INNOVISION

INSIGHTS + PERSPECTIVES

Part 2

Over 70 contributions offering insights and perspectives on how technology is likely to develop over the next 12 months

IN ASSOCIATION WITH

DATACENTRE SOLUTIONS

DIGITALISATION WORLD

ISSUE II 2021
digitalisationworld.com

Editor's View

By Phil Alsop

Welcome to Digitalisation World InnoVision 2021 – Part 2

WE'VE GATHERED TOGETHER over 70 contributions offering insights and perspectives on how technology is likely to develop over the next 12 months or so. So, between Parts 1 and 2, that's near enough 150 viewpoints, providing a great snapshot of the technologies and topics set to dominate over the next 12 months.

In this issue, security is the headline act, for obvious reasons, but there's also some great content on data centres, analytics, storage and networks, along with individual contributions on a range of more specialist areas. There's some 'flexibility' in terms of which contributions appear under which categories – so please forgive us if certain contributions don't appear where might seem most sensible or obvious (!) - but the important thing is that there's a whole host of valuable information contained within this supplement, so please enjoy reading it.

If there are key themes which emerge from the many viewpoints in DW InnoVision, these would be the need for flexibility, agility, speed and a focus on the customer experience (with the customer being both the internal and external users/experiencers of an organisation's IT infrastructure). The events of the past 12 months have demonstrated the need to be able to re-organise and re-focus the business, quickly and reliably. And, if necessary, to continue this process to respond to changes in demand as they occur.

Crucially, there is now a general recognition that the experiences of employees and end users are the driving force behind the shape of an organisation's IT footprint. Whether it's working from home, buying goods and services remotely or simply consuming digital content, expectations are universally high.

Specifically, for Part 2, we can't escape from cybersecurity 'domination'. The more everything goes digital, the more security issues arise. That's not a reason to not go digital, but does mean extra care needs to be taken. After all, documents in a locked filing cabinet, in a locked office, in a locked building, policed by a security guard, have to be safer than digital information in a connected world. But the ability to do so much more with the 1s and 0s, as opposed to ink and paper is a more than satisfactory business trade-off – provided you take seriously the issue of cybersecurity.

Hopefully, the contents of DW InnoVision will inspire you to ensure that innovation, including around cybersecurity, is very much a major focus for your organisation into the future – a future that remains uncertain – but full of opportunities!

DW 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 Executive 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

Chairman: Stephen Whitehurst
CEO: Sukhi Bhadal
CTO: Scott Adams

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

Angel BUSINESS COMMUNICATIONS

DW INNOVISION
INSIGHTS + PERSPECTIVES

CONTENTS

ISSUE II PART II 2021

CYBERSECURITY

DATA ANALYTICS

DATA CENTRE

DW INNOVISION
INSIGHTS + PERSPECTIVES

CONTENTS

STORAGE

NETWORKS / TELECOMS

FINANCIAL

APPS

CHANNEL

MISCELLANEOUS

DW INNOVISION
INSIGHTS + PERSPECTIVES

CYBERSECURITY

Cybersecurity continues to be a major focus for virtually all businesses, as they struggle to with the central complication of the digital age: the more everything is connected, the more opportunity and the easier it is for cyber-criminals phish, hack and ransom data.

IN ASSOCIATION WITH
DW DATACENTRE SOLUTIONS
DW DIGITALISATION WORLD

ISSUE II 2021
digitalisationworld.com

Kyle Turner
Cyber Security Regional Manager, Middle East
www.aoitgroup.com

Top cybersecurity trends for 2021

IN AN EVER-CHANGING WORLD of cyber security so many things change while others remain the same, the most important thing any organization can do in such a daunting environment is stay up to date with what is happening while ensuring that they have the most basic security principles in place at the same time.

Keeping up and staying secure can be a challenge, especially when you do not have reliable information to base your risk management strategies on. How do you defend yourself if you cannot see your enemy?

“To know your Enemy, you must become your Enemy.” Sun Tzu
As an industry expert with over 50 years of IT and Cybersecurity experience A&O IT Group provides industry insights into what the market leaders are seeing happening in these challenging times.

Key Highlights

- The biggest challenge will be to fill the growing skill gap for cyber security resources.
- COVID-19 related attacks are increasing and becoming more sophisticated.
- A greater move is needed toward automation of monitoring, detection and response.
- Mobile and cloud adoption continue to disrupt traditional security methodologies.
- Data privacy and digital trust are rapidly changing with increased advancements in digitization.

“The relentless pace of digital business and ongoing transition to cloud are challenging traditional security approaches. Acting on these developments, security and risk management leaders can improve resilience, better support business objectives, and elevate their organizational standing.” Gartner

Biggest Losses in cybersecurity

Email and Payment Scams

Though phishing and similar social engineering attacks are nothing new, the way in which these attacks are delivered, and the techniques used to deliver them are ever changing, attackers will often theme these attacks around what is trending in the news and with that there is an increased target on COVID-19 related scams.

According to the FBI IC3 2019 Internet Crime Report [1] e-mail related scams will top 26 Billion in the next 3 years while payment fraud has already caused losses of over 3.5 Billion for 2020.

Recommendation

Awareness training and education are the key to thwarting social engineering attacks, along with simulation attacks that test the effectiveness of the training being provided.

Biggest Spending Trend

Deception Technologies & Post COVID Spending

The use of AI and ML in furthering deception technology used to divert attacker’s efforts to honey pots and exhaust their time and resources to prevent APT’s is seeing the greatest investment and forecast to reach 2.48 Billion by 2025. Source: Mordor Intelligence [2]

Even with Information security spending [3] expected to increase to 151 Billion by 2023 with a forecasted CAGR of 9.4% prior to COVID-19 and remaining positive [4] at 6.2% after the pandemic, cybersecurity budgets [5] remain largely underfunded.

Recommendation

Paying attention to where other organizations are spending money helps in knowing where to allocate your investment for risk management. Early investment in the right technology can greatly help in staying ahead of the curve.

Attack Trends

COVID-19 Attack Trends

Since remote working has now become the new normal the security landscape has completely changed, organizations now need to refocus their efforts to facilitating work from home (WFH) situations which is causing an inevitable disruption in regular day to day security operations. Source: Gartner

Recommendation

Constantly testing new technologies being implemented is a vital part of managing the associated risks. Work from home solutions should be thoroughly tested as they often provide much less security than normal.

Deep Fakes & Disinformation

Perhaps not directly related to cybersecurity, we are seeing an increase in deep fake content being distributed to cause increased anxiety and untrust in the media and then used to further social engineering campaigns.

The term "Fake News" has become a major media highlight and again not directly related to cybersecurity, hacking organizations are spreading misinformation to advance social engineering attacks based off news trends and social anxiety.

Recommendation

Again, education is key here, since the weakest link in any system are the people that use it, these people are also often your last line of defence when it comes to these techniques being successful.

Synthetic Identities

Identity spoofing (faking) is becoming way more sophisticated to the point that these false personas have detailed banking records, birth certificates and social profiles making it extremely challenging for automated and even human AML/KYC systems to spot the difference between a real and a fake identity.

Recommendation

Relying on purely automated solutions for AML/KYC systems may not be sufficient to adequately spot these false identities. It is important that additional validation is performed after the fact.

AI Powered Cyber Attacks

Attackers have long used AI and ML in furthering their attacks and this trend will continue to show advancement as the technology reaches maturity and access to greater computing power becomes cheaper and more available.

Recommendation

The use of artificial intelligence being used by cyber attackers has made it nearly impossible for traditional cyber teams to be resilient against these attacks, cyber teams need to be augmented to protect against these techniques.

Attacks on AI Systems

AI poisoning attacks used to tamper with ML while still training is increasingly being used to add biases to training sets and allow for malicious activities to look benign, causing AI monitoring systems to miss the activities they are meant to detect. Source: Gartner

Recommendation

Securing training sets properly can be the difference between your AI data sets either doing what they need to or the complete opposite.

Cyber Physical Systems

The fact that cyber incidents can now impact physical systems means that attackers can now cause harm not only to computer systems and data but even to human life and disrupt physical systems that most cities rely on. Operational and Information security have for long been siloed but can now affect each other more and more. Source: Gartner

Recommendation

Treating these different domains as completely siloed entities is the worst thing that major OT vendors and providers can do. Operational Technologies need to be tested as vigorously as any other IT system as the risks go far beyond just cyber.

Defence Trends

Working from Home

Organizations are now having to shift their cybersecurity focus from traditional corporate networks to an almost completely remote solution where digital transformation takes precedence over corporate network security. Source: Gartner

Recommendation

The majority of security expenditure is mostly focused on corporate networks and not necessarily for remote working and even then, these implementations are susceptible to attacks. Sufficient penetration testing of remote working solutions is of the utmost importance.

AI Immune Systems

The sheer amount of data needing to be analyzed to effectively monitor and prevent cyber incidents is far too much for human teams to handle, and so the need for AI and ML tools has become a saving grace for companies looking to enhance their cyber capabilities while lowering the cost associated with hiring large cyber teams. Source: Gartner

Recommendation

Using AI and ML to augment human resources are absolutely a must to protect against new breeds of attacks, along with using the correct technologies, companies should outsource the bulk of monitoring, detection, and response tasks to dedicated managed security service providers.

Software Defined Networks

While everything moves into the cloud and digitalization is transforming the way we think about traditional computer networks the last part to be completely physical is the network aspect. SDN's offer a much lighter and more manageable solution when it comes to maintaining and monitoring these massive networks.

Recommendation

SDN implementations may be costly and complicated to set up, and does not make sense for smaller networks, but having any sort of cloud hosting solution, companies should look at providers that are taking advantage of the technology.

Automated SIEM and SOAR Solutions

With the ever-increasing gap in cybersecurity workforce and the advancement of technologies being employed it is now more important than ever to increase the use of automated systems used to monitor and detect cyber threats. Source: Gartner

Recommendation

Automation is key to being able to handle the vast amounts of alerts being generated on a daily basis. Companies need to take advantage of technology to sift thought the many false positives so that cyber teams can be free to do threat hunting and other remediation tasks.

Data Privacy

Data privacy and security concerns has moved to the top of the list for most organizations, with breaches now leading to massive penalties and compliance becoming more data centric this has led to a major hiring move for data protection personnel over the last two years. Source: Gartner

Recommendation

The first step to understanding your exposure regarding data is to know what regularity and compliance issue your industry and business must adhere to. Once that has been defined organizations need to assess the guidelines associated with them to confirm they are in good standing and then perform regular penetration tests to assess the security measures taken.

Hiring Strategies

CISO's and other security hiring managers are constantly looking for diverse teams to handle cyber operations, and keep talent motivated in the work that they do, the challenge with this is that cyber security skills span many areas and professionals are expected to fill multiple tasks that were not what they set out to do. Gartner

Recommendation

Along with augmentation of cyber teams with technology, it is important to understand that this is still not sufficient, the best strategy is one where internal teams and technologies are coupled with trusted partners who can handle the bulk of the workload while your internal team manages more important tasks on the ground.

References

[1] https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

[2] https://www.mordorintelligence.com/industry-reports/deception-technology-market

[3] https://www.idc.com/getdoc.jsp?containerId=IDC_P33461

[4] https://www.researchandmarkets.com/reports/5021764/global-cyber-security-market-analysis?utm_source=dynamic&utm_medium=BW&utm_code=x9x8bq&utm_campaign=1387343+-+Global+Cyber+Security+Market+is+Forecast+to+Grow+at+a+Slower+Average+Rate+of+6.2%25+per+year+to+2023+Due+to+Economic+Consequences+of+COVID-19&utm_exec=cari18bwd

[5] https://www.isaca.org/go/state-of-cybersecurity-2020

Candid Wüest
VP of Cyber Protection Research
www.acronis.com

Cybersecurity predictions for 2021

Attacks on remote workers will only grow

With COVID-19 infection numbers growing rapidly, it is hard to imagine that the pandemic will end this year. More likely, it will take all of next year and maybe even 2022 for a vaccine to be globally distributed. That means remote, poorly protected workers are here to stay. In 2020, cybercriminals realised that phishing still works very well and that employees are the gateway to companies' data. We expect attacks on remote workers to grow in number and sophistication as more cybercriminals strive to get to the business data and systems located in empty offices and data centers.

Data exfiltration will become bigger than data encryption
Recent ransomware cases showed that cybercriminals want to monetise every attack. More than that, they saw that extortion based on stolen confidential data is working very well, maybe even better than when they simply encrypt the same data. That is why we expect the main target in every ransomware attack will be data exfiltration.

Data protection and data loss and leakage prevention solutions will be very important in the coming year because even if we see a reduced number of new ransomware families, the active ones will do huge damage and be very successful. That means next year we expect ransomware to still be the number one threat for businesses.

More attacks on MSPs and small business

With more small and medium businesses using cloud MS(S)Ps, more cybercriminals are invited to attack them. In 2019-2020, bad guys realised that attacking MSPs is very efficient, especially smaller ones who may not be prepared. By attacking MSPs, they attack the dozens of companies the MSP serves and can get more money through ransomware infections or banking Trojans. In addition, the attackers can make use of well-established tools, such as remote access and software delivery tools. These types of attacks are more likely to grow in number and geography as both small businesses and MSPs aren't ready for serious attacks and yet are still able to pay a moderate ransom.

Cloud under attack

During the lockdown, many companies moved their services to the cloud. Unfortunately, the configuration was often done in haste and is therefore not perfectly secure, leaving cloud applications and data services exposed to everyone on the internet. This scenario provides an opportunity for attackers to access and exfiltrate data, as we have already seen with data breaches on S3 data buckets and elastic search databases. Furthermore, identity and access management is still frequently overlooked, although identities are becoming the new perimeter. This situation will lead to an increase in user entity behaviour monitoring and dynamic access controls.

Onkar Birk
Chief Product Officer, Alert Logic
www. alertlogic.com

Lessons learned in 2020: The case for managed detection and response

K see a variety of cybersecurity breaches, but it could be said that 2020 was characterized by just one major event. The COVID-19 pandemic shaped much of the landscape this year, rapidly transitioning most of the globe to a remote workforce and placing unprecedented demands on digital systems as a result of widespread shelter-in-place orders. While this presented opportunities for cybercriminals and led to a number of security issues, it has also provided several lessons that can be applied to increase protection in the new year. Here are some of our predictions for 2021.

Defense strategies focus on the “home” front The 2020 pandemic forced an ad-hoc shift to remote workforces with the number of remote workers more than doubling since the beginning of the pandemic. Unfortunately, that accelerated transition to remote work exposed some gaping security holes. More than half of employees use their personal computers and mobile devices for work, even though three-out-of-five say their employer hasn’t provided tools to secure these devices. Predictably, cybercriminals have capitalized on the crisis with nearly two thirds of all security pros saying they’ve seen a rise in cyber attacks since the pandemic began.

We should expect these trends to continue. Even with a vaccine likely before the end of the year, most companies will extend their work-from-home arrangements well into the new year, and others will make full-or part-time remote work standard for some portion of their employees.

Organizations will have to continue addressing the increase of employees connecting to their networks from their own devices over the public internet. Basic security precautions such as making sure both company-issued and personal computers are patched and updated against the latest threats, ensuring

workers connect to the company network through a VPN, and educating workers to be vigilant with emails requesting sensitive information, will be critical. Additionally, Chief Information Security Officers (CISOs) and small-business security vendors will need to focus on interoperability by investing in integrated services and tools that provide tangible ROI, rather than a combination of multiple disjointed solutions.

The attack surface expands exponentially

"There is no perimeter anymore" has been a common refrain in cybersecurity for a while, but the pandemic has driven the point home. With a majority of employees working remotely, a wealth of corporate data now sits on home networks connected to "smart" speakers, thermostats, security cameras and kitchen appliances. These often poorly secured Internet of Things (IoT) devices and fusion of home and work assets comingled on shared computing platforms and modems will loom as a heightened risk to sensitive company data in the new year.

The increased mobility of employees taking advantage of greater Internet coverage from satellite-based broadband systems and 5G network speeds will further expand the attack surface and complicate visibility into already extremely complex environments. This will make risk management paramount in 2021. A steep increase in the usage of SaaS applications has been another byproduct of the new remote workforce. Without the friendly office IT person popping over to fix or install our applications, the way has been paved for a new avenue of attacks. The days of worrying only about securing the workstation is a distant memory.

