges lie in the limitations of many home networks: reduced bandwidth can make it difficult for these networks to support a wide variety of devices and technologies at the same time, whilst maintaining optimum performance. In these circumstances, it's important that organisations deploy solutions that are optimised for any number of different environments.

In fact, there are several different remote working scenarios designed to meet a range of requirements:
· Basic teleworker: This group represents most of the remote workforce. The basic teleworker only requires access to email, internet, teleconferencing, limited file sharing, and function-specific capabilities (finance, human resources, etc.) from their remote work site. This is equivalent to an employee working from their hotel while traveling or otherwise away from the office.

- **Power user:** Power users are employees that require a higher level of access to corporate resources while working from a remote location. This may include the need to operate in multiple, parallel IT environments, such as system administrators, IT support technicians, and emergency personnel. One option for power users is to extend the network's access layer to them through a VPN connected wireless access point.
- **Super user:** A super user is an employee that requires advanced access to confidential corporate

resources, even when working from an alternate office such as their home. This includes administrators with privileged system access, support technicians, key partners aligned to the continuity plan, emergency personnel, and executive management. Making a super user's location a direct extension of the network by placing the appropriate networking and security devices at their location will replicate their normal office set up.

Securing the intangible

Most businesses are fairly advanced in their adoption and transition to the cloud and software-as-a-service (SaaS) apps. Even when an enterprise hasn't yet directly embraced SaaS, users are self-selecting cloud-based applications – or what's commonly called shadow IT – to get their jobs done. With the shift to remote working, the reliance on SaaS and its universal access will only grow. For example, it's easy to appreciate the value that file sharing and cloud storage applications like Sharepoint, G-Drive, or Box deliver. Even if the corporate network and local folders are unavailable, cloud applications make it easy to upload and share files. And this can easily be extended beyond employees, to partners or suppliers, or even end customers.

Deep visibility and control mechanisms must be put in place to address potential SaaS security risks, such as the unauthorised downloading of files or creation of shadow IT resources. A Cloud Access Security Broker (CASB) provides critical technology designed to secure these cloud-based applications and assets, allowing customers to understand their SaaS traffic, protect corporate data and guard against threats. Depending on the deployment, CASB can even provide real-time visibility into unsanctioned application traffic, so that IT teams can act immediately and shore up potential risk points.

Cyber-profiteering in action

Significant social events are usually a catalyst for new threats to emerge – there are always evil players looking to exploit others during times of crisis, and the current situation is no different. An unprecedented number of unprotected users and devices are now connecting remotely via the home network, which creates a perfect storm of opportunity for cybercriminals. As a result, the FortiGuard Labs team is seeing an average of about 600 new phishing campaigns per day. These phishing attacks range from scams related to helping individuals deposit their stimulus checks, to providing access to limited medical supplies, and helpdesk support for new remote workers.

The future is unknown, but the threat landscape will continue to evolve. Organisations need to keep the unpredictability of global crises top-of-mind when developing security strategies, to ensure they are sufficient to protect a distributed remote workforce. Business leaders must prepare for a permanent shift to remote work by building security policies that will stand the test of time. Remote working should be seen as a catalyst for evolutionary change, and by focusing on long-term security measures, organisations can build resiliency and lay the foundations for people and architectures of the future.

Significant social events are usually a catalyst for new threats to emerge – there are always evil players looking to exploit others during times of crisis, and the current situation is no different. An unprecedented number of unprotected users and devices are now connecting remotely via the home network, which creates a perfect storm of opportunity for cybercriminals

DIGITAL CHANGE MANAGEMENT SUMMIT

25.11 2020

www.dcmsummit.com

How Managed Service Providers and Cloud Service Providers can help SMEs on the road to digital transformation

A unique online event to connect MSPs, VARs and System Integrators with their target market

If Zero Trust is the future of cybersecurity, how do we implement it?

No cybersecurity framework has seen more impact, applicability and wide scale adoption than Forrester's Zero Trust Framework.

BY DAVE KLEIN, SENIOR DIRECTOR OF CYBERSECURITY ENGINEERING, GUARDICORE.

THE ANALYST FIRM makes it clear that investing more resources to shore up perimeter defenses will not prevent determined cyber actors from circumventing or breaching those defenses to wreak havoc. Forrrester stipulates that in order to build secure IT environments, we need to go about security in a fundamentally different way. The new model they propose, the 'Zero Trust Framework', assumes that no user, device or application, whether outside or inside the network, can be deemed safe, and that each must be validated before being allowed access to network assets. (See also: https://www.guardicore.com/zero-trust-security/).

The number one question on the mind of those considering adopting a Zero Trust framework is how to best implement it. The good news is that you can break down the implementation of Zero Trust into an initial strategy and five sequential steps. In doing so you can operationalise its tenants to come up with a simplified, digestible and prioritised methodology to gain more visibility, control, security and risk reduction across your network.

Initial Strategy

Today's business demands IT departments bring measurable competitive advantages through accelerated delivery, efficiencies and savings. IT has delivered by adopting a DevOps and Cloud model in which IT is better able to overcome challenges and deliver to those demands. By applying DevOps and Cloud to cybersecurity solutions we can more easily adopt Zero Trust.

- **Solutions must work agnostically and comprehensively across all environments**
  Most enterprises are dealing with complex, heterogeneous environments. These environments include everything from legacy operating systems and platforms, to modern virtualized machines, clouds, containers and serverless applications. In other aspects of IT, enterprises have found solutions that simplify things by working across these platforms seamlessly. By finding solutions that work agnostically across all of these environments things are done in a more cohesive, accelerated unified fashion and fewer resources are required.

For example, in identifying your critical workloads within your environment, visibility should not be disparate for individual platforms and silos. Rather, it should be agnostic, decoupled from the underlying operating systems and platforms in a single, unified manner. Same is true for finding methods of enforcement; having the ability to establish micropermeters in a similar unified/ uniform matter, replacing disparate, multiple methods makes great sense.

- **Solutions that can take advantage of dynamic and automated playbook capabilities**
  Just as it has benefited from automated provisioning through the use of playbook capabilities, having these for use in cybersecurity also helps to automate what would otherwise be manual and arduous.

Five Sequential Steps to a Zero Trust Network

1. Identify Sensitive Data and Assets
Step one in implementing Zero Trust is establishing visibility into your enterprise that helps you to identify sensitive data and assets. To do this successfully you'll want to incorporate data from various things including existing configuration management databases (CMDBs), meta data provided from your various platforms and cloud providers. Beyond the technical input you will also need to get input from your enterprise business leaders as well.

2. Map the Flows of Your Sensitive Data
Going way beyond traditional perimeter security with rudimentary policies by port and IP address, Zero Trust is based on granular, more concise policies. Therefore, the next critical step is taking the data from above and mapping out the workflows that include critical details like associated users, fully qualified domains and processes involved in these workflows.

3. Architect Your Zero Trust Micro-perimeters
Now that we have gained visibility and mapped out the workflows, we can begin to segment these compliance-critical workflows easily at a granular level by implementing policies around them. Usually you start by applying policies and micro-perimeters by prioritizing what matters most and then working your way through your enterprise.

4. Continuously Monitor your Zero Trust Ecosystem with Security Analytics
Once Micro-perimeters are established, it is necessary to monitor your environment and assess how well they perform. One of the inherent benefits of micro-perimeters is that you gain a lot of intel on breach attempts. You can use these valuable insights to fine tune your policies.

5. Embrace Security Automation and Orchestration
By far the greatest time saver is being able to take the above work and find ways to utilize playbooks like Chef, Puppet, Ansible and other techniques to automate further. This means as new workloads come online, the whole process becomes automated. This ensures that you will remain secure and that the effort will be with minimal manual moves, adds changes and deletes.

Zero Trust framework has brought us an easy to implement, prescriptive method to streamline the process of shoring up security within enterprise networks. By utilising a DevOps and cloud model and the five sequential steps we can truly reduce risk in a much easier fashion than we have in the past.
For a deeper dive, download the Guardicore white paper co-authored by Dave Klein: "Zero Trust: What it means and how to get there faster."

About Dave Klein: Dave Klein is senior director of cybersecurity engineering at Guardicore. He has over 20 years of experience designing and implementing security solutions across very large data centre and cloud environments, mostly in the US, UK and Europe. Before Guardicore, Dave spent ten years as a contractor working with various US Government agencies including: US DoD, Civilian Agencies, US Senate and Executive Office of the President.