Security as a Service becomes the norm, at least temporarily
Nationwide lockdown orders have had a crippling impact on many organizations, forcing them to layoff or furlough staff. Security teams are no exception, and the knowledge and resource gap created by security staff reductions leaves the businesses more vulnerable in 2021.

There will be more urgency for IT companies to turn to "security as a service" offerings such as managed detection and response (MDR) to bolster their dwindling resources and ensure they remain protected. We may also see those furloughed and laid-off security professionals being contracted as a service to resource-strapped companies to provide 24/7 security monitoring. This gig-economy model may result in a disruption in security similar to what we've seen in transportation and other industries, at least until the economy recovers.

Though 2020 is coming to an end, it actually signals the beginning of a new era of cybersecurity issues, policies and practices. Taking lessons learned from this tumultuous year will better prepare us for what lays ahead.

Theresa Lanowitz
Director, AT&T Cybersecurity
www.cybersecurity.att.com

Security budgets 2021:
Planning for the unexpected

IT'S FAIR TO SAY 2020 will go down as one of the more memorable years in our lifetime. From a remote working perspective, cybersecurity was propelled into the limelight, reinforcing it is a critical business matter.

As a consequence, cybersecurity will be a key talking point discussed in boardrooms when budget allocations are addressed, whether this is for threat management and intelligence, consultancy, or training. While this may seem positive going into the new year, security leaders are still worried that this will still be insufficient, as recent research revealed that nearly one third (28%) of cybersecurity professionals are concerned about the prioritisation of security investments. Given that budgets and finances are commonly re-evaluated at the end of the year, organisations must factor in challenges related to security that previously hadn't been accounted for as 2021 approaches.

Direct costs that might not be planned but must be factored
When budgets were being planned for 2020, those planning in 2020 would not have factored in a global pandemic. Yet, the major disruption caused by Covid-19 has unexpectedly transformed the world. Many organisations have had to invest more than they had expected to continue business operations. Most businesses were forced to have employees work remotely from home; and to do this in an effective and highly secure manner, cybersecurity was an area where high, albeit unexpected, investments were made. This involved providing additional cybersecurity training, acquiring VPN licenses, extra licenses for secure email gateways, additional managed security services (MSS), and other typical cybersecurity budget line items.

Businesses must also consider the reality of a cyber-attack. At a time when suffering an attack has become a matter of when, and not if, boardroom executives must be proactive and plan for the disruptions caused by a successful cyber-attack. This should include remediation time during the aftermath. In addition to this, factor in any potential for business growth – whether this is achieved organically or through acquisition, and any rapid change to accommodate competitive business initiatives. While it's been said that you can't plan for an event or situation if you've never experienced one before, enterprises that have the most long-term success strategise for these unknown eventualities. Understanding where business risk may creep in over the course of the year helps organisations have a realistic budget that can help to successfully survive disruptions.

Those that fail to plan, plan to fail, and given the current global situation, the businesses that have either failed to plan or adapt quickly have suffered. The inability to embrace digital or online transformation, or make the quick switch to everything being remote, virtual, and touchless accelerated the decline of these companies. It's unfortunate, but over the course of the past 7-8 months we've witnessed household brands either go out of business or completely restructure.

What about the indirect costs?

On the other hand, let's address the indirect cybersecurity costs that organisations will face - starting with crisis management. This is closely related to unexpected disruptions and if a crisis arises, seeking external help from consultants or cybersecurity specialists is common practice to remediate the issue. If a ransomware attack has occurred, financial payment can be extorted and must be discussed when planning possible expenditures.

Crisis situations are often extreme with low possibility of actually occurring but having a strategy in place for a crisis is not a failure – it is being realistic. Forward thinking could potentially save the business millions in finances and reputation. If an enterprise is hit by a crisis, and hasn't had a plan in place, this can have a detrimental impact on the brand, customer loyalty, share prices (if it is publicly listed) and confidence in the running of the company. Given the events, disruptions and cyber-attacks that have taken place in 2020, this next year is likely to bring more of the same. It's therefore imperative business leaders take action to provide that their organisation can withstand the expected and plan for the unexpected in the coming year.

Alan Bentley
Head of Global Strategy at Blancco
www.blancco.com

2021: As enterprises shift from private to public data centre, a heightened focus on secure data management will emerge

SPENDING ON PUBLIC DATA CENTRE infrastructure jumped 25 percent year on year to nearly $17 billion in the second quarter of 2020. Enterprises have slowed private data centre investment due to the pandemic, but cloud providers have naturally continued to support remote working as businesses migrated their operations in droves.

The mass migration to the cloud that we've seen this year is set to continue into 2021. However, with the benefits come risks. By failing to review data ahead of a migration, keep what's needed and remove what is not – and crucially, ensure that data is properly sanitised – enterprises will unnecessarily expose sensitive material. What's more, this is exacerbated when the process is accelerated, which has been the case during the pandemic. Rushing to the cloud inevitably causes data security issues. The role of Data Protection Officers will rise in popularity – and we'll see a new demand for tools which enable data management in remote environments. Although, we do expect that cloud services generally will support this global shift, investing in more security to continue fueling cloud growth and to avoid increased risk of exposure.

2021: As ESG gains momentum, eWaste will be pushed further into the spotlight

Responsible investment became a buzzword more than a decade ago. But in the past few years we've seen a sea change, a sharp acceleration in the uptake of ESG investing. With this has come a maturing of philosophies and practices around responsible investment. COVID has augmented, rather than delayed this trend. According to Morningstar, the first half of 2020 showed net inflows into ESG funds in the US reached $21 billion, almost totally the entire amount of last year (which was in itself a record – four times the previous record for a calendar year).

This data suggests that in 2021 there will be even more messaging, momentum, and business strategy around sustainability, due to its direct link to revenue generation. Upcoming legislation such as the European Parliament's vote on a "right to repair" will only accelerate this change in the new year.

More than 53 million metric tons of eWaste was produced in 2019. And with technology investment on the rise to support a move to home working environments on the rise, it's an issue which is set to be pushed further into the spotlight. In fact, our own research showed that nearly half (47 percent) of large global enterprises created roles responsible for implementing and ensuring compliance with eWaste policies specifically to deal with technology investments generated from the COVID-19 pandemic. The incentive to extend the life of IT equipment and maintain it within a circular economy will continue to grow, with organisations looking to data erasure as a crucial factor in achieving their sustainability goals and ESG practices.

2021: ICO fines, reduced but certainly not going away
We've witnessed a slight relaxation on data privacy regulation in light of the pandemic, with more time given to rectify compliance failure. This was expected given the challenging economic environment faced by businesses around the globe, with regulators cutting some companies a little slack. For example, the reduction of both BA and Marriott's GDPR fines by tens of millions. But on the other hand, we have seen some even larger penalties levied. However, despite these cases of leniency, data privacy regulation, alongside the threat of fines and reputational damage, will continue to drive businesses to act on data privacy in 2021.

There is a general communication from the ICO and private security advisors that now is the time to be cautious. Companies globally are working in a new and unfamiliar distributed working environment, which brings new data privacy challenges.
As we step into 2021, organisations must ensure their data management policy is adapted to fit the "new normal". This means ensuring that all IT assets handling sensitive data are tracked and dealt with securely upon end of life.

Anthony Young
Director, Bridewell Consulting
www.bridewellconsulting.com

Top six cyber security trends in 2021

Bridewell Consulting, an independent cyber security and data privacy consultancy, has issued some cautionary advice for businesses as it sets out its top six predictions that will impact cyber security in 2021.

1. Sustained remote working provides new challenges

As a result of the Covid-19 crisis, increased home and remote working, decentralised workforces and outsourcing of skillsets are all contributing to a huge increase in connected devices.

This in turn increases the number of risks associated with centralised data and infrastructures, as well as vulnerabilities around multiple access points. In 2021, cyber security will be even more difficult to ensure as the attack surface is bigger and the measures to implement and control security and data policies are often lacking in a remote environment.

2. Death by cyber attack

A major concern is that the UK may start to see the first deaths associated with a cyber attack, as hospitals are stretched and attackers are continuing to target healthcare. The sector is particularly at risk due to the massive economic and operational impacts it is currently suffering and sadly we have already seen such a case in Germany. A homicide investigation was launched after a patient died in a Düsseldorf hospital which had its systems knocked by a cyber-attack. If this leads to a prosecution, it would be the first confirmed case in which anyone has died as the direct consequence of a cyber attack.

3. The evolving threat

Another impact of remote working will be more organisations relying on IoT devices for measuring and monitoring processes. With the continued expansion of IoT, along with the rollout of 5G, cyber attackers will be relishing the growing opportunity to compromise systems and networks, as even more devices become connected to the internet.

Organisations still need to adequately segregate insecure IoT and 5G-enabled devices from the rest of their network. In healthcare, for example, wearable IoT sensors enable remote patient monitoring, so unsecure devices could facilitate the misuse of sensitive patient data.

4. Detection, not just protection

Despite these new threats there are hopeful signs that the sophistication of defensive security will finally catch-up with its offensive counterparts due to new innovation and capabilities. Technical cyber defence will still be of uppermost importance, along with the need to focus on detection of cyber threats, not purely protection and prevention. Over the next year there is likely to be an acceleration in the use of Cloud SIEM, with human guided threat hunting, supported by machine learning-powered SIEM tools like Azure Sentinel, helping to uncover infiltrators before they access sensitive data. This will be augmented by SOAR (Security Orchestration, Automation and Response) software programs that enable businesses to collect data about security threats, and automatically respond to low-level attacks. We also expect to see more use of UEBA (User and Event Behaviour Analytics) which uses machine learning and deep learning to model the behaviour of users on corporate networks and detect behaviour that could be the sign of a cyber attack.

5. Defending aviation from attack

Cyber security has been spotlighted by the World Economic Forum (WEF) as one of the biggest issues facing the aviation industry. The economic and operational impacts it is currently

> The most likely threats to aviation are from the same sorts of threats as other businesses, may they be phishing attempts, data breaches or ransomware. Although cyber security is being taken seriously in the boardroom, much work is still to be done to bolster aviation businesses cyber defences

suffering mean this sector will be particularly at risk over the coming months. The most likely threats to aviation are from the same sorts of threats as other businesses, may they be phishing attempts, data breaches or ransomware. Although cyber security is being taken seriously in the boardroom, much work is still to be done to bolster aviation businesses cyber defences.

6) Business Email Compromise (BEC) isn't going away
BEC will continue to be one of the most financially damaging online crimes and one of the most popular methods for criminal groups to make money. BEC scams exploits the fact that so many of us rely on email to conduct business, both personal and professional. We've likely all been targeted by this kind of attack in the past - an email message that appears to come from a known source making a legitimate request, such as a supplier a company regularly deals sending an invoice with an updated mailing address. Employees need to be constantly vigilant for this type of attack.

"During this period of high uncertainty across all sectors cyber threats are constantly evolving and with more people working remotely, the pandemic has only accelerated threats. Organisations need to be allocating more investment and resource to cyber security not decreasing it, as the strongest possible level of protection is more important than ever," says Anthony Young, Director at Bridewell Consulting.

HYGOOD

Stop fires. Not hard drives.

Acoustic Nozzles

For suppressing fires in hazard areas where sound levels from standard nozzles may affect sensitive electronic equipment.

For more information visit hygood.com

The power behind **your mission**

Johnson Controls

Paul Norbury
Founder and Chief Executive, Cardwave
www.cardwave.com

Passwordless authentication to gain traction in 2021

2021 SHOULD BE THE YEAR that passwordless authentication really takes off. Analysts Gartner predict that by 2022 60% of large and global enterprises and 90% of midsize enterprises will implement passwordless methods in more than 50% of use cases. Away from predictions, Microsoft has said that more than 150 million people are now using passwordless authentication every month. This number can only grow as organisations realise the security and cost benefits passwordless authentication brings, and individuals warm to its ease of use - essentially that they no longer need to remember passwords and enter them manually.

From passwords to handsfree

Passwordless authentication comes in various forms. Many people are already familiar with fingerprint readers on their phone or laptop, and with face-based login such as that provided through Windows Hello. While these methods are efficient and effective, they tie an individual to a single device. More exciting – and much more useful for the corporate and public sectors – are systems which allow an individual to authenticate themselves on any computer. Most compelling of all are systems which achieve this hands free, authenticating a user just because they are nearby.

This technology exists, and is already being used. It frees people from needing to remember passwords, and enables them to use whatever computer they happen to be near to continue with their work.

Think of the healthcare sector, where practitioners might log in to different computers tens of times a day in order to access or update patient records, and consider the time saved if they just automatically get logged in when they approach a computer they want to use.

Not only can this free up literally hours of practitioner time every day, it allows the practitioner to focus on the patient, not on tapping a password onto a screen or keyboard. At Iron Country Medical Center, for example, the team of 20 is gaining 75 to 95 minutes every day. All the practitioner needs to do to make this happen is to carrying their login token. This can be as simple as a small fob on a keychain.

As well as allowing people to log in to a computer seamlessly, passwordless authentication systems can ensure each person is given the right level of access to information, so that data security within the organisation is ensured. And, because passwordless authentication is proximity based, when someone moves out of range, they are automatically logged off, eliminating data security risks.

The end of 123456

For more years than I care to remember research that shows how bad we are at managing passwords has passed across my desk at regular intervals. When the National Cyber Security Centre released what it had learned about passwords already known to hackers I was unsurprised to discover the most frequently used password was “123456” and other common passwords included “123456789”, “qwerty”, common first names, Premier League football team names and, that most easily guessed password of all, “password”.

It is difficult to blame individuals for this situation. I know as well as anyone how hard it is to think of a strong password, and how much harder it is to remember that. I also know that no system should ever allow a numeric sequence to be a password – but clearly they do.

The good news is that even for large corporate organisations passwordless authentication need not be expensive or difficult to put in place. In these times of working from home the back-end technology can be configured remotely by technical teams, and any required proximity equipment (such as a key fob token) delivered to the user by courier to ensure its security. From then on administration, such as permissions management, is handled remotely. As organisations begin to realise this during 2021, we may finally see the back of “12345”.

Further information from Cardwave’s specialist division Secure Drives **https://www.securedrives.com**

Fermin Serna
Chief Information Security Officer at Citrix
www.citrix.com

Remote work is here to stay

AT THE OUTSET OF 2020, remote work was something most companies were experimenting with. But mid-way through the year, things got serious as COVID-19 began to spread and mandates forced the masses to work from home. While many companies viewed remote work as a short-term solution to the pandemic problem, they are now realizing that it is here to stay. Research shows that over three-quarters of more than 3,700 IT leaders in seven countries believe most workers will be reluctant to return to the office post pandemic. And they will need to revamp their security policies to support them as they work from anywhere.

There will be no perimeter

Three years ago, everything was on prem and the security perimeter was defined by firewalls. Today, applications and services are rapidly moving to the cloud, people are working from anywhere and the perimeter has all but disappeared. Corporate information security teams will no longer rely on traditional, VPN-based strategies to provide access. Instead, they will shift to a Zero Trust model that uses contextual awareness to adaptively grant access based on user behaviors and access patterns.

Experience will influence strategy

In a recent survey conducted by Citrix and Pulse, 97 percent of 100 IT decision makers in North America, Europe, the Middle East, Africa and the Asia Pacific region said employee experience is a key influence on their security strategy. And 75 percent said they are looking to improve the user experience through their design and execution. Security teams will take an intelligent , people-focused approach to security that protects employees without getting in the way of their experience by securing all tools, apps, content, and devices they need and prefer to use in a simple experience that can be customised to fit personal preferences and evolving work styles.

Cyber actors will become more sophisticated and scale
New ways of working mean new ways of attacking corporate networks. Ransomware and other malicious attacks are on the rise, with cybersecurity researchers reporting a seven-fold increase in malware campaigns at the mid-point of this year. Flush with cash from their demands, bad actors, have been empowered to scale their operations. And they will. Attacks will continue and become more sophisticated and dangerous.

Security will get smarter

As attackers get smarter and scale, security will get smarter and more creative as well. Machine learning and artificial intelligence will deliver real-time insights into user behavior and access patterns, and security teams will use them to automate the process of identifying security incidents, atypical activity and policy violations and defend across gaps.