Francois Rodriguez, Chief Growth Officer of Adeya, offers the following thoughts on the cybersecurity landscape and zero trust in particular:

Enterprise and Emerging Risk Responses: Educate executive leaders on the fast moving and more complex emerging risks will empower them to answer questions from stakeholders

Risk Management Process: Help executive leaders understand the risk management process and the role of all executives in that process and how it can be optimized to deliver more value at a lower cost, given the interconnectivity between risks

Is zero trust the answer?

Yes, the adoption of zero-trust tactics is the way forward for all enterprises.

In general, businesses are moving towards this security model. The zero-trust concept suggests that users should behave with zero trust when using any endpoint device - especially in the era of BYOD (Bring Your Own Device).

Individuals have to assume that their device might be infected, vulnerable, or insecure. Further to this, users are leveraging their home networks, which must always be considered to be insecure and unsafe. The

reason is that most people have weak passwords or use shared distributed connections, and now, IP providers are moving into a shared connective environment - these situations highlight the increasing number of possibilities for data breaches and hacks (endpoints to hack, networks to hack).

As an immediate step, when adopting zero-trust principles, enterprises must assess the widespread security threats that could negatively affect their employees and customers. Attacks such as ransomware and phishing require implementing a strategic continuous adaptive risk and trust assessment approach.

Such a plan includes the following tactics:

Understanding Application in Control:
A system administration console ensures application permissions and controlled access.

Data security in transit and hosting procedures:
Where you host your applications, and by extension, your data, has a dramatic impact on how secure you are. Encryption secures data in transit, enabling user connectivity through any network.

Controlled Identity:
access to organization tools, infrastructures, and employee's Identity.

Devices Access: Users might pose threats, but devices are their way in.

In today's world, cyber terrorists are always looking for ways to exploit ineffective security procedures, often exposing vulnerable human behaviors. Security and risk management leaders must define strategies and deploy effective tactics to perpetually evolve their security awareness training programs to mitigate people-centric threats. Zero trust is the only way to do this.

What does the future hold for cybersecurity - the technology, the compliance and the education needed? Is zero trust the answer?

Peter Yapp, Partner at security specialist law firm Schillings, offers the following observations:

With any security policy now and in the future, leaders need to remember the fundamentals of what they are trying to achieve. Everyone wants their business to do well and be successful, and that means protecting data, while keeping business critical systems up and running efficiently. Already today, we're putting a focus on security – and have seen new compliance laws in relation to that. Requiring compliance with regulation is just one way of trying to force the market to adopt minimum acceptable standards. But this is just that – the minimum – and every business leader needs to aim higher than that level.

In the current climate, data and CYBERSECURITY are imperative for any organisation, so rather than ticking a box when it comes to meeting standards for them, instead, wider business strategies should be formed around them.

They must, from hereon in, be a point of discussion in every new development, whether a new investment, acquisition, product launch or even change of working practice.

Hopefully in the future, all organisations will bake the basics of CYBERSECURITY into the very fibre of the organisation. But this will not come about through technology alone; it will require an investment in people; ensuring there are enough suitably trained individuals to carry out all of the necessary processes to guarantee a sufficient level of CYBERSECURITY. And it will also need all of the workforce to receive an education on CYBERSECURITY, making them aware enough to report anomalies. They should feel reassured that they will be thanked for flagging any security risks or mishaps – too often we see staff hiding incidents from IT, as they're worried they'll be punished for doing something wrong.

Assuming all of this is in place, that your own house is in order and that you are scanning for vulnerabilities on a daily basis, then the next stage will be to ensure that all supply chains are protected to the same standard and with the same policies that are applied in-house.

All of this should be in place in the present day, but as we move to the future, it's time to start looking at designing a 'zero trust' network. With a zero trust network, you make the assumption that attackers could come from both inside and outside your network. No one is automatically trusted – even members of staff – and neither are any devices.

In this scenario, you would look to apply the principle of least privilege access. This is something most companies should be doing in some form already. For example, any application or piece of data should only be accessible to those who really need it.

Furthermore, multi-factor authentication will need to come into play – where anyone logging onto the network will need to use an additional factor such as a token or one-time password, physical location or user behaviour analytics. But these are just elements in the Zero Trust model which should be part of an overall digital transformation strategy that takes full advantage of the move to the cloud.

CELEBRATING 11 YEARS OF SUCCESS

Announcing the 11th edition of the premier IT awards: The Storage, Digitalisation + Cloud Awards 2020.

In what has been, and continues to be, extraordinary times for the business world, it seems doubly important to recognise the projects, innovations and individuals which have made such a huge difference during 2020. Almost overnight, employees switched from office working to working from home, and the new, or next, normal, means that, into the future, what might be called a 'hybrid work' model looks set to evolve, with flexible working very much the order of the day. What was already becoming a trend as part of many organisations' digital transformation programmes, has been accelerated.

The SDC Awards 2020 will celebrate the achievements of end users and the IT community as they have innovated like never before to ensure business continuity in these challenging times. This year more than any other, please do make sure that you enter our SDC Awards. There's no limit to the number of entries, all of which are free of charge, and we'll be promoting all the short-listed entries via Digitalisation World's multi-media platform over the coming months, ahead of the awards ceremony. We really do want to celebrate and recognise the many amazing achievements which have come about in response to the coronavirus.

WHY ENTER?

MAXIMISE VISIBILITY
Free PR opportunities with 5 months of marketing utilising the Digitalisation World portfolio.

POSITIONING
Position your product or service as an innovator in your field.

INCREASED CREDIBILITY
An award win, shortlisting or nomination acts as a 3rd party endorsement.

NETWORKING
Over 300 industry leaders attend the gala awards evening.

COMPETITIVE ADVANTAGE
Gain an advantage on your competitors.

NOMINATION IS FREE OF CHARGE AND VOTING IS DONE BY THE READERSHIP OF THE DIGITALISATION WORLD STABLE OF PUBLICATIONS.

SDC AWARDS 2020

www.sdcawards.com

Data protection and the new normal

How pubs and restaurants should handle customer data.

BY TIM HICKMAN, PARTNER AT WHITE & CASE

SINCE THE EASING of the UK's COVID-19 lockdown began, pubs and restaurants have been key focal points. On the one hand, they are businesses that rely on a steady stream of customers. On the other hand, that steady stream of customers has the potential to bring, and spread, the COVID-19 virus. The UK government's solution to this problem has been to issue guidance stating that pubs and restaurants should collect personal data of those customers, as part of the NHS Test and Trace program. According to the government's guidance, the aim of these data collection activities is to "help contain clusters or outbreaks" of COVID-19.

There is no one-size fits all solution to these data collection obligations. Some restaurants have adopted a system of requiring all customers to book in advance, and then confirming arrivals on a digital system that automatically maintains the necessary records – but clearly that approach only works for a limited number of businesses. Other pubs and restaurants have turned to third party services, including the use of innovations such as QR codes displayed around the premises, so that customers can scan the codes on their mobile devices, enabling them to provide their details without needing to interact with staff. However, this may mean that some customers

do not scan the QR codes, reducing the accuracy of the data collected. As a result, the system of collecting data remains fragmented.

When these data collection obligations were first introduced at the start of July, many commentators observed that there were serious challenges in implementing them, not least the fact that there was no official guidance on how pubs and restaurants should satisfy their data protection obligations. Since that time, the UK Information Commissioner's Office ("ICO") has released some helpful guidance that explains to pubs and restaurants (and other businesses) what they are required to do. The issues set out in the ICO's guidance will be familiar to anyone who has experience of the UK's data protection regime, but are nevertheless likely to be helpful to pubs and restaurants who may be addressing these issues for the first time. The key points are:

- Only collect the data that are strictly necessary (e.g., name, address, arrival time) and avoid collecting unnecessary data (e.g., marketing details)
- Be transparent with customers by explaining to them how their personal data will be used (e.g., in the form of a privacy notice)
- Keep the data secure (which may prove a challenge for pubs and restaurants who are collecting data on a tight budget)
- Do not re-use the data for other purposes (e.g., marketing)
- Securely delete data that are no longer needed for the purposes of compliance with the government's guidelines

However, the ICO has indicated that during the pandemic it expects to conduct fewer investigations than normal, focussing its attention on those circumstances which suggest "serious non-compliance". For pubs and restaurants that fail to comply with the ICO's guidance, it remains unclear whether the ICO is likely to take enforcement action, or what such action might look like in the current circumstances.