Vendors will get a closer look

The data chain is longer and more complex than ever And with the perimeter gone, companies need to think beyond protecting their own systems and data and closely monitor all third-parties with whom they interact, as all it takes is one weak link to create a breach.

With corporate brands, customer trust and business continuity at stake, security teams will place more scrutiny on their vendors and select only those who meet the highest standards for data privacy and protection.

CISOs will become more agile

Companies are rapidly moving to simplify and shift things to the cloud. And CISOs are adapting to secure the new environment. But ten years ago, there was no cloud. And five years from now, there will be something else. CISOs will become more agile in adapting to changes as technology evolves in 2021 and align closely with business leaders to provide a secure environment that fuels innovation and growth.

Companies are rapidly moving to simplify and shift things to the cloud. And CISOs are adapting to secure the new environment. But ten years ago, there was no cloud. And five years from now, there will be something else.

Looking ahead at a time when things have never been more uncertain may seem like a futile exercise. But there are lessons to be learned today that can help shape a better tomorrow. Just like work, cyberattacks can happen anywhere, anytime. And in order to successfully protect the systems and information people need to get things done, wherever they happen to be, security organisations need to become more intelligent and flexible. In doing so, they can create the secure environments needed to keep employees engaged and productive and fuel innovation and business growth.

Ryan Weeks
CISO at Datto
www.datto.com

Healthcare and homeworking

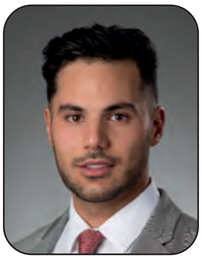
Healthcare organisations need to remain on red alert in 2021
Given the COVID-19 pandemic, it's no surprise that the healthcare industry has been a primary target for cybercriminals in 2020. Between highly desired intellectual property and the opportunity for major payouts, the in centive to exploit even the smallest of healthcare institutions, let alone larger networks, will remain a top priority for malicious actors in 2021. Specifically, ransomware will be the primary attack method because the consequences are higher for healthcare organisations that can't risk down time due to the critical services they provide for patients. It will be critical for hospitals and other healthcare organisations to evaluate their IT and security budgets ahead of the new year to ensure they're able to implement advanced security and data management tools that allow them to effectively back up and secure networks while enabling business continuity efforts in 2021.

We'll see an increase in insider threats as employees continue to work from home:
An insider threat is defined as current employees, contractors and visitors who have access and knowledge of an organisation's digital and physical systems as it pertains to security and information. There are two types of insider threats, malicious insiders who are, on their own accord, deliberately exploiting the systems within an organisation for monetary compensation and then there are colluding insiders who are potentially being forced to, or paid to, share information or execute illegal acts. I believe that in 2021, we will see an increase in insider threats, specifically the colluding insider, because it's easier for employees to get away with suspicious activity.

For example, an employee making a £34,000 salary could be lured by a cybercriminal to execute an attack in the form of installing software or providing access to information by a promised pay out of just under £200,0000. This is a pretty low risk for a large pay out. We're seeing a rise already in 2020, which is why I believe we'll see more of it in 2021.

Cybersecurity predictions for 2021

The team of cybersecurity experts at DigiCert gathered to debate and formulate their list of 2021 cybersecurity predictions. This team consisted of (from left to right) **DEAN COCLIN**, Senior Director of Business Development; **AVESTA HOJJATI,** Head of R&D; **TIM HOLLEBEEK,** Industry and Standards Technical Strategist; **MIKE NELSON,** VP of IoT Security, and **BRIAN TRZUPEK,** SVP of Emerging Markets Product Management at DigiCert.



Prediction: Social engineered attacks will get more complex
According to Verizon's Data Breach Investigations Report for 2020, social engineering is a top attack vector for hackers, and we expect threat actors to leverage current events to unprecedented levels. Consider the following:

- **Unemployment fraud:** With unemployment fraud at an all-time high, we will see an even larger increase in 2021 as pandemic-focused unemployment programs from governments have lowered the barriers to collecting benefits, and security methods have not been able to keep up. Should we see additional stimulus funding from governments to provide relief for the effects of the pandemic, this will only make this a richer channel for fraudsters.

- **COVID-19:** Free COVID-19 tests will be leveraged heavily by threat actors in the New Year. Scammers will utilize social engineering to dupe users into providing a mailing address, phone number and credit card number with a promise to charge 25 cents to verify their information and qualify for a free COVID-19 testing offer.

- **More COVID:** The offer of fake, "government-approved" cutting edge technologies to fight COVID and take the temperature of those in proximity will trick users into downloading malicious apps on their smart devices that can be leveraged for nefarious activities by threat actors.

- **Tax deadlines:** With the fluctuation of tax filing deadlines in 2020, expect threat actors to leverage this to their advantage in 2021. Phishing around tax season will drastically increase.

Prediction: The "New Normal" will be under attack
We predict that individuals and businesses alike will adjust to a new normal sometime in 2021. This new normal will result in an increase of travel, a reduction in unemployment, and a transition for workers to return to the office, leading to threat actors' attacks on the following:

- **Travel:** Fraudsters looking to take advantage of the new normal will target vacation-starved travellers looking for good deals online or via email. Phishing attacks will be the tool of choice and will be leveraged successfully by fraudsters.

- **Back to the office:** As workers return to the office, there will be a steady crescendo of applications offered by threat actors with the promise of increased productivity tools to ease the transition to the office. Tools such as apps that provide ambient sounds will be leveraged in these attacks. Expect new attack vectors to emerge not only for social engineering, but also attacks targeting common home devices that are used at home for workers splitting time working at home and the office that can be used to compromise an individual and allow for lateral movement into a business. Workers splitting time between the home and the office will only exasperate this transition period, causing confusion and an increase in security risk for business.

- **Data Breach News:** News of data breaches will increase in 2021 as the public learns of exploits on companies that haven't done a good job securing their remote workforce. (Avesta Hojjati, Dean Coclin, Mike Nelson)

Prediction: 2021 will bring increased focus on automation and efficiency solutions in the security market

- As organizations work to keep the lights on and scrutinize the bottom line, there will be a resulting push for efficiency in security technologies.

- Security teams will be asked to do more with even fewer resources. 2021 will bring an emphasis on technologies that allow organizations to do more with less, and automation will play a significant role in terms of security innovation in the New Year. According to a 2020 SANS Automation and Integration Survey, 12% of respondents had no security automation in 2019. In 2020, that dropped to 5%. We predict the level of automation in 2021 will increase exponentially.

- A consolidation of security vendors will take place in 2021 as businesses look to reduce the number of vendors within their environments. Trusted vendors with leading global technology and local resources where their customers live will be valued, as will be their emphasis on automation of security tasks. (Avesta Hojjati)

- As security investments focus on immediate value, Quantum Computing will continue to move forward. We will see the effect of Moore's law on Quantum Computing. As Quantum Computing allows for tasks to be more efficient, organizations will prioritize its continued development. Improvements and efficiency are recession-resistant. (Tim Hollebeek)

Prediction: Staying safe online:

Identity and consumer accountability of their permissions and controls over their data will lead to a new interest in how to stay safe online and with connected devices. Concerns over contact tracing and other government invasions of personal privacy will lead to a new desire by the public for ways to identify organizations with which they connect online and for better assurances of the security of the connected devices in their everyday lives, including connected cars, homes, buildings, websites, emails, etc.

Predictions 5-10 years in the Future:

Always looking to exceed expectations, our experts also looked beyond 2021 and into their crystal ball for the next 5-10 years for what security innovations will await us.

- **Holographic teleconference to minimize travel:** Each generation brings a new technology which "shrinks" the globe. In the early part of the 20th century, steam ships allowed people to make trans-Atlantic crossings in about a week. Then propeller airplanes shortened it to two days (with stopovers). Once commercial jets became viable, the same trip which took one week on a ship took less than 10 hours on a plane. With the advent of the Internet and email, instant communication was made possible. Fast forward to today, where everyone is using video teleconference tools to communicate, which have in many cases, eliminated the need to travel. In the next 10 years, expect holographic teleconference or sophisticated telepresence devices, where participants can view others in 3D without the need for special glasses. Holographic projectors located on the back of cameras will project the image in front of you, which will give a more lifelike experience to conferencing. This will further reduce the need to travel across the globe to meetings. To make this a reality, a backbone of high speed, secure communications pathways will be required. In addition, on the hardware side, a migration to higher capacity processors and higher resolution cameras and projectors will be needed. For the software, codecs that can operate in 3D with the appropriate encryption controls are a must. While this technology will start with businesses, it will easily expand to consumer use cases as families will be able to "visit" each other using this holographic method. (Dean Coclin)

- **Data privacy:** The data "given away" by the current generation of children in the home will come back to haunt this generation in the future, inspiring a new generation to carry infosec securely into the future. Children being forced into online learning at home will instill in some a discovery and passion for technology. This newfound passion for technology among this virtual learning generation will inspire new technology and security solutions and will inspire a new generation of innovators. The generation growing up now will have a tremendous impact on the careers they choose in the future. (Mike Nelson)

Simon Eyre
MD & Head of Europe, Drawbridge
www.drawbridgepartnersllc.com

Cybersecurity in 2021 What can we expect?

WHEN THE WORLD HEALTH ORGANIZATION declared COVID-19 a pandemic, organizations across the globe had to adapt and change the way they operate, fast. As we changed the way we work, cybercriminals followed because the modern criminal is constantly evolving in line with shifts in online behavior and trends. As we prepare to welcome 2021, what trends can we expect from the cyber world?

The 'working-from-home economy' will increase demand for sophisticated cybersecurity technology

Working from home has become a critical weapon in our fight against COVID-19. However, remote workers also provide an opportunity for skilled cybercriminals. In 2021, we can expect cybercriminals to finetune their attack strategies and adapt to the "work-from-home economy", pursuing remote workers even more so than in 2020. Unmanaged home machines will become targets, and, in turn, these easily compromised machines at home will become the pivot point to home-bound corporate devices allowing advanced persistent attacks.

As a result, we can expect to see a continued decline in the use of VPN technology as a trusted extension of the corporate network, and cybersecurity technologies will continue to move away from the edge and network applications into endpoint protection.

These changes are likely to cause a spike in demand for technology that was once reserved for trained cybersecurity staff, and cybersecurity providers will respond to the change. Businesses will begin to converge and offer software solutions for the changing workplace, launching more sophisticated technology into the market. Services such as web-filtering, intrusion detection and more sophisticated endpoint protection will grow in the consumer market. Amid the ongoing cybersecurity skills gap, there will also be an increased demand for corporate cybersecurity staff and experts.

'Security and privacy by design' will be put at risk, as criminals continue to target the health and financial industries

The rapid deployment of technology in the health sector to manage track-and-trace programs, vaccine logistics, mobile

applications and other activities will lead to examples of software not adhering to the 'security and privacy by design' philosophy. This deviation will likely be the cause of large-scale privacy breaches putting patients and their data at risk. Coupled with ransomware, we may see the first government held to ransom by criminals demanding payment for decryption or making data leak threats.

In addition to this, as the pandemic triggered a spike in online banking, we can expect a rise in phishing, spoofing and impersonation attacks on consumers and businesses. Schrems II will continue to affect multi-national technology firms In July 2020, the Court of Justice of the European Union invalidated the EU–U.S. Privacy Shield and confirmed the validity of the EU Standard Contractual Clauses.

This was for the transfer of personal data to processors outside the EU/EEA in Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (called "Schrems II").The Schrems II decision means that the EU-U.S. Privacy Shield framework is an inadequate mechanism to guarantee compliance with EU data protection requirements.

This will have a knock-on effect on privacy rulings and requirements among countries. In 2021, we will continue to see multi-national technology firms affected by these privacy rulings, and an increased need to strengthen privacy protections and invest in more sophisticated cyber security measures.

For criminals, ransomware is king

Cybercriminals are motivated by money, so for as long as it is economically beneficial to them, ransomware cases will continue to rise. Today's criminals are creative, capable, and opportunistic, so they will carry on expanding their repertoire of ransomware techniques. In 2021, ransomware attacks will include not just a demand for organizations to pay a ransom, but threats of data being exfiltrated and leaked.

These double-threat attacks will reduce the mitigation ratings of disaster recovery and business continuity for protection against ransomware in most risk assessments. As organizations will be tempted to pay the criminals, governments must crack down on those who pay money to criminal entities on sanctioned lists.

Jenn Markey
Product Marketing Director at Entrust
www.entrust.com

Remote working: The year of digital identities

A RECENT PwC study indicated that 85% of employees wish to work from home at least one day a week after working from home during the pandemic and 55% of surveyed executives planned to offer the ability to work from home to staff in response1. The leadership team at Entrust envisage that the surge of remote working will continue around the world due to the nature of global restrictions and the traditional way of working has fundamentally changed and has already introduced a hybrid working model that we expect many companies to adopt in 2021. At Entrust eligible employees can already elect to work remotely for 2 days a week and the coming year will see this sort of way of working become the norm as centralised offices become less important to the day to day operations of organisations around the world.

A new age of balance between digital and physical work environments that accompanies the normalisation of hybrid working models will usher in widespread usage of identity authentication as temporary measures put in place during the pandemic are replaced with secure alternative systems.

Allowing staff members to securely access organisation networks and materials with robust identification methods will be the focus of IT security teams for the coming year and is integral to a business model with a high level of flexibility. The use of tools like identity proofing, originally designed for consumers to safely access online accounts, will rapidly grow in popularity to facilitate the onboarding of new and existing remote employees.

Creating a secure digital identity for a remote workforce will require the issuance of mobile and digital credentials to access company resources from anywhere in the world as businesses move away from traditional identity authentication methods like passwords. It will become an increasingly rare occurrence to see physical badges and smart cards used to access systems and networks as employees work from increasingly diverse geographical locations. Credential based authentication with proximity-based logins will mitigate the risk of less secure home office environments and generally enhance the security capacity of a majority of organisations and businesses.

2021 will also see that digital identities will also be increasingly used in a widespread improvement in digital security for collaborative working tools and platforms that have required investment and attention for some time. Verifying identities for online meeting attendees will be a part of enterprises' increasing demand for more security controls that may also include approving secure networks to facilitate confidential meetings that require a higher level of security or enforcing the use of headphones. In addition to that level of control leaders will look more than ever for efficiency from digital tools leading to the accelerated adoption of cloud platforms and security infrastructure like Public Key Infrastructure. Historically only a priority for larger enterprises in the coming year businesses of all sizes, from SMEs to corporations, will invest in efficiency and security technology but the challenge will be reshape network security, access management and data protection in ways that empower employees and enable productivity and efficiency rather than hinder it.

Our digital and physical worlds will continue to converge until it is impossible to discern where one starts and the other ends. Central to navigating this new reality is your trusted digital identity. Ultimately, you won't have one identity for work, one for mobile banking, another to travel, and so on. The future is one trusted digital citizen identity that can be used everywhere.

By Mike Campfield, VP, GM International and Global Security Programs at ExtraHop

Ransomware will change and stay the same

In 2021, we see new strains of ransomware as attackers continue to profit. We will also find new gangs entering the picture and continued development of attack tactics. Following the trend of recent years, Ransomware will set its sights on ever higher value targets in healthcare, institutions of education and financial services. The more things change, the more they stay the same - the essential threat of ransomware is no different. Enterprises will develop workarounds to resist paying the ransom, ransomware continues to be the greatest threat to enterprises. We expect 2021 to produce new victories in the long ransom war.

The future of remote workforce brings new security headaches

Now that workers and employers have benefited from remote work, they're going to demand it from their employers. In 2021, remote work will cement its place as a standard part of working life and create a new raft of considerations for enterprise security. How will an enterprise protect their network if endpoints are employee owned constantly on and off the corporate network either from home or in the office. How are enterprises going to protect themselves without the benefit of enterprise security controls? In 2021, the fact of long term remote work is going to force us to rethink how we secure enterprise data and infrastructure.

By Ronnen Brunner, Vice President of EMEA Sales at ExtraHop

Hybrid and Remote work will be here to stay

The global pandemic has made remote work an absolute necessity. Given its clear benefits - remote working is likely here to stay in full or at the very least in a hybrid form. Employees love the added flexibility and employers benefit from the increased satisfaction of their employees and the reduced costs associated letting go of expensive office locations. But this new state of being involves a radical change in traditional enterprise IT infrastructure and security. In 2021, enterprises will reap the benefits of remote work, but grapple with how to protect this new architecture which will be heavily cloud/SaaS based.