Britt Endemann, Co-Head of Data Governance at Forensic Risk Alliance, offers a perspective on data privacy:

She says that collecting customer information for NHS Test and Trace proves that technology companies are under increased pressure to help us adapt to the 'new normal'. Without technology, the hospitality industry most probably wouldn't have been able to open up again in the same way.

Britt says that: "GDPR goes some way to protect consumers, however a successful regulatory regime, protects not only against current threats but also future ones and the world Covid-19 is creating is a unique one. Collective adherence is key to fight the pandemic. Hospitality companies and consumers signing up to new technology software or services recognise this. Most are collecting and providing information in good faith."

"However, valuable information and data regarding the habits and profiles of individual consumers is being placed in the hands of technology companies in a way never seen before. When you grab a quick pint, pick up your favourite local takeaway, or open an electronic menu at the restaurant (by bat code scan) – this is now data that's being captured, packaged and resold, resulting in long term unforeseen consequences.. As we move forward in this pandemic it's critical that the government protects the rights of individuals through appropriate legislation, consumers have transparency and clarity on what they are signing up to, and effective enforcement moves beyond data breaches and into safeguarding the rights of individuals."

Keeping in mind England's test and trace programme has broken a key data protection law - conceded the initiative to trace contacts of people infected with Covid-19 was launched without assessing its privacy impact, Kelvin Murray, a Senior Threat Research Analyst at Webroot, shares the following thoughts:

Given the urgency in rolling out the test and trace programme, it is clearly challenging to balance the importance of public data privacy with the need to track the epidemic accurately to keep people medically safe. This was always going to be difficult given the timeframe, but privacy and security still need to be front of mind when dealing with any personal data. This is especially important with healthcare data, which is at particular risk of cyber-attacks and data breaches as information such as health records is very valuable to criminals. There, therefore, needs to be stringent security controls and processes in place to ensure that individual data is treated extremely sensitively and remains secure.

With apps such as these, uptake will be based on trust. The technical details aren't going to be understandable to most UK citizens, but the level of trust they have for their government will be based on the history of their government and all of its intelligence agencies, law enforcement bodies and partners. With several high-profile data breaches having taken place in the healthcare industry recently, the government is particularly under the spotlight with compliance efforts being more carefully scrutinised and recorded than ever before.

WHAT'S NEXT?

for cybersecurity?

A recent HP panel discussion sought to provide some answers to this question – topics covered including: the ethics of paying ransoms, to politicised destructive attacks and the new 'anchors' of compute infrastructure in a remote world.
Here we look at some of the key discussion points.

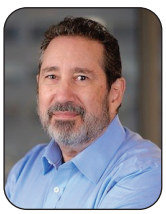
The long-term impact: a look at what's changed for the long haul. What are the positives and negatives of the pandemic for CYBERSECURITY? Will we 'snap back' into old models?

Kris Lovejoy, EY Global Cybersecurity Leader and former CISO of IBM:

"According to our research 84% of the world introduced some work from home capability, 60% introduced technology to enable that, and 60% of those either completely skipped or abbreviated the security checks as part of that implementation"
"We see CISOs being left out of the decision-making process around transformation and budgets are being cut. So why be optimistic? Because usually organisations just buy more stuff to deal with crises or compliance. They never take anything out. My hope is that this pressure will mean we streamline and reduce complexity. The combination of top down focus, and budget restrictions will fundamentally change our approach to cyber."

Ian Pratt, Global Head of Security (Personal Systems), HP Inc:

"We're seeing an acceleration of trends that were happening any way. Even very simple IT work practice has changed. Organisations have had to work out how to get laptops to employees with all the correct compliance, credentials, and certificates without it stopping off at an IT practitioners' desk. We're now enabling organisations to order machines not only imaged, but also provisioned with security credentials straight from the factory, so employees can use them securely straight out of the box. We're at a point where end-points really have to be able to look after themselves at every stage."



Charles Blauner, Partner & CISO in Residence at Team8, former Global Head of Information Security, Citigroup:

"COVID-19, if nothing else, has started to get people thinking about

operational resilience. The good CISOs understand how to use the idea that security is a foundational aspect of operational resilience. Those who do are getting more budget and expanding the definition of what it means to be a CISO. This is an opportunity for good CISOs to change their relationship with their CEO and their business."

Boris Balacheff – HP Fellow and Chief Technologist, Security Research and Innovation, HP Inc:

"From remote work, to IoT infrastructures, to all forms of automation – massively distributed infrastructure is becoming the norm. In a distributed world, endpoint devices are truly on the front line of the CYBERSECURITY battle ground. No one is going to turn up at your door to help you if something goes wrong. Look back at early destructive attacks like Shamoon - going after 35,000 workstations. It's simply not possible to have the sort of IT intervention that took to get people back on their feet today. We need to give the technology that underpins our information systems the autonomy and self-healing capability to guarantee resilience, designed and anchored into the hardware itself."

Where does threat go? Are we already seeing something different? What's been the biggest shift you've observed, in your respective roles, from the criminal element and where do you think adversaries will turn next?

Kris Lovejoy, EY Global Cybersecurity Leader and former CISO of IBM:

"We've got a major trust deficit between consumers and the institutions that serve them. People don't trust governments or corporations. They don't trust them with their personal data and that drives regulation. And that lack of trust isn't just expressed in angry consumer tweets – it's expressed in the boycott of brands, disinformation campaigns and in cyber attacks. We're seeing a strong increase in the number of disruptive and destructive attacks that are perpetrated by social activists. As a CISO, that frightens me. We have to recognise that the nature and frequency of these disruptive and destructive attacks are going to increase."

Boris Balacheff – HP Fellow and Chief Technologist, Security Research and Innovation, HP Inc:

"With most employees operating remotely, disruptive or destructive attacks become even more damaging. As exploit sophistication increases, firmware attacks could become an extremely dangerous and attractive target. Attacks aiming to 'brick' devices could isolate workers and halt operations entirely on a large scale. Devices that can offer autonomous recovery, a self-healing capacity, built into the hardware, beneath the software and operating system, becomes mission critical."

Has the threat model changed?

The trickle-down effect of cyber warfare. Undetectable malware.

Ian Pratt, Global Head of Security (Personal Systems), HP Inc:

"Things that would have been regarded as requiring nation state sophistication are now being perpetrated by criminal organisations. There exists a criminal supply chain of different organisations contributing specialist skills – finding vulnerabilities, building exploits or payloads, crafting the lure, distribution, etc. In addition, the whole yield management has become much more sophisticated – criminals making sure they extract as much money as possible from a victim, increasingly playing the long game. We're seeing more maturity, more sophistication, but the actual model itself hasn't changed. Endpoints are targeted. It's still users being duped to invite the attacker in."

"Most security is detection based. And the thing that bad guys have done very well is evading detection, using machine generation and automation to mutate malware to evade detection. Testing against common security products is just part of the QA process prior to an attack – it's typically outsourced as one of the specialised functions in the criminal supply chain. That's why we use isolation technology, virtual machines that can seamlessly spin up and contain these risks. This provides protection without relying on detection, resilience against the undetectable."

Do you pay the ransom? Recent news suggests some major companies have paid out in ransomware cases – what are the issues in play here?

Charles Blauner, Partner & CISO in Residence at Team8, former Global Head of Information Security, Citigroup:

"It's a very tough ethical question. You have a responsibility to shareholders, employees' livelihoods, and customers safety, as well as a responsibility to think through where that money might end up - from potentially funding a group involved in modern day slavery, to an active terrorist cell. There

is no easy answer. But what I struggle with is that too many companies have left themselves in the position where that's a question they might have to face. There should not be the circumstance where a ransomware attack could bring a major corporate entity to its knees. That means an absolute failure in security design."

Does cyber-insurance change the equation?

Kris Lovejoy, EY Global Cybersecurity Leader and former CISO of IBM:

"Historically ransomware hasn't been considered a disclosable event. That's beginning to change but as ransomware providers do more data exfiltration, what we're seeing is both more attacks, and more disclosure. In the background cyber insurers are looking at things like Baltimore.