The need for cloud and hybrid security will increase as enterprises drop on-premises data centres

In 2021, we'll see an increased need for cloud and hybrid

security as more enterprises migrate from the on-premises data centre to cloud environments. That sort of digital transformation had been trending for years, but the pandemic forced massive migrations at a previously unheard-of pace.

Now that they have experienced the benefits of expanded cloud use, expect more enterprises to leave behind traditional on-premises environments. Capital One bank closed all their on-premises data centres in favour of cloud deployments, and Deutsche Bank is also moving heavily moving to the cloud. These are early indicators of what we can expect in the coming year, and 2021 will see enterprises grapple with what it means to upend their traditional architectures and effectively protect their environment through what may be a long transition period.

Niche cloud tools go extinct as businesses are forced to cut the fat

The pandemic solidified cloud's role as a key pillar of the modern enterprise. Think of working over the last several months without AWS, Slack, or Office 365! Yet despite cloud's seeming ubiquity, cloud security remains a remarkably nascent, highly fragmented market. There are specific tools for containers, for SaaS apps, for each major IaaS provider, etc. But with COVID-19 forcing strict budget cuts, there will be intense pressure in 2021 to significantly consolidate IT and security toolsets.

Niche solutions like CASB and CSPM will soon go extinct as the most forward-looking organisations will invest in higher-value, more encompassing cloud security tools that enable detection and response across the entire hybrid environment.

Economic Downturn leads to cuts to IT

The projected economic downturn may mean deep cuts for Enterprise IT. The UK's Chancellor of the Exchequer Rishi Sunak has recently announced that the UK economy will contract by 11.3%. That means that IT departments may soon experience punishing cuts as enterprises tighten their belts. 2021 will likely mean that IT priorities will have to be re-evaluated and IT security will need to find ways to do more with less and do it quickly - the question on CISOs minds will be how to be leaner and more efficient when it comes to protecting the enterprise.

Safi Raza
Director of cybersecurity, Fusion Risk Management
www.fusionrisk.com

Cybersecurity - what to expect in 2021?

2020 WITNESSED a seismic physical, economic and cultural shift among global organizations, as businesses adapt to working during a pandemic.

When COVID-19 brought sweeping changes to the way we operate, communicate, and do business, cyber criminals were in the wings waiting to seize any opportunity they could to exploit security weaknesses for monetary and disruptive gains. In light of this, we've experienced a sharp rise in cyber-attacks across a range of industries including healthcare, education, and ecommerce. Today's cybercriminal is constantly evolving to take advantage of online behavior and trends – the COVID-19 pandemic is no exception to this.

So, what will cyber criminals bring to the table in 2021? How do organizations ensure they have the appropriate cyber security strategy in place to mitigate ever changing and evolving cyber threats?

The rising risk of remote working

Today the majority of organizations have a remote workforce, and many employees are relying on personal devices to conduct work – this method of working is not secure. Why? Remote employees are sharing the home network with smart TVs, phones, tablets, and various IoT devices that are not adequately secured. The exchange of highly sensitive and confidential information that once occurred behind the fortified infrastructures is now being conducted from fragile home networks.

For the modern CTO this situation is a not ideal. As home working cyber related risks will only become greater during the next year, CTOs and their teams are relentlessly exploring avenues to help mitigate the cyber risk. In 2021, organizations will need to spend more time and money on endpoint security and end-user training.

AI is the future of cybersecurity

The massive and sudden increase in the number of people working from home has furthermore validated the role of artificial intelligence (AI) in the future of cybersecurity. Unlike traditional security solutions, AI does not depend on known signatures. Instead, it relies on user and attack behavior analytics and network traffic analytics, quickly neutralizing a threat before it becomes a crisis.

Phishing is the most commonly known threat countered by the use of AI. Microsoft and Google already use AI to detect spam and phishing emails. Several cyber security companies including Rapid7, Dark Trace, Barracuda, and Palo Alto, are using AI-powered SIEM, firewalls, and a variety of other applications to ensure organizations remain secure.

The implementation of AI and Machine Learning helps us identify attacks by being able to analyze and predict attacks in real-time. In 2021, we will see much more of this as organizations invest in avoiding cyber-attacks, before they become a threat.

Ransomware becomes a greater threat

Cybercriminals follow the money, so ransomware cases will continue to rise. After all, criminals will use a tool for as long as it is effective. In 2020, many hospitals and health care facilities were victims of ransomware. In fact, the Cybersecurity and Infrastructure Security Agency, FBI, and Department of

Health and Human Services recently warned that there is a “an increased and imminent cybercrime threat to (specifically) US hospitals and health care providers.”

The extortion techniques are changing too. For example, a recent hack of a mental health services provider, Vastaamo, resulted in hackers contacting the patients and threatening to release their therapy notes and other data unless a sum of 200 Euros was paid. For any organization, whether a business or a hospital, the freezing of its digital systems threatens customer and patient care, creating urgency to pay up and recover. For as long as it is monetarily viable, ransomware will continue to be a top threat for many years to come.

Social engineering - the dangers of deep fakes

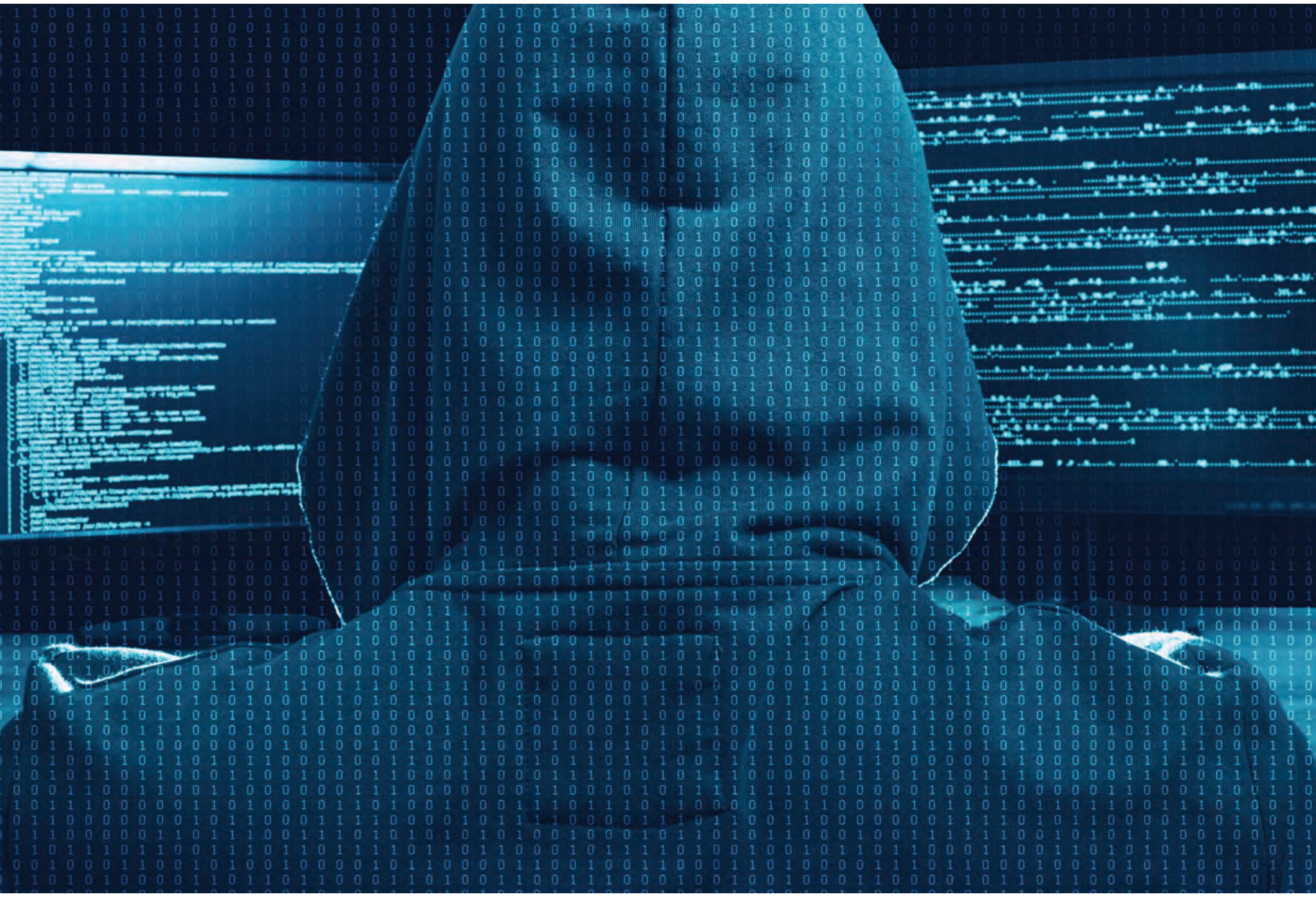
Human beings are the weakest link in the cybersecurity chain. As more defensive technologies integrate with artificial intelligence, it is becoming increasingly difficult for bad actors to compromise network boundaries. Because of this, there is an increase in reliance on social engineering. Deep fakes are a newer social engineering tool in a hacker’s arsenal. ‘Deep fake’, which is a term for audio or video recordings that combine existing information and develop it into a new image, video, or audio recording, can be pooled with existing tactics to cause maximum damage.

For instance, imagine an organization’s accounts payable employee receiving an email from the CEO regarding the transfer of funds, followed by a CEO’s phone call. People tend to be cautious with the email as they may be aware of phishing techniques and learned about them in security awareness training but receiving a phone call from an executive of the company makes it less suspicious. Deep fake tools are easily accessible online. An open-source program named Avatarifyn superimposes someone else’s face onto the user’s face in real-time, during video meetings. The code is available on Github for anyone to use. The lack of effective deep fake detection technology attracts many bad actors to use deep fakes and this threat will only become stronger in 2021.

Third party risk

The cyber incidents caused by supplier negligence are increasing at an alarming rate. The infamous 2013 Target hack was successful because hackers compromised the HVAC contractor and used stolen access details to infiltrate Target’s infrastructure. The incident cost Target over $300 million. Organizations must implement an effective third-party management program to ensure periodic validation of confidentiality, integrity, and data availability.

2021 is set to be more challenging than ever as cyber criminals adopt increasingly sophisticated ways to break into organizations’ IT systems. It is vital that employees follow strict IT security policies, whether they’re working in the office or at home. It only takes a simple error or lapse in judgement to create a large scale, highly damaging cyber-attack.



Cyber-attacks set to become more targeted in 2021, according to HP Inc.

Cybersecurity predictions for 2021 show the ripple effect of COVID-19 is likely to continue, leading to a rise in thread hijacking, whaling and human-operated ransomware

HP has released its 2021 predictions on how security threats – such as human-operated ransomware, thread hijacking, unintentional insider threats, business email compromise and whaling attacks – are set to increase in the next 12 months.

HP's cybersecurity experts including – Julia Voo, Global Lead Cybersecurity and Tech Policy; Joanna Burkey, CISO; Boris Balacheff, Chief Technologist for Security Research and Innovation at HP Labs; Dr. Ian Pratt, Global Head of Security for Personal Systems; and Alex Holland, Senior Malware Analyst – and experts from HP's Security Advisory Board – Justine

Bone, CEO at MedSec; and Robert Masse, Partner at Deloitte – all gave their predictions for the year ahead.

Weakened organizational security will lead to more unintentional insider threats

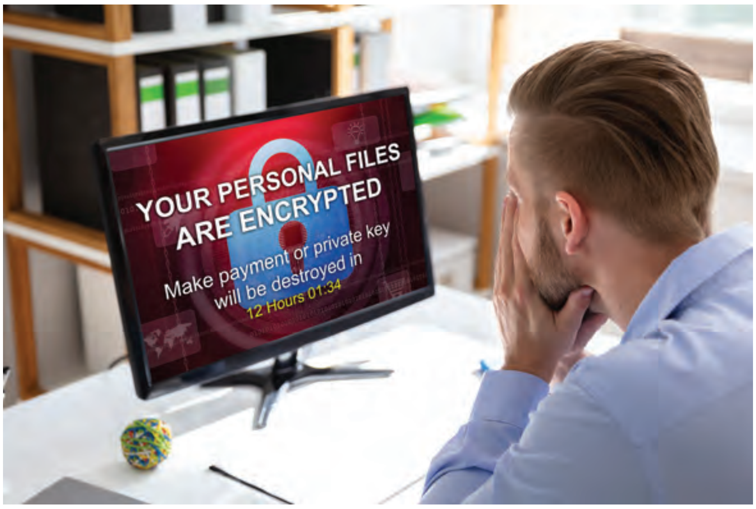
The dramatic changes to how we work in 2020 and the shift to remote working will continue to create challenges, says Julia Voo: “COVID-19 has weakened organizational security. Remote access inefficiencies, VPN vulnerabilities and a shortage of staff that can help the business adapt means data is now less secure.” From a cybercriminal’s perspective, the attack surface is widening, creating more opportunities, as Joanna Burkey explains: “We can expect to see hackers identifying and taking advantage of any holes in processes that were created, and still exist, after everyone left the office.”

Boris Balacheff points out that this also means that home devices will be under increased pressure: “We have to expect home infrastructure will be increasingly targeted. The scale at which we operate from home increases the incentive for attackers to go after consumer IoT devices and pivot to business devices on the same networks. And as we know, if attackers are successful with destructive attacks on home devices, remote workers won’t get the luxury of having someone from IT turning up at their door to help remediate the problem.”

Burkey also believes there will be more unintentional insider threats: “With employees working remotely, the lines between work and personal equipment are blurred, and innocent actions – such as reading personal email on a company machine – can have serious consequences.” Overall, the pandemic has increased the risk of employees making errors, as Robert Masse explains: “If you view the pandemic as a war experience, then organizations will be dealing with employee burnout. This can lead to an increased risk of errors in judgement.”

Human-operated ransomware attacks will remain an acute threat

Ransomware has become the cybercriminal’s tool of choice, and this is likely to continue in the year ahead, comments Burkey: “What we’ll see is a rise in



ransomware-as-service attacks where the threat is no longer the ‘kidnapping’ of data – it’s the public release of the data.”

The rise of ransomware has fueled the growth of an ecosystem of criminal actors who specialize in different capabilities needed to pull off successful attacks. Malware delivered by email, such as Emotet, TrickBot and Dridex, are often a precursor to human-operated ransomware attacks. “To maximize the impact of an attack, threat actors use their access to compromised systems to deepen their foothold into a victims’ networks. Many crews use offensive security tools to gain control of a victim’s domain controllers, which are often the best point in a network to deploy ransomware,” explains Dr. Ian Pratt.

This trend is of particular concern to those in the public sector, as Alex Holland explains: “The rise of ‘double extortion’ ransomware, where victim data is exfiltrated before being encrypted, will particularly hurt public sector organizations, who process all manner of personally identifiable information. Even if a ransom is paid, there is no guarantee that a threat actor won’t later monetize the stolen data.”

Greater innovation in phishing will see thread hijacking and whaling attacks

In 2021, there will be more innovative phishing lures designed to trick users and make attacks harder to

HP’s cybersecurity experts including, from left to right: Julia Voo, Global Lead Cybersecurity and Tech Policy; Joanna Burkey, CISO; Boris Balacheff, Chief Technologist for Security Research and Innovation at HP Labs; Dr. Ian Pratt, Global Head of Security for Personal Systems; and Alex Holland, Senior Malware Analyst – and experts from HP’s Security Advisory Board – Justine Bone, CEO at MedSec; and Robert Masse, Partner at Deloitte – all gave their predictions for the year ahead.

identify. “The most innovative mass phishing technique we see is email thread hijacking, which is used by the Emotet botnet. The technique automates the creation of spear-phishing lures by stealing email data from compromised systems. This data is then used to reply to conversations with messages containing malware, making them appear very convincing,” explains Dr. Ian Pratt. We can also expect to see more of these attacks targeting individuals working remotely, says Justine Bone: “Thanks to everything relying on strong authentication, as opposed to in-person presence, there is more opportunity for hackers to engage in social engineering to trick employees into divulging credentials.”

The prospect of continued social isolation has encouraged people to share more personal information online, which cybercriminals can weaponize. “Whaling, a form of highly targeted phishing attack aimed at senior executives, will become more prominent with cybercriminals able to take personal information shared online to build convincing lures leading to business email compromise fraud,” comments Masse. Many of these phishing emails will continue to exploit people through fear, according to Voo. “New fears will be used to drive people to open malicious emails – whether it’s COVID vaccines, financial concerns related to the lockdown and any political instability.”

> The prospect of continued social isolation has encouraged people to share more personal information online, which cybercriminals can weaponize

Hackers will tailor attacks to target specific verticals – in particular, critical infrastructure, pharma and healthcare, Industrial IoT and education

One of the most at-risk verticals in 2021 will be healthcare. “Healthcare has been a perfect target – society depends on it and these organizations are typically under-resourced, change-averse and slow to innovate. Education also fits this criterion and could be another prime target,” says Bone. However, this threat extends beyond hospitals and doctor’s surgeries into more critical areas. “Due to the race to develop a new vaccine, pharmaceutical companies and research facilities will also continue to face adverse risk,” comments Masse.

But the next 12 months will also see other targets come into consideration for hackers. “Car makers, particularly EV companies, will become bigger targets as they grow in prestige and profitability, and we can also expect to see critical infrastructure and the Industrial Internet of Things continue to be in hackers’ crosshairs,” explains Masse.

Zero trust is here to stay, but needs to be implemented in a way that is transparent to the user

Zero trust as a concept isn’t new, but the increase in remote working means that it is now a reality that organizations need to accept. “The traditional ways of securing access to the corporate network, applications and data are no longer fit for purpose. The perimeter has become obsolete. Over the years the workforce has become more dispersed, and SaaS adoption has risen – this means critical data is being hosted outside the enterprise firewall. The time has come for organizations to start protecting against the unknown, which means utilizing zero trust, but in a way that is transparent to the user,” comments Pratt.

COVID-19 will be a key driver behind zero trust adoption and also means we’ll see greater innovation in this area. “Zero trust is the best defensive approach for enabling remote working, but for identity and access management to be seamless it needs to be easy to use. Quality authentication methods are a key enabler of zero trust, which is why technologies such as biometrics will be expected by end users in the future,” comments Bone.

A new approach to security is needed

“2020 demonstrated that is has become critical to manage highly distributed endpoint infrastructure,” comments Balacheff. “Organizations need to accept that the future is distributed. Everything from remote workers’ devices to industrial IoT devices have become the new frontlines of the cybersecurity battleground in our increasingly cyber-physical world.

To meet this challenge, organizations need to re-think their security architectures and controls, and embrace the necessary innovation in technology and processes to help them support this new environment.

For example, modern hardware technology exists that can help not only protect but also recover employees remotely and securely in the face of destructive attacks like those we have seen in the last few years.”

“Organizations face a huge security challenge in the year ahead, with cybercriminals becoming savvier about how to extract the most value out of victims,” comments Ian Pratt. “Relying on detection alone will only result in an unsatisfactory outcome for the organization, so a more architecturally robust approach to security is required; one that builds protection in from the hardware up. Hardware-enforced technologies like micro-virtualization are transparent to the end user – this means they can click on email attachments and download files as they normally would, but are safe in the knowledge that if anything is malicious, it is rendered harmless. This protection-first approach leaves hackers with nothing to steal and no way to persist, helping organizations to deal with the variety of threats 2021 and beyond will throw at them.”

Oliver Obitayo
Chief Sales Officer at IDnow
www.idnow.com

Identity verification – predictions for 2021

AFTER POSSIBLY the most turbulent ever year for business, many organisations have faced unprecedented trading conditions all over the globe, IDnow's CSO, Oliver Obitayo, discusses what he expects 2021 to bring to the identity verification market and the industries it supports.

Moving onboarding process from compliance to competitive advantage

For many years, the onboarding process, including Know Your Customer (KYC) requirements, has been viewed as an unavoidable necessity in order to remain compliant. Unfortunately, many firms underestimate the importance of this process and view it in too narrow a context. For example, comparing identity verification providers based purely on price rather than thinking more broadly about the process and the overall experience it offers potential customers is a missed opportunity in terms of added value.

Consumers expect a frictionless onboarding process and this can be the difference between converting a prospect or not. Businesses are increasingly realising the power beyond the process, with many seeking verification providers that understand the customer as well as the KYC regulatory landscape.

As such, I expect many to switch onto the concept that onboarding can actually offer a competitive advantage, where customers are put at the heart of the onboarding process and where KYC becomes a much broader business topic, even in the boardroom.

Rise of consumerisation

Consumers have come to expect a seamless online experience, even more so this year since the pandemic drove the entire world to their smartphone or laptop and this consumerisation megatrend has now hit onboarding processes and KYC.

Most end users expect all processes they encounter to be available in an App, instantly granting them access to the service or product they demand. To remain relevant, firms must fulfil this expectation and with that, comes a need for hardcore technology that will deliver compliance and security.

I expect this consumerisation to continue to grow as more and more customers switch their lives and interactions with businesses online.

Embedding and improving existing technologies

Covid-19 has significantly accelerated global digitalisation – experts suggest by as much as five to eight years. Many industries and businesses have had to quickly adapt and pivot in order to retain their share of the market, placing huge pressure on firms to implement technology in order to deliver this digital, remote experience.

Thankfully, technology innovation has been the main driver of the identity verification market for many years, enabling the sector to meet the significant rise in demand with speed and efficiency. In our recent Security Report, we reported significantly higher demand for our products and services as restrictions around Covid-19 continue to push digitisation. There was a strong increase of 250% in fraud attempts this year, with new developments in identity fraud heavily impacting the global cybercrime figures.

Our order intakes rose by 358% year-on-year, while transactions via IDnow AudoIdent grew tenfold, with an increase of 1,000% in the number of transactions recorded between January and June 2020.

For 2021 then, I expect to see a focus on embedding and improving some key technologies that make the identity verification market as secure as it is. Priorities will be enhancing the use of Artificial Intelligence and sophisticated technology in order to drive automation and detection of dynamic security features in ID documents. In addition, Machine Learning, biometric face recognition, 3D modelling, wallet and reusability and integrated electronic signatures (eIDAS standard) processes will be improved.

I also predict the development of a global identity verification platform that caters to the different KYC client needs within multi-geographical, multi-regulatory frameworks in order to maximise conversion, fraud prevention and user experience in a compliant way. Ideally, this would be delivered by a single provider.

Evolving regulatory landscape

With the rise of cybercrime and identity theft, more and more countries are updating their regulatory frameworks more frequently, and often making them much stricter. The rules surrounding Anti-Money Laundering are also expanding to cover more industries. This evolving regulatory landscape will become increasingly complex, not least when the UK leaves the European Union on 31st December 2020.

As such, I expect firms to become much more reliant on their identity verification providers to offer the highest level of regulatory compliance, regardless of their geography or sector.

Market proliferation

As already discussed, Covid-19 has really driven growth in demand for online services and as a result, firms are increasingly seeking secure and compliant identity verification partners.

I see this demand only increasing in 2021 with more multi-jurisdictional regulations, dramatic uptake of remote business models and contactless processes, all of which drive the need for onboarding and KYC processes backed up with secure identity verification from established providers with pan-European operations.

Emerging markets and passing geographical boundaries
We are predicting a substantial increase in the need for online identity verification across many new geographies and industries next year as manual processes are replaced by automated alternatives. Opening bank accounts from home in a compliant, secure and convenient way via an App or web; signing contracts in a legally binding manner or renting cars within a couple of minutes have already become the norm for many.

Industries such as travel or hospitality will introduce automated, digital ways to onboard and engage with their passengers/guests; eHealth and using a true electronic patient record will become the norm; the financial industry will continue to further optimise their frontends, but also better integrate backend processes seamlessly. Meanwhile, governments and insurance firms will need to become more digitally available, as they face an urgent need to verify and know their customers.

With all these various trends and developments, the market for identity verification providers serving only one or two verification methodologies and regulatory environments is closing. Sectors and organisations the world over will increasingly seek a one-stop shop for best and seamless identify verification for the new normal. Which is why we are transforming into a global identity verification platform provider, which continues to add a broader range of products and services to its offering.

> With the rise of cybercrime and identity theft, more and more countries are updating their regulatory frameworks more frequently, and often making them much stricter. The rules surrounding Anti-Money Laundering are also expanding to cover more industries

Keith Glancey

Systems Engineering Manager, Europe at Infoblox

www.infoblox.com

When it comes to cybersecurity in 2021, organisations should plan for the worst and hope for the best

CYBERSECURITY is an ever evolving industry that is required to react to new threats on a daily basis. 2020 brought fundamental changes to the way we live and work, expanding the threat landscape as a result, and this story of uncertainty is expected to continue into the New Year.

So, what are the biggest cybersecurity threats and trends for enterprises in 2021?

COVID-19 and Brexit will create the perfect storm for data privacy issues in 2021

The combination of COVID-19 and Brexit has created the perfect storm for data privacy issues in 2021. Cybercriminals are exploiting the vulnerabilities brought about by the pandemic, both at an organisational and individual level, whilst Brexit will put a question mark over data sovereignty laws that is likely to linger well after the December 31st cut-off.

The uncertainty of what is to come could mean mayhem for IT teams in charge of data protection, and it's that very uncertainty upon which cybercriminals thrive.

From a legal standpoint, organisations need to be especially cautious about where they're holding their customer data and be ready to adapt once new regulations have been laid out. When it comes to security, the newfound chaos will mean investing in solutions that are going to protect data in network environments that are increasingly de-centralised by expanding security to the edge to accommodate the explosion of end-points outside the traditional security perimeter.

Trust nothing in 2021, until proven otherwise

Zero Trust won't remain just a security methodology for access management, unfortunately, in 2021 it will become the default stance of consumers and organisations alike when it comes to cybersecurity. From the rising number of cyberattacks to fake news and wild conspiracy theories, 2020 has made us warier than ever.

It wasn't long ago that employees connected their laptops to the corporate network via an Ethernet cable at their desk inside an office block. First, we expanded to services like Office 365, making online remote-work possible – a game-changer at the time. Today, the network edge has moved, and on top of a large percentage of the population working from home, everything from Tesla cars and warehouse security cameras are sending information back to an organisation's network. The corporate network is no longer just HQ, it's everything connected to it, too.

Firewalls and VPNs will no longer be fit for purpose in a remote working economy

In a time where an organisation's work doesn't begin and end at the revolving office door, traditional firewalls and VPNs that

protect the core network still have a place in corporate security networks, but the surge in remote workers has increased the load on those traditional methods and move the requirement for secure connections to the edge of the cloud.

As network activity shifts further and further towards the edge, new risks across DNS, DHCP and IPAM (otherwise known as DDI) have opened up. Despite all we've learnt about securing the network in 2020, these weak points are still being overlooked by security teams.

Organisations need to be looking at cloud-managed DDI to give them more visibility into network activities across their extended networks and simplify management complexities. This will give security across every device on the network, anywhere in the world.

The benefits of cloud-native security solutions will be realised
Cloud computing is now a given, but the path to the cloud is still paved with challenges. A common option is to 'lift and shift' your IT infrastructure into the cloud, but this doesn't take full advantage of what the cloud can offer. Instead of picking up an on-premise solution and copy + pasting it into the cloud, it's cloud-native solutions that will offer the real benefits organisations need in order to compete at scale. What does this mean for security? Well, cloud-native solutions that use Docker and Containerisation don't carry the same legacy baggage. They're lightweight apps that allow you to pinpoint problem areas and fix them in isolation. This makes remediation times for security flaws much faster and more efficient. Cloud-native security solutions allow organisations to resolve security issues without taking down the entire system – meaning increased uptime and less strain on resources, two things that are particularly important given rising consumer demands for always-on services mixed with the increased attack vectors we'll see in 2021.

No matter what next year brings, companies will need to stay vigilant. Political changes are likely to impact privacy issues and maintaining trust is going to be absolutely critical for organisations. Protecting employees while working remotely will continue to be imperative and cloud-native security solutions will be fundamental in resolving security issues. Whilst the world is hoping for calm waters ahead, if cybersecurity has taught us anything over the years, it's to plan for the worst and hope for the best.

> cloud-native solutions that use Docker and Containerisation don't carry the same legacy baggage. They're lightweight apps that allow you to pinpoint problem areas and fix them in isolation

Evgeny Goncharov

Head of ICS Cert, Kaspersky

www.kaspersky.co.uk

ICS threat predictions for 2021

Random infections

- Infections will tend to be less random or have non-random follow-ups, as cybercriminals have spent the past several years profiling randomly infected computers that are connected to industrial networks or have periodic access to them. Access to such computers will be — and is perhaps already being — resold to more sophisticated groups with specific schemes for monetising attacks on industrial facilities already in place.

- For several years now, various groups have specialised in attacks against industrial enterprises with the express aim to steal money — through BEC schemes or advanced hacks to gain access to victims' financial and accounting systems.

Through years of criminal operations, they have come to understand the business processes of industrial enterprises and gained access to a large amount of technical information about network assets and operational technologies. We expect to see new and unconventional scenarios of attacks on OT/ICS and field devices, coupled with ingenious monetisation schemes. Cybercriminals have had more than enough time and opportunities to develop them.

Ransomware attacks

- Ransomware is becoming more technically advanced and sophisticated. Cybercriminals will continue to employ hacker and APT techniques, painstakingly exploring and probing the network of the target organization to locate the most valuable/vulnerable systems, hijack administrator accounts, and launch simultaneous blitz attacks using standard admin tools.

- Cybercriminals have developed a fondness for industrial companies, because they tend to pay ransom. This means that the attacks will continue.

- There will be hybrid attacks involving document theft with the threat to publish the documents or sell them on the darknet in case of refusal to pay up.

- The ideas implemented in Snake for ransomware attacks targeting OT/ICS will gain traction.

- It is highly likely that we will see attacks disguised as ransomware but pursuing completely different goals — a repeat of the ExPetr technique.

Cyberespionage

- Cybercriminals will figure out (some already have) that inside the OT perimeter secrets are not guarded as well as in office networks and that OT networks may be even easier to break into, since they have their own perimeter and attack surface.

- The flat network topology and other access control issues in OT networks can make them an attractive entry point into the

> For several years now, various groups have specialised in attacks against industrial enterprises with the express aim to steal money — through BEC schemes or advanced hacks to gain access to victims' financial and accounting systems

intimate recesses of the corporate network and a springboard into other related organisations and facilities.

- The desire of many countries for technological independence, alongside with global geopolitical and macroeconomic upheaval, means that attack targets will include not only traditional opponents, but also tactical and strategic partners — threats can come from any direction. We have already seen examples of such attacks.

APT

- The number of APT groups will continue to grow — we will see more and more new actors, including ones that attack various industrial sectors.

- The activity of these groups will correlate with local conflicts, including those in the hot phase, with cyberattacks on industrial enterprises and other facilities used as a warfare tool, alongside drones and media-driven misinformation.

- In addition to data theft and other piecemeal operations, some group is likely to get down to more serious business in 2021, perhaps in the vein of Stuxnet, Black Energy, Industroyer and Triton.

COVID consequences

- Against the backdrop of economic decline, lockdowns, slower growth and ruin for small businesses, the ranks of cybercriminals are sure to swell as skilled people seek alternative employment, and groups associated with national governments will strengthen as well.

- The online presence of municipal services and utilities and the increased digitisation of government and public services will make them more vulnerable to attacks of cybercriminals and create more opportunities for cross-agency attacks and assaults on central and local government functions and the systems that support and implement them. For example, a threat actor could use a governmental or municipal web service as an entry point, compromise the victim's internal infrastructure and use the communication channels and supply chain connecting various governmental, municipal and even private organisations to reach their final target (such as shutting down transportation systems).

- Restrictions on on-site work, which prevented new equipment from being installed and configured, have slowed down the efforts of many industrial enterprises to beef up their perimeter security. Together with the increasing number and variety of remote sessions, this may even reduce the level of perimeter protection of industrial networks. This being the case, the safety of industrial facilities will largely depend on the performance of endpoint solutions and the security awareness of employees. At the same time, cyberattacks aimed at industrial companies are maturing. As a result, despite the currently observed drop in attacks on OT/ICS computers, the number of serious incidents is not going to decrease.

- The reduction in on-site personnel who are able to promptly transfer systems and installations to manual control in the event of a successful cyberattack on the industrial network could facilitate the wider spread of malware and lead to more severe consequences.