In May 2019 Baltimore got hit and the ransom was 79k USD. They said no and ended up spending 18 million to rebuild their network. Today, insurance providers are largely recommending paying the ransom. Many of the questions I get become 'how the heck do I buy bitcoin', 'who will do the negotiation'."

HP Survey Security Insights

Sample: 1070 IT Managers and IT decision makers surveyed. Data fielded in May 2020.

- 51% End-users feel they're not set up adequately for remote work
- 80% IT Managers believe IT is in a more visible role
- 81% Believe IT is more tied than ever to the success of the business
- IT spend is more optimistic than earlier in the crisis, 44% of IT Managers are increasing spend for this year. 26% are decreasing spend for this year
- 40% IT Managers plan to augment security because of current situation
- 49% have increased spend on network security
- 44% have increased spend on cloud and server security
- 33% have increased spend on endpoint security
- 46% are outsourcing more in their network and/or endpoint security

CELEBRATING 10 YEARS OF SUCCESS

The 2020 DCS Awards feature 31 categories across FOUR groups.

THE DCS AWARDS are now firmly established as the data centre industry's premier annual celebration of all that is great and good. End user projects, product innovation and individual excellence are all recognised in an evening that pays more than lip service to the idea of data centre and IT convergence. So, the award categories cover both the facilities and IT aspects of the data centre, recognising the achievements of vendors, their business partners, their staff and their customers.

Getting involved with the DCS Awards couldn't be easier. Take a look at the award categories, and make sure to nominate your company, a customer, or maybe an individual – better still all three (!) – for a chance to be recognised for outstanding achievement when it comes to projects, product innovations and individual contributions within the data centre industry.

Once you've made your nominations, make sure to book a table for the Awards night. You wouldn't want to win an award and not be there to collect it! (And even if you don't win an award on the night, there's a cocktail reception, three course meal and a top comedian to entertain you – we have a track record of booking individuals on their way to the top of the comedy circuit).

To 'We look forward to welcoming you to the Awards night in December.

NOW, GET NOMINATING!

WHY ENTER?

MAXIMISE VISIBILITY
Free PR opportunities with 5 months of marketing utilising the Digitalisation World portfolio.

POSITIONING
Position your product or service as an innovator in your field.

INCREASED CREDIBILITY
An award win, shortlisting or nomination acts as a 3rd party endorsement.

NETWORKING
Over 300 industry leaders attend the gala awards evening.

COMPETITIVE ADVANTAGE
Gain an advantage on your competitors.

NOMINATION IS FREE OF CHARGE

The DCS Awards panel will validate entries and announce the final shortlist to be forwarded for voting by the readership of the Digitalisation World stable of publications in October 2020.

The winners will be announced at a gala evening at the LEONARDO ROYAL ST. PAUL'S HOTEL, London on 10 December 2020.

DCS AWARDS 2020

www.dcsawards.com

Supported by

dca The data centre trade association

It's all about edge, APIs and 5G

Pascal Geenens, director of threat intelligence, Radware, offers some fascinating insights into some of the security issues thrown up by the digital world.

SMART CITIES and agriculture through to smart energy and healthcare will require a more dynamic edge computing model. But security will need to catch up. Over the next 18 months we'll see more emphasis on securing APIs at the edge, and models that orchestrate and automate security.

Securing edge computing and APIs – A case of local decision making based on global intelligence.
CYBERSECURITY must focus on protecting APIs and edge computing. Why? Mobile applications, business automation, logistic automation, manufacturing devices right through to the advent of smart devices and autonomous cars use APIs to manage data and upload it to big data applications in the cloud.
We are familiar with the concept that large scale APIs can be deployed in large central clouds, but APIs for solutions that use low-latency and real-time data should be deployed as close as possible to their consumer, which means in the edge cloud and at the mobile edge.

APIs, much like web applications, need DDoS protection, application level security provided by Web Application Firewalls (WAF), and a good bot management solution. However, there's a problem. These forms of APIs cannot be backhauled through a central security stack because it would 'break' the concept of edge computing.