Ilia Sotnikov
VP Product Management, Netwrix
www.netwrix.com

The security gaps of pandemic-driven fast fixes will manifest next year

IN 2020, organisations across the globe, in every industry, were forced to quickly adapt to new ways of working and implement new technologies, with little experience and nearly no time for planning and testing. While this enabled many of the world's employees to carry on working from their homes, we have also seen a rise in the number of cyber-attacks partly driven by bad actors spotting gaps they can take advantage of.

As head in to the new year, we will undoubtedly experience unintended consequences of many of this year's fast fixes, including hackers innovating old attack methods for new types of attacks, which will in turn drive changes to how businesses respond to attacks and security as a whole. As such, here is how I envisage the development of security over the next 12 months:

- The rapid digital transformation in 2020 will have a delayed impact on cybersecurity in 2021.

In 2021, the security gaps caused by the inevitable mistakes during this rapid transition will be exploited, and we will see new data breach patterns like the recent Twitter hacks.

- Ransomware causes increasingly substantial damage to encourage payments.

The next generation of ransomware will aim to do damage that is more difficult to recover from, forcing organisations into paying the ransom. One example is "bricking" devices by modifying the BIOS or other firmware. Cybercriminals will also be expanding to new targets, such as operational technology and IOT devices. These attacks may have a much more visible impact on the physical world, so they will become more common as more of these devices are deployed and the industry standardises on communication protocols.

- Hackers will increasingly target service providers.

Lack of internal cybersecurity expertise and talent will lead organisations to turn to managed services. In response to this

increased adoption, hackers will conduct targeted attacks on MSPs – for example, by compromising the credentials of contractors – in order to get access to the provider's customers.

- Cloud misconfigurations will be one of the top causes of data breaches.

The rapid transition to cloud applications required to support remote work without a proper understanding of the shared responsibility model will backfire in 2021. Add in the high pressure IT teams are under and their lack of time to learn about the new infrastructure, and misconfigurations will be inevitable, resulting in overexposed data.

- Cyber security and business will be more aligned.

The challenges of the pandemic will force organisations to reassess their priorities. In particular, IT teams will have to find the right balance between security and business needs like flexibility and accessibility. Expectations will shift from ensuring unrealistic 100% security to determining and meeting acceptable levels of risk and resilience.

- Proof of value will drive business conversations.

Cybersecurity will be on the agenda at many board meetings. Executives will be looking for specific metrics to prove the value delivered by the products the company has purchased and the efficacy of the security measures that have been implemented.

A practice when IT leaders have to justify the necessity of new investments and demonstrate that money is not being spent in vain will become more generally accepted.

- Insurance and legislation will drive mass adoption on f fundamental security practices.

2021 will see both new privacy laws and stricter enforcement of existing regulations. To minimise the risk of incurring steep fines for compliance failures, businesses will turn to cyber insurance. However, those policies will come with their own security standards and requirements, such as regular risk assessment and effective detection and response capabilities.

As a result, organisations will be equally focused on meeting those criteria as much as they do on complying with the regulatory standards themselves.

This year has certainly catalysed the world's reliance on technology to go about their daily lives, greatly increasing the associated security risks. The good news is that we hope to see organisations implementing real changes – whether that's incident or legislation-driven – and 2021 will solidify cybersecurity's rise on the agenda to ensure a safer world for everyone.

In 2021, IoT security issues will come to the fore

As more workers continue working from home, their personal IoT and smart devices will become a greater threat to their company's corporate security problems.

Marc Rogers, VP of Cybersecurity at Okta

WE ALL USE these devices to automate our lives, entertain ourselves, and monitor our health, which has become an extremely fast-growing market. Sports devices now offer medical-grade sensors, allowing users to track where they go and how their heart and body perform. Very few people who actually use or even create these devices, however, have truly thought about where their data goes, how it's managed, and how it's secured. These devices' lax data policies call to light how vulnerable we are, and yet companies continue to develop similar technology for houses, cars, and cities.

Throughout 2020, few device manufacturers or security researchers have paid nearly as much attention to this issue as they have to software vulnerabilities. Consequently, most IoT hardware has very weak to no protections against attacks aimed at prying secrets from device firmware. The issue with all of these systems, and indeed all IoT devices, is that most proprietary information about the device – including certificates, keys, and communication protocols – is typically stored in poorly secured flash memory. Anyone with access to an IoT device and some basic knowledge of hardware hacking can easily access the firmware and look for data, including vulnerabilities that could potentially allow them to launch attacks against similar devices without requiring physical access.

In 2021, we'll see IoT begin to mature from a security standpoint, with new frameworks and policies emerging worldwide that could force manufacturers to embed at least some level of security into devices out of the box. The UK offers a "secure by design" program, the US Senate has unveiled a bill specific to IoT, and countries like Australia and Malaysia are creating an IoT framework.

These all cover common themes: devices must not have weak default passwords, devices must be patchable, manufacturers must support them, and manufacturers must have bug programs. While this is great news for 2021 and beyond, there are still millions of devices left behind - and the new year signals a new opportunity to support policies that better protect IoT devices. It also gives enterprises the opportunity to implement a security approach that protects against these blind spots.

Ultimately frameworks and policies make for progress, but not a silver bullet; the massive explosion of IoT will continue to accelerate and continue to be one of the largest security risks faced by both consumers and enterprises.

Business investment in security will spike as security culture becomes mainstream

Ben King, Chief Security Officer EMEA at Okta

SECURITY CULTURE is becoming more mainstream as businesses and consumers are continually faced with increasingly sophisticated cyberthreats. Cybersecurity threat awareness has grown significantly this year, particularly following a number of public high-profile cybersecurity incidents. This is leading to a complete shift in how organisations think about, and consider their approach to the threat landscape.

A recent Okta report this year found that less than a third of office workers were completely confident that the remote online security measures implemented by their employer would keep them safe from cyberattacks, with just 4 per cent saying they weren't confident at all. 2021 will see more of a security-focussed mindset at leadership level, as the C-suite clamps down on this lack of confidence.

In 2021, investment in security is sure to leap up as security cultures become more established, and as businesses recognise the cruciality of effective frameworks.

Due to the shift to remote work, employees will be learning first-hand what Zero Trust security means, becoming familiarised with new authentication methods and making a more conscious and collective effort to end "password-only" security. There will be a drive for education from the top down to ensure security is integrated across all levels of employees, as remote workers are the front line and must be switched on to risk. For end users, there will be a greater understanding about the dangers of poor security hygiene, triggered by more regulation and a general improved awareness of the value of our data. We're already witnessing a cyberthreat gold rush, and with that, the increased sophistication and diversification of threats, such as deepfakes.

While deepfake visual technology is not currently at the stage of fooling the majority, deepfake audio is already incredibly convincing, but awareness of this is lagging.

As soon as next year, it could be nearly impossible to distinguish what is real and what is not, and the frequency of attacks will increase. As deepfake attacks continue to proliferate, we will start to see pressure build for a more defined and centralised infrastructure to set out how businesses can deal with the rise in threats. In the UK, where specific legislation does not exist, pressure will mount on platforms themselves to help stop the spread.

As this pressure increases, we're likely to see some conflict arise as to what legislation might entail and how best to stamp down on deepfake attacks on a global and local scale.

There's so much to talk about when it comes to security

Ping Identity experts give their views on security in 2021 and beyond

Andre Durand, CEO of Ping Identity

- "AS A DIGITAL SOCIETY, we are facing a privacy reckoning and a crisis of confidence — and we'll see it come to a head in 2021. The level of data collection by tech companies has reached a new peak, and consumers are losing faith in service providers' ability to manage their data respectfully. 2021 will be the year that consumers demand more control of their personal data and how it's used and shared. The identity security industry, specifically, will evolve to address this demand with new 'personal identity' frameworks that give consumers control over their identities and which attributes to share with service providers. By allowing people to pick and choose specific data and identity attributes to share with apps, and giving them the capability to validate their identity without revealing more than necessary, we'll put an end to the status quo of giving up excessive amounts of personal data to do basic tasks in our everyday lives."

Robb Reck, CISO, Ping Identity

- More and more companies will transition their consumers to a passwordless experience. This trend will pressure others to invest in smoother customer user experiences just to keep up.
- We will see a number of high profile breaches due to unsecured integrations to business critical SaaS apps. Security focus will turn in that direction.

From left to right: Andre Durand, Robb Reck, Emma Maslen and Baber Amin at Ping Identity

- Zero trust went from a buzzword to a strategy in 2020. In 2021 this will accelerate, with CISOs creating their own zero trust strategies, instead of adopting them from vendors.
- After the horrible ransomware impacts in 2020, in 2021 combined efforts between government and industry will significantly decrease the effectiveness of ransomware attacks.
- Based on the continued decline of malware over the past five years (based on 2020 VDBIR), attackers will be pushed to more sophisticated attacks to defeat MFA. Enhanced authentication techniques will be critical against that threat.

Emma Maslen, VP & GM of EMEA & APAC, Ping Identity

- The biggest lesson I see for 2020 is the need that employees need to be enabled for a greater level of remote working support in the future. What this year has shown is that companies need to be agile with their strategies to ensure business keeps moving in uncertain times, with no disruption to service for employees and customers.
- I see a couple of challenges descending on us for the future which Ping can really address.
- The first is where we work. The pandemic has created a greater dependence on home working, whilst we may have some employees who return to the office in the future - some employees are now enjoying the reduction in commuter, more family meal times and greater flexibility in the working day which I think they will be reluctant to let go in the future. Ensuring our employees are enabled to work from home, in a productive way, will be a big theme for the future?
- Why that is, brings me to a second point - the war on talent. This war continues. As the world is disrupted, employees are looking for visions, missions which resonate and working environments which empower employees to do their best. Frictionless access to tech will ensure reductions in frustrations and attract and keep the best talent.
- Identity is going to be a big consumer focus in the future. Not only are we working from home more - we are shopping from home more. Users/ consumers are bombarded with username and password requests, identity challenges and a friction-ful experience which results in high basket abandonment to our besieged retailers. For companies to ensure their maximum share of wallet they must replace legacy experiences and disrupt their environments. The frictionless experience for consumers will drive loyalty and a larger share of wallet. Those focusing on those challenges will be the winners of 2021, certainly in retail, insurance, banking and many other sectors.
- I don't think we are yet seeing the sort of fines expected as a result of GDPR. The intent was good by the regulators, the risk is real for consumers and customers, and yet we are not seeing that many public exposes or fines.
- Cybersecurity inherently carries a negative connotation. But there are so many positives. If we think about what cybersecurity enables..... frictionless online experience = greater baskets completed = higher revenues = greater customer spend / loyalty...

Baber Amin, CTO West, Ping Identity

- A greater focus on privacy as more services are provided digitally.
- Greater focus on securing remote workers using modern tools and moving farther away from centralized command and control.
- More sophisticated deepfake attacks and use of AI on both sides i.e. red team and blue team both will leverage AI.
- A backlash against remote work, remote learning, as creativity and innovation decline.

> The pandemic has created a greater dependence on home working, whilst we may have some employees who return to the office in the future - some employees are now enjoying the reduction in commuter, more family meal times and greater flexibility in the working day

Nigel Thorpe

Technical Director at Secure Age Technology

www.secureage.com

It's time to focus on the data

Nigel Thorpe, Technical Director at Secure Age Technology looks at some of the predictions that should come true in 2021, but probably won't

AFTER A TUMULTUOUS YEAR, 2021 should be a year for the cyber security industry to take stock and change the way it has always done things. We need to stop trying to prevent unwanted access to IT systems and data, because it's simply not possible to keep all the cyber criminals out, all of the time. This has been exacerbated over the course of 2020 because the remote, hybrid office, now provides more soft points of entry into the corporate network. As a direct result of this mass move home, the attack surface has got bigger, while at the same time, the insider threat has been extended as third-party service providers who have greater access to data and systems.

For too long, the traditional methodology has been for organisations to add more layers of defence, or just accept the inevitable and have incident response plans and procedures in place in order to recover and pick up the pieces. While this won't change overnight, hopefully 2021 will mark a change of mindset.

Can we trust Zero Trust?

Adding defence layers and building as many micro-perimeters with authentication and access controls is valid still, but if a cybercriminal – insider or external – gains user access, then data is there for the taking. Relying on full disk encryption on a running system is about as useful as a Secret Santa.

What should happen is that security is built right into all data using file-level encryption. Only this approach ensures that even if stolen, data remains protected and unusable by the cybercriminal. This is the simplest solution that gets to the heart of the problem without disrupting the way people or applications work. However, this extension of Zero Trust into the data is unlikely to happen because of the belief that more doors and more monitoring will keep data safe.

Home IoT devices as back doors to the corporate network
The growth of connected devices, from smart light bulbs to digital assistants can give cybercriminals access to home networks as IoT security is still woeful and has not kept up with the expanding use of devices. This isn't going to change any time soon. Once in, the jump to an employee's laptop and into the corporate network is relatively easy. Even trusted technologies for securing remote workers such as multi-factor authentication (MFA) and Virtual Private Networks (VPNs), do not defend against a cybercriminal who has hacked their way onto the home PC.

All data will be considered equal

Cybercriminals aggregate data stolen or purchased on the dark web to build personal profiles for identity theft. This means all data is a security risk and should be protected. But the traditional approach is to only protect and encrypt the 'important', sensitive data – so called data classification. According to Ponemon, 69% of respondents say discovering where sensitive data resides in the organisation is the number one challenge in planning and executing a data encryption strategy. And 32% say classifying which data to encrypt is one of the major hurdles. So, if this is the top concern, why not just encrypt everything? If it's simple and seamless – why wouldn't you?

Don't rely on everyone being a security expert

While more of us recognise a suspicious link or email attachment, it's still too easy to click on something that releases ransomware or other malware and no amount of education will eliminate this risk. Most organisations still rely on the 'human firewall' to block malware; a dangerous gamble. The better approach is behave like the nightclub doorman - if you're not on the list, you're not coming in.

Time to focus on the data

All these weaknesses could become irrelevant if we stopped just trying to prevent access to the data we want to protect and make sure that security is built into the data itself. This ensures that even if it is stolen, it remains worthless and unusable by the cybercriminal. No data, no ransom.

Dave Waterson
Founder & CEO at SentryBay
www.sentrybay.com

Adopt a uniform security posture or face devastating breaches in 2021

ANYONE WITH ANY SENSE would steer clear of predictions following a year in which a virus came seemingly out of nowhere and changed the entire face of the world. Those of us in the cybersecurity industry are accustomed to foreseeing the likely impact of computer viruses, but nothing could have prepared us for COVID-19. Except, of course, the utter predictability of cyber criminals using it for their own malicious ends.

What can be said with a degree of certainty is that threats in relation to the pandemic are unlikely to ease, working from home (WFH) is likely to continue, and as a result, corporate organisations will face the ongoing battle against the threat of unmanaged endpoint devices well into 2021.

This threat has been well publicised ever since enterprises were quickly forced into lockdown in March. Employees using endpoint devices such as laptops, smartphones and home PCs with inadequate security opened the gateway to the corporate network, and with it, the risk of data being stolen. Even now, employees are being enticed by cleverly worded emails, purporting to be from management, to activate malicious code hidden in attachments. There is one attribute of criminals that we have seen over the years, and that is they will be very creative in exploiting all possible angles in new emerging situations. We may see criminals exploiting other members of a WFH household, such as children, in order to gain access into mum or dad's corporate network.

As threats become increasingly sophisticated and more carefully targeted, so regulatory authorities will have to become more stringent in enforcing protection mechanisms. One of the biggest issues is the widespread adoption of cloud technologies to better facilitate WFH. What regulators will need to figure out is how best they can adapt regulations to ensure that the home environment is protected to the same degree as the office environment. We can expect changes in this regard sooner rather than later.

Where is the threat coming from?

One trend that has been growing over recent months is the exposure of smaller enterprises to a level of sophisticated cyber-attack that was previously reserved for large multi-nationals. Often less well protected, these organisations have previously escaped the attention of cyber criminals and have been just secure enough to fend off standard threats. With the move to WFH, use of unmanaged endpoints has revealed chinks in the corporate armour and attackers are quick to sense the opportunity and act on it. This is exacerbated if employees are geographically dispersed, and for many organisations they are ill-equipped to deal with breaches of this nature in the current climate.