There's also another consideration. Current technologies used to host APIs take the form of containers or serverless compute. This means that as edge computing becomes more prevalent so security must evolve to become more 'light-weight' and take a form that can easily integrate with containers, Kubernetes pods, and applications on the edge.
But this is only possible if the bulk of the big data processing and central intelligent policy management is kept away from the resource constrained edge. Security needs to follow a control and data plane model: a centralised control plane used to oversee

the strategy, while enforcement and local security decisions happen at the edge.

Orchestration will therefore be essential to manage complex and distributed network architectures. It's a complex security challenge and one that can only be effectively managed by adopting security solutions that come with a control plane and a standardised set of protocols that can be integrated with a higher level orchestrator. This approach means that an orchestrator can help organisations and managed security service providers oversee security across multiple vendors and a distributed architecture.
Automation is imperative

But still this will not be enough. Automation will be critical to manage the speed and volume of decisions that have to be taken in order to protect the network. This means using algorithms that can automate detection and mitigation of DDoS attacks in seconds versus the time it takes a human brain to spot a pattern and respond.

The intelligence that can be gathered from such security approaches will also help security teams focus on strategy, giving them room to improve alerts and build better automated responses. This flexibility in planning will become essential as more and more 'things' are added to the network and should help avoid potential blind spots developing in the security strategy.

5G brings about the possibility of driverless cars, but also more security risks

Continuous innovation in the connected world demands lower latency and near real-time decision making and communications. That's why 5G is so exciting and why driverless cars are a real possibility this decade.

The trials for autonomous vehicles focus on ensuring the vehicle is aware of its surroundings, road conditions and traffic flows so it can moderate speed and behaviour. This level of autonomy and real-time decision making promises to deliver greater safety and fewer road traffic accidents, reduced congestion, optimised battery efficiency and ultimately greener cities.

It's done by using predictive algorithms,that receive input from connected devices in the immediate vicinity. However, this information must be accurate and timely for driverless cars to succeed.

Real-time decision making and communication like this relies on data being available where it is needed at the exact moment it is needed. So no longer can we rely on backhauling communications for all connected devices to a central cloud. It will only increase latency and slow down decision making. Instead decisions need to be made at the mobile edge.

However, this approach to computing significantly increases the attack surface because you are not just dealing with one device but potentially millions of devices, and a network of APIs that make them work. APIs are a dream for hackers because they can use them to deploy remote attacks to connected 'things' at scale.

Disruptive attacks such as Denial of Service can target the API acting as a service for the connected device in a city. Such disruption may be enough to render all the smart devices within the area ineffective.
Take electric charger points or smart parking meters, these could easily be attacked and abused for credit card skimming campaigns.

Manufacturers will therefore need to ensure that APIs and services are adequately secured. However, achieving this in a highly distributed architecture is complex due to the large number of light-weight edge services, many of which will be running on third-party edge computing systems. The approach to protecting a distributed environment is significantly different to securing a centralised system.

Attacks are growing more complex and becoming automated, requiring more intelligent detections based on a broader context. This translates to lots of CPU and memory resources and big data lakes, something that is available in the public cloud but not readily available in the cloud and mobile edge.
APIs, much like web applications, need DDoS protection, application level security provided by Web Application Firewalls (WAF), and a good bot management solution. However, there's a problem. These forms of APIs cannot be backhauled through a central security stack because it would 'break' the concept of edge computing.

There's also another consideration. Current technologies used to host APIs take the form of containers or serverless compute. This means that as edge computing becomes more prevalent so security must evolve to become more 'light-weight' and take a form that can easily integrate with containers, Kubernetes pods, and applications on the edge.
But this is only possible if the bulk of the big data processing and central intelligent policy management is kept away from the resource constrained edge.
Security needs to follow a control and data plane model: a centralised control plane used to oversee the strategy, while enforcement and local security decisions happen at the edge.

It's a complex security challenge and one that can only be effectively managed by adopting security solutions that come with a control plane and a standardised set of protocols that can be integrated with a higher level orchestrator. This approach means that an orchestrator can help organisations and managed security service providers oversee security across multiple vendors and a distributed architecture.

enel x

Energy management solutions that deliver commercial and environmental rewards

Global resources, local market knowledge and specialist technological expertise make Enel X the trusted energy management partner for data centres and large scale enterprises all over the world.

Join us as we pave the way for a cleaner, more dynamic future.

enelxuk@enel.com | www.enelx.co.uk