The greatest threat in 2021 will come from key logging and screen-grabbing malware. This is because these are the attack vectors through which sensitive data is most often, and most easily, stolen. Both make use of endpoint devices to gain access to networks and data and neither two-factor authentication or standard anti-virus solutions are sufficient defence. Keylogging, along with spyware, is widely ranked as the top cyber threat to businesses. It works by covertly installing malware to record keystrokes which can later be used to steal sensitive data (such as PII or sensitive corporate data), passwords and log-in details.

It is possible that we will face further lockdowns of different degrees, which means that smaller enterprises must learn from previous experiences and take security measures that match the threat they face. Back in March, all too many organisations thought that a virtual private network and an off-the-shelf AV or EDR security solution would be sufficient to protect their remote workers from a data breach, but evidence suggests that this was not the case.

Adopt a uniform security posture

The aim should be to ensure that any unmanaged device that accesses the corporate network has the same security posture as managed devices that reside within the corporate perimeter. This requires the use of solutions designed specifically to protect data entry on BYOD and unmanaged devices, particularly into remote access apps like Citrix, VMWare, WVD, web browsers and Microsoft Office applications. Browsers that access the corporate network should be locked down, including URL whitelisting, enforced certificate checking and enforced https.

> It is possible that we will face further lockdowns of different degrees, which means that smaller enterprises must learn from previous experiences and take security measures that match the threat they face

To conclude, we predict challenges ahead when it comes to securing data and ingenious but highly damaging cyber attacks designed to get around the smallest vulnerability. If unmanaged endpoints continue to have access to corporate networks, breaches could rise by as much as 40% and companies will face failure. This is not scare mongering; it is the consequence of not taking the cybersecurity threat seriously enough.

From left to right: Erik Kristiansen, Adrian Beck, Chris Pick and Thomas Stanley, at Tanium

Tanium's 2021 predictions

The Endpoint: How will the role of the endpoint evolve in the coming year?

THE ENDPOINT is the network. Zero Trust, remote work and cloud all come together to invalidate investments in network equipment. Organisations will move to make the internet their networks and to deploy architecture and new technology to solve for security and management on untrusted networks. -
Erik Kristiansen, Senior Director, Product Marketing

If COVID-19 continues, we will continue to see the network fragmented and endpoints more at risk through legacy tools not being able to effectively secure and manage those endpoints. Attackers will have a greater attack surface with widely distributed endpoints and each one potentially outside of the existing control frameworks of corporate networks, meaning higher likelihood of malware, phishing attempts and other security events. The risk profile will increase dramatically and security teams will be blind to much of it. If COVID-19 dissipates, endpoints will start returning to traditional network boundaries. In this scenario, we will see an uptick in unpatched, infected and insecure machines. IT teams will have their work cut out, in either scenario.
Adrian Beck, AVP of Customer Success

"Digital transformation has been a topic for years, but it took a global pandemic to push organisations to make it a reality. Nearly overnight, we've had to support thousands of distributed employees, shift to cloud or SaaS-based technologies, and reimagine how we engage with our customers, partners, and employees in a remote-work environment. In 2021, companies will lean in even further by giving employees the freedom to live and work from anywhere, which will make endpoint visibility and control an IT imperative."
Thomas Stanley, Chief Revenue Officer, Tanium

Legacy technology:

What legacy technology will die? What new technology will emerge to fill a need?

The EPP market will be solved by Microsoft. Microsoft will continue to develop native controls and protective mechanisms that will solve for the bulk of the attack vector at the endpoint. However, it won't be enough. Breaches will continue to impact organisations both large and small. The industry will realize they need IT first responders who are embedded into the rhythm of the incident response process with rapid response remediation tools.
Chris Pick, CMO, Tanium

Antivirus becomes a commodity within an overall unified endpoint security (UES) approach. With the move to Zero Trust networks, organisations will have to refocus on visibility, hygiene and endpoint hardening to maintain security. More organisations will leverage existing entitlements to Windows Defender versus paying for third-party AV solutions.
Erik Kristiansen, Senior Director, Product Marketing

Continued drive to optimise both cost and efficiency will see niche point solutions struggle to justify their presence on the endpoint. IT leaders will begin to consolidate onto core endpoint platforms, like Tanium, improving the end user experience, simplifying workflows internally and reducing cost and overhead. Any solution that only addresses a small fraction of the overall needs of IT security and operations will be under threat.
Adrian Beck, AVP of Customer Success

Tools consolidation and a need to get back to basics started this year, but the work is far from complete. -
Chris Hallenbeck, CISO of the America

One of the lasting legacies of 2020 will be the distribution of workforces. Now that organisations and employees know that they can go remote, many will stay that way. Now that the shock of the transition has faded, CIOs in particular are starting to think about how you do IT when there are no corporate networks and when the need for remote access isn't limited to a select few employees. 2021 is going to be the year when CIOs really figure out how to take IT to the

employee, empowering them with knowledge, tools and access that keep them connected and productive while limiting risk for the organisation.
Chris Pick, CMO, Tanium

The challenges of 2020 showed that VPNs and on premise centric solutions are long past their sell by date; a massive bottleneck preventing workforce agility and mobility. Not to mention VPN infrastructure being a significant target for hackers in 2020.
In a world of highly distributed employees with unpredictable working patterns on premise centric IT management and security tooling that saturates VPN links just doesn't make sense. Businesses shouldn't have to choose between securing their systems and business productivity - as many have been forced to. Expect to see the continued adoption of Zero Trust platforms and cloud based management solutions to support enterprises move to hybrid and multi-cloud computing relegating the VPN to niche requirements
Oliver Cronk, Chief IT Architect, EMEA

The distribution of endpoints and the exposure they face every day will do away with traditional vulnerability practices. A monthly scan will no longer suffice. IT teams will need to create continuous vulnerability and configuration practices to ensure compliance and security.
Pete Constantine, Chief Product Officer, Tanium

5G:

5G impact on endpoints?

We've seen with WFH and school from home that connectivity is king. Every day I get new fliers in the mail from the major carriers for cellular broadband for my house - the ultimate cord cutting! However, ubiquitous connectivity doesn't just provide opportunity for legitimate users, it also gives bad actors a leg up. From a business perspective, it provides challenges and opportunities for the teams that have to maintain these new endpoints.
Chris Hallenbeck, CISO of the Americas

5G will drive exponential growth in data. We'll see more devices added over the next five years than we have in the time leading up to 2021. While businesses and consumers will jump to have connected everything, CIOs will need to figure out how to scale their technology stack from supporting thousands of endpoints to managing millions of endpoints. Very few technology providers today can handle that scale.
Egon Rinderer, Global VP of Technology and CTO, Tanium Federal

Risk

Customers, board of directors and mandated regulation will force companies to look at their risk and truly assess the cost of not doing anything. Technology providers will need to up their offerings to create tools that allow for a real-time view of an organisation's risk with assigned values and benchmarking measures.
Pete Constantine, Chief Product Officer, Tanium

The Role of Data

It feels like a lot of companies are becoming data companies -- yet what are we doing to harness the learnings from all that data? How will this change in 2021?

In IT ops and security the role of accurate data becomes paramount. With emerging technologies for AIOps and XDR, IT teams will realize they must improve data quality in order to realize the value of machine learning.
Erik Kristiansen, Senior Director, Product Marketing
Data fatigue or death by data could be a growing concern. Managing, consolidating, analysing and acting upon data is now more important than ever. IT leaders may begin to question why the breadth and depth of data is needed and who is using it. Companies will begin to strip back their data sets to leverage on the most important aspects in decision making. The rest can be seen as redundant, and in that sense, a cost to the business. Again, Covid has changed the focus. Knowing what you have and where it is at all times is perhaps more important than the variety of data you have access to.
Adrian Beck, AVP of Customer Success

What role will big data play in 2021 that's new/different?

The role of big data continues to grow in both Ops and Security. Data quality will be a primary issue in terms of success.
Erik Kristiansen, Senior Director, Product Marketing

There is a point of view that centralized data is always ideal and while there are many benefits, there also are drawbacks, especially at scale. In a highly distributed world such as the one we live in today, organizations need to understand data has gravity. That means the more you have, the more burdensome and expensive

it can be to move it. By keeping data on the endpoint, businesses enjoy more efficiency when interacting with data, whether that's investigating a breach or understanding the health of a device; Not to mention some serious cost savings.
Elvis Greer, Senior Director of Product Marketing, Tanium

The world has changed: Distributed workforces, virtual organisations, some industries in terminal decline, the rise of AI, potentially seismic changes in the EU, US elections. All of these are drivers for companies to leverage big data to make strategic decisions to increase competitiveness, enter new markets, adjust supply chains and engage in transformational programs. Any company that does not have the right data at their fingertips, or is lost in their own data lakes, will miss an opportunity to take decisive action and accelerate ahead.
Adrian Beck, AVP of Customer Success

Data finally will come to fruition in its ability to communicate risk. Simply put, better data means a better view of overall risk. In 2021, organisations will demand technology partners help contextualize their data across common frameworks and standards and do away with the manual process behind compliance, risk and regulatory audits. By accessing real-time, accurate data, leaders will have the ability to present risks in a way that speaks to the overall business.
Chris Pick, CMO, Tanium

Sales and marketing teams are used to real-time data and insights, such as daily updates on prospects, revenue, and pipeline. IT and Ops teams on the other hand continue to work with stale data. They wait weeks or even months for information and are forced to correlate data from numerous, disparate tools and systems. In 2021, we will see an information revolution as IT and Ops teams demand access to real-time visibility and control of their network and endpoints to accelerate their ability to respond to the business." -
Thomas Stanley, Chief Revenue Officer, Tanium

Government/SLED/ Nation State Attacks

What is the top cybersecurity challenge the Gov/SLED sector will face in 2021?

Distributed workforces have impacted the Government sector as much as the commercial sector. What makes the Government different in 2021 is the sustained and impactful budget pressure. Governments have been thrown into turmoil in 2020, borrowing heavily to execute appropriate COVID-19 response programs. That may continue in 2021 and, if so, budget pressure will be more intense than ever. IT Leaders will need to strip back their spend to the fundamentals, extracting every last saving possible. This could introduce cyber security gaps for attackers to exploit
Adrian Beck, AVP of Customer Success

The spate of ransomware attacks targeting state and local governments revealed the struggle these mission critical agencies face. Partnerships between public and private industry, additional budget considerations and industry standards for risk will allow these organisations to focus on the fundamentals of IT security and make them a much harder target.
Chris Pick, CMO, Tanium

The Federal sector's biggest concern is managing and securing a remote user base. Traditionally, they locked down rights and privileges on the endpoint, creating a strong account and execution privilege posture. However, they are not tooled appropriately to provide secure connectivity nor remote management and visibility of their users. Given the continued uncertainty of the pandemic in 2021, the Federal Government needs to focus on these fundamentals for a secure, remote workforce.
Egon Rinderer, Global VP of Technology and CTO, Tanium Federal

How will the concept of Zero Trust evolve in 2021? What can CIOs/CISOs do to stay ahead?

Zero Trust is more important than ever with distributed workforces, BYOD and access to company resources from any device, any network, any time of day. Many traditional security controls are largely irrelevant now. IT leaders will begin to shape an overall Zero Trust framework by looking at the 'new normal' and trying to figure out how to apply Zero Trust principles to all combinations of information consumption and all layers of the stack -- from users through applications, devices and the network. This will be incredibly difficult to do with reduced control and budget pressures.
Adrian Beck, AVP of Customer Success

Threat Landscape

What new threat(s) will emerge in 2021?

Ransomware has been around for the better part of a decade, but it quickly became the cyberweapon of choice in 2020 as threat actors sought to take advantage of chaos, confusion and millions of employees working from home. While ransomware isn't going away, 2020 has taught us some important lessons, including the need for speed when it comes to these attacks. Good segmentation and permissions can help to stop ransomware, but there's going to be a growing focus on having a "kill switch" — something that can shut things down to stop the spread before it locks down your entire environment.
Chris Pick, CMO, Tanium

The ease with which cybercriminals can successfully execute ransomware attacks will be a catalyst for change in 2021. The current market of execution and application control solutions is broken. The industry needs a true baseline on endpoint controls, a solution that doesn't require the expertise of a small army and

provides streamlined, immediately actionable alerts.
Egon Rinderer, Global VP of Technology and CTO, Tanium Federal

Ransomware as a Service will be one of the highest impact technologies. Cybercriminals are evolving their business model to include for hire services that will target our distributed workforces and any endpoint that isn't appropriately protected.
Egon Rinderer, Global VP of Technology and CTO, Tanium Federal

All the "big game hunting" attacks we experienced in 2020 will continue to grow, with more and more targeted attacks, mostly ransomware based but also blackmail in general for data leaks and IT operations disruptions. Nevertheless, 2021 and after will also be the years where the usage of 5G & IPv6 will grow like never before. This will lead to expose connected devices more than ever and we are exposed to a structural risk of RCE vulnerabilities exploitation, more important botnets and, at some point, IOT/ICS/Mobile used in new types of intrusion sets and campaigns. - **Dagobert Levy, VP South EMEA, Tanium**

How will cybercriminals take advantage of hybrid workforces?

For years, I've been hearing from IT and security leaders about how tool sprawl is adding a huge management burden and resulting in more siloed teams and data. 2020 exacerbated this challenge and organisations moved to rapidly adopt cloud platforms to better support remote workforces — and were forced to adopt point solutions to manage those individual cloud environments. This is not a sustainable model, and as the dust settles on 2020, there's going to be a much bigger push to find platform- and environment-agnostic tools that can give security and IT leaders the big picture.
Chris Pick, CMO, Tanium

General/Cybersecurity

What's the biggest challenge facing CIOs/CISOs in 2021?
The biggest challenge now, and well into the future, is around people. CISOs are being asked to relax corporate cybersecurity policies in an effort to support a distributed workforce — one which is tired, stressed and looking at ways to juggle home/work priorities brought about by these uncertain times. Business executives are putting CISOs under pressure to relax the rules regarding device usage or network split tunnelling. The rationale is understood, but the potential repercussions aren't always considered. It's important to focus on the foundations of security such as patch management, vulnerability assessment and risk.
Chris Hodson, Global CISO

IT teams are in for a wild ride. Strategies that are typically planned a year in advance will need to evolve at least every six months, or even every quarter. Security orgs are taking a leaf from the engineering playbook and working via principles of failing fast and agile project management. Teams will need access to real-time, accurate data more than ever before to guide these shifts.
Chris Hodson, Global CISO

In 2021,CISOs better buckle up. Ransomware is transitioning from primarily targeting SMBs to hitting large enterprises. It's lucrative and, relatively speaking, easy to execute. With the explosion in poorly protected endpoints and users existing outside the protective perimeter of the enterprise, this is the year for it.
Egon Rinderer, Global VP of Technology and CTO, Tanium Federal

The latest evolution of the threat landscape associated with major changes in the digital workspace can put CIO/CISO in a difficult situation. On one hand they have to deal with more demands of WFH, new-generation practices and liberties of use, on the other hand more sophisticated threat actors. All of that is unfortunately happening while Detection / IR / Red-Teaming advanced skills could be hard to find. Challenges will be to find these skills, train them, keep them and put the right processes and tools in place without slackening the efforts on the basics.
Dagobert Levy, VP South EMEA, Tanium

How will the pandemic continue to shape or shape the tech world in new ways in 2021?

While some employees enjoy the freedom that a work from home culture gives them, there are just as many that pine for the ability to directly interact with coworkers. Watercooler conversations and a "drive-by whiteboarding session" just isn't the same via Zoom. When we're able to clear the major hurdle of an effective vaccine, there will be a push to bring teams together. It may take on a hybrid look where some work from offices all the time, while others are at home (even if in the same city as the office!) but they'll come in 3-5 days per month.
Chris Hallenbeck, CISO of the Americas

In 2021, CISOs will demand managed control planes to pull both structured and unstructured data together in meaningful ways. They need tools that can provide bi-directional information on threat vectors, IT assets and overall IT hygiene to eliminate the silos of activities across organisations. This will allow both security and IT operation leaders a new level of visibility and assurance that they are mitigating risks far better than ever before.
Chris Pick, CMO, Tanium

Cybersecurity teams will finally get the budget greenlight for scenario planning, and not just for your run-of-the-mill, annual tabletop. Teams will receive budget to run worse case scenarios like entire workforces unable to come to the office, buildings knocked off the network, or an enterprise-wide ransomware infection. Boards need to embrace the planning and shift their mindset around credible threats. While the biggest cybersecurity dangers are often linked to overlooked basics, they also can be the unlikely, unexpected scenarios such as the IT impact of a global pandemic.
Chris Hodson, Global CISO

I want to share a word of caution with leadership in 2021. Given the pandemic and a distributed workforce, teams understandably had to focus on availability and connectivity. However, don't lose sight of the other essential roles that cybersecurity plays in an organisation. Availability will continue to be important, but not more important than confidentiality and integrity.
Chris Hodson, Global CISO

If we don't close the holes around what's eating people's lunch, all the bells and whistles and next gen security products in the world aren't going to matter. Ninety percent of malware that is successful is so because we've simply not dealt with enormous swaths of fundamental security problems. AV wasn't the answer and NextGen AV won't be either. Mark my words, malware, especially that associated with ransomware, is and will continue to increase precipitously over the coming months unless we focus on the foundation of security and IT hygiene.
Egon Rinderer, Global VP of Technology and CTO, Tanium Federal

IT administrators should focus on controlling the end user's ability to do stupid things on their endpoint. User education alone is not the solution. There are controls on every single modern operating system to limit the ability of users to do things that put themselves and their organizations at risk, but they're completely unmanageable at any sort of scale. Fix that and you win the internet.
Egon Rinderer, Global VP of Technology and CTO, Tanium Federal

IT teams have tended to focus on their internal networks and perimeters in the past as only about 15-20 percent of employees were true road warriors. With our here-to-stay distributed workforce, the majority of employees will work remote. In 2021, IT teams will need to shift their focus to the edge. Endpoint management and security will be priorities as they enable employees to access company and third-party data and applications from anywhere on any device.
Thomas Stanley, Chief Revenue Officer, Tanium

Even before COVID-19 upended our planet, there was a trend toward organizations becoming less interested in owning servers, running data centres and being responsible for mission critical infrastructure to run their business -- they just wanted to run their business. Looking ahead, the SaaS market, historically targeting the small and mid-market, will become the go-to choice for enterprises of all sizes. Even companies with hundreds of thousands of endpoints will want the flexibility and scalability afforded to cloud-based technology.
Pete Constantine, Chief Product Officer, Tanium

Enterprises will need to continue to support more types of devices from employees. As the pandemic rages on, there still are companies who can't purchase enough computers for their remote workforce. This push to accept all types of BYOD will encourage more discussions around Zero Trust. And that process of not trusting anything inside or outside its perimeters elucidates a need for tools that can quickly verify all information on the endpoint.
Pete Constantine, Chief Product Officer, Tanium

Skills Shortage/Cybersecurity Hiring

How will the cybersecurity job landscape change in the coming year?

The overall cybersecurity job market will focus on automation and doing more with less. The pipeline for talent will always lag behind the demand.
Chris Hallenbeck, CISO of the Americas

The most essential consideration for an organisation that wishes to have a viable and functioning business in a highly virtual, distributed world is cybersecurity. It's outsized importance in 2020 and into 2021 as companies get their online house in order will elevate the profile of talented cybersecurity professionals. These individuals will not be job seekers— they will be sought! I also expect to see increased interest in cybersecurity programs at colleges, more robust internship programs and more + better technical training and certifications for the platform partner ecosystem.
Vanessa Black, Head of People Programs and Engagement

What should companies do differently in 2021 to attract and retain top talent?

In 2021, companies need to train their talent, treat them well, equip them for success and give them interesting problems to solve. Part of automation isn't

2021 will see partners focusing on their core competencies and looking to other partners within the ecosystem to supplement their capabilities for the greater good – of the customer and each other

eliminating jobs, it is about removing repetitive, boring tasks. Taking the boring stuff off the table still leaves a lot of engaging work for talented cyber folks.
Chris Hallenbeck, CISO of the Americas

In 2020, we all gave remote work our best shot. I've never witnessed a more thoughtful and collaborative undertaking around employee engagement, productivity and support. But 2020 is almost over, and 2021 is brimming with expectation. The slack employees gave their employers while things were getting "figured out" will lessen, and companies need to be prepared to articulate their commitment to the "future of work" based not on workarounds, but purpose-built, based on clear decisions and best practices. Companies must make explicit choices on whether they will be remote-first, what flexibility they will offer, how they will put their people first and continue to develop them in their careers. Top talent will be looking for companies who have moved past the air of uncertainty and are prepared to show up in a bigger way in 2021.
Vanessa Black, Head of People Programs and Engagement

Many organisations have recognized in recent years the need to invest in their cybersecurity capabilities. If they wish to retain the talents they use today to build or improve these capacities, they must be attentive to the implementation of the organic structure so that it does not excessively isolate the cybersecurity professions from one another. Talents should be continuously trained and organisations have to provide them with the opportunity to carry on conducting various activities in order to understand the cyber environment as a whole (red team, detection, incident response, etc.)
Dagobert Levy, VP South EMEA, Tanium

What will the workplace look like in 2021?

In 2020, kids bumping into zoom calls, impromptu introductions to family pets and a whole lot of home-cooking made our lives and relationships with each other richer. I don't think we'll ever go back to a time where we felt the need to silo these parts of our life away in the name of professionalism. In fact, I think we'll embrace a whole-person work experience even more in 2021.
Vanessa Black, Head of People Programs and Engagement

When offices finally reopen in mid-2021, we'll see a lot of renovations, more sustainable choices, and (finally!) the move away from open bullpens to intentionally designed spaces better suited for social and collaboration. This people-centric shift will create a new pull to the office, even though progressive workforces will take on a flexible posture as to where people need to be to work. The primary use case for offices will be connection.
Vanessa Black, Head of People Programs and Engagement

Every meeting that should have been an email will become an email. Zoom fatigue is real and we're finally ready to fight that good fight to become more efficient, asynchronous and respectful of each other's time.
Vanessa Black, Head of People Programs and Engagement

The Channel

How will 2021 look different for the channel? What priorities will change for the channel in the new year? How will the pandemic continue to shape the channel landscape?

Especially in the post-COVID-19 world, customers are relying on their tried-and-true relationships, making it harder for other partners to gain a foothold. 2021 will see partners focusing on their core competencies and looking to other partners within the ecosystem to supplement their capabilities for the greater good – of the customer and each other.
Cindi Johnson, Partner Program Director

The channel (SI, MSPs, GSIs) plays an even more vital role in the world we live in today and that will only amplify in 2021. With unpredictable forecasts, there is a hesitancy to hire more people yet companies need assistance to solve the new or exasperated set of challenges they are facing for both IT security and operations. This is where the channel will shine. End users are turning to their tried-and-true relationships for help, recommendations and resources to supplement or completely outsource work.
Todd Palmer, Global Head of Partner Sales

Given the remote world we are living in, it is hard for companies to establish new relationships and build trust with prospective customers and suppliers. Because of this, the channel is even more important to their vendor partners (ISVs) who are struggling to find new customers.
Todd Palmer, Global Head of Partner Sales

Barak Perelman
VP Operational Technology at Tenable
www.tenable.com

The threat to operational technology goes into hyperdrive in 2021

WITH INDUSTRIES increasingly relying on digital tools and systems to operate infrastructure, 2021 will see the cyber consequences of a world where critical operational systems are co-dependent with IT.

Universally, organisations around the globe have embraced new technologies to enhance efficiency and output, ultimately benefiting the bottom line. This digital transformation has led to the convergence, often intentionally but also accidentally, of two systems that were traditionally siloed from each other: IT systems, utilising servers, routers, PCs and switches; and operational technology (OT) that often controls critical infrastructure, which encompasses programmable logic controllers (PLCs), distributed control systems (DCSs) and human machine interfaces (HMIs) to run physical plants and factories.

What's more, the arrival of 5G in 2021 will revolutionise, but also further endanger, the OT/IT landscape. More devices will be brought online than ever before and there will be further blurring of the IT / OT border as these environments entwine.

OT in the attackers cross hairs

In the last twelve months, there have been instances of critical infrastructure falling victim from cybercriminal activity, particularly ransomware such as EKANS. According to a study conducted by Forrester Consulting on behalf of Tenable, 96% of UK organisations experienced one or more business-impacting cyberattacks, with 65% saying these attacks involved OT assets. Twenty-two percent even admitted to paying ransoms after falling victim to ransomware attacks.

A further complication is that cyberattacks that start on one side of the converged infrastructure can laterally creep to the other – from IT to OT, and vice versa.

In times of crisis, the infrastructure and supply chains that underpin modern society — agriculture, food and beverage manufacturing, pharmaceutical development – go into hyperdrive. This means that 2021 must be the year that organisations start planning for worst case scenarios to ensure the uptime and security of these critical systems now, and well into the future. Whether it be ransomware or a rogue USB, the threats to OT cannot be understated.

Plan for the worst, hope for the best

While cyber hygiene issues that have plagued IT infrastructure for years have slowly been improving, the same is not true for OT environments which are severely lagging behind, and still suffering from these age-old concerns.

Historically, OT environments had very restricted connectivity, both internally with local networks, and externally to the internet, third-party contractors and so on. Given this segregation, when the subject of security was discussed, it was typically dismissed due to the perceived 'air-gap.'

As organisations continue to connect their OT infrastructure, threat actors are seeing more possibilities to exploit vulnerabilities and exposures in legacy industrial control systems. The merging of these two previously separated environments poses a real risk by introducing even more attack vectors, while making cybersecurity threats harder to detect, investigate and remediate.

A safer tomorrow

Moving forward, there will be no OT without IT, and securing these converged environments is crucial. It's not just about protecting data, as an attack against OT systems could have physical consequences on the business infrastructure, and potentially even lead to physical harm. Since most attacks target devices rather than networks, it is also essential to utilise a solution that actively queries and provides security at the device level.

Organisations need to prioritise gaining a single view of their IT and OT environments to illuminate potential attack vectors and asset blind spots that may have eluded traditional security strategies. Since it's impossible to secure assets that you may not even know exist, having a detailed inventory of OT infrastructure that can be automatically updated as conditions change is essential to protecting industrial operations.

In 2019, over 20,000 new vulnerabilities were disclosed – yet fewer than half of these vulnerabilities actually had an available exploit. Rather than wasting time on theoretical risks, security teams should be laser focused on the threats that pose an actual risk. This is only possible with full visibility of the assets that are critical to the organisation's ability to function. Focus should be on the exploitable vulnerabilities affecting these devices and services.

The industry can also learn lessons from cloud adoption and embrace a shared risk responsibility. As data continuously flows through potentially vulnerable 5G infrastructure, it will e essential to build holistic security to close the exposure gap.

To combat new and emerging threats, this will require both users and service providers to lock arms to prioritise security measures and build an ecosystem of trusted vendors.

IT and OT teams must find common ground to eliminate the substantial risk factors of both planned and accidental IT/OT convergence in 2021. Only by getting clear and complete visibility of the attack surface can organisations identify, address and mitigate cyber risk across both their IT and OT systems next year, and beyond.

From left to right: Ed Williams and Derek Taylor from Trustwave

Trustwave trends and predictions

1. Brexit & data privacy/cyber security – Derek Taylor, Lead Principal Security Consultant at Trustwave

Ultimately the Brexit transition is likely to have an impact on data privacy because the UK will no longer be subject to GDPR unless we decide to maintain equivalence. There is an increasing direction of travel from the Conservative party towards deregulation, boosting the financial sector and not maintaining equivalence with the GDPR. In my opinion, that attitude is likely to impact data privacy as well. In essence, moving into 2021 I would expect the individual to have less control over their data and we will likely see the enablement of companies to mine the vast amounts of PII and other data in marketing intel and shadow databases. The timing is up for debate, but I really don't see that not happening.

2. Taking advantage of intellectual property – Derek Taylor, Lead Principal Security Consultant at Trustwave

What I think this year has shown in terms of attacks, is that the real focus in on intellectual property. We've seen an awful lot of news about COVID vaccines and the intellectual property associated with them. Moving forward, I think the trend here is frankly that we will see both government-level or state-level actors as well as criminal organisations and potentially even countries, seek to gain advantage through intellectual property and acquisition, and I think that's related to the fact that we're starting to see a split of the Internet around macro, political geographies. The US and China are the two big ones and Europe is somewhere in the middle. Look at Hong Kong for example, a lot of companies are either routing around Hong Kong or coming out of Hong Kong as it spirals more and more under the Chinese influence. I think we therefore are likely to see attacks between these opposing aspects of the Internet.

3. Ransomware as a service & WFH – Ed Williams, EMEA Director of SpiderLabs at Trustwave

Both attackers and ransomware as a service are opportunistic and there's no bigger news headline than COVID-19 and vaccines. I frequently get a lot of spam around COVID-19 and some of it actually looks pretty good. Ransomware as a service is very effective, and it only takes one or two people to do stupid things like click on a link in an email and it's all over.

I would also say, from my perspective, COVID-19 and WFH have really shone a light on people rushing to do their work, yet not having the due diligence and the process wrapped around security.

One example we've seen first-hand is when organisations are deploying VPN infrastructure to allow people to access the business network remotely. This is bad practice as it allows ransomware and malicious actors to get into an organisation and spread through the network. A VPN can be a good thing, but if it's implemented badly, it's a bad thing. Organisations have the right idea but when they're rushing this kind of infrastructure out, not patching it and not getting it tested, that then leads to greater exposure and greater impact.

Even this late in the year, we're still seeing this when we have conversations with clients and ask them whether they've put something on the Internet to allow remote work, and they'll inevitably say yes. I'll ask, has that been tested? They'll inevitably say no. Then two or three weeks later I'll look at the report and find they've put services on the Internet that they shouldn't be doing, and things that should be secure, are not. As WFH stays the norm, I predict we'll continue seeing this moving into next year, any maybe even beyond.

4. An acceleration of digital transformation – Derek Taylor, Lead Principal Security Consultant at Trustwave

Our continuance of remote working, even once the pandemic is over, is all part of an acceleration of the digital agenda, and the core part of that from a business point of view is cloud adoption because it provides business agility and flexibility, and it transforms large upfront capital expenditure into relatively digestible operational expenditure on an ongoing basis. I predict that in 2021, we're going to see more and more cloud adoption to facilitate the new ways of working. The problem associated with that is that we see an awful lot of businesses thinking that because they've outsourced all of their IT to their cloud provider, they assume they'll take care of security, however this is not true. Under GDPR and UK law, the business remains accountable and responsible for data privacy and security, irrespective of the use of third parties, including cloud providers.

I think a big trend for next year is that we'll see a lot of companies who are breached, who have adopted cloud, and who then make the excuse that it is the cloud provider that screwed up.

5. M&A – survivors acquiring strugglers – Ed Williams, EMEA Director of SpiderLabs at Trustwave

I would imagine M&A is going to be a big trend next year as we’re now seeing a professionalisation of cyber criminals. They’re getting much slicker and more professional, and cyber crime is truly organised at the people level

there’s a lot of opportunity for the organisations still standing to scoop up struggling businesses at a cheap valuation. When that happens, there’ll be a lot of opportunity for things to go wrong, be that bad implementation or trust zones being crossed and passed. Poor security can have implications on price and whether the actual M&A still goes ahead. We’ve previously been in positions to see that before, where things don’t go ahead for that very reason.

To prevent this, organisations are going to have to carry out their due diligence to ensure if an organisation acquires another, be it cloud or on-prem, they know what their security posture looks like, as well has how the infrastructure has been structured. I predict many will have a lot of work to do there.

6. Key types of attacks moving into 2021 – Ed Williams, EMEA Director of SpiderLabs at Trustwave

Firstly, I see ransomware as a very quick way for criminal organisations to monetise a potential attack. If they can figure out that something is vulnerable, like VPNs for example, attackers will be able to get in and spread the ransomware through the network. Ransomware in my opinion is very easy to mitigate, but if not, the impact is serious. This year, we’ve seen that the days of just encrypting hard drives is gone. Attackers are smarter now, they’re taking data out as well as encrypting all the hard drives, and then threatening to put the data they’ve extracted for sale online. They’re becoming a bit more pernicious in what they’re doing and have evolved to the next stage, and this is something that’s likely to continue to evolve in the future.

Secondly, we’re now seeing a professionalisation of cyber criminals. They’re getting much slicker and more professional, and cyber crime is truly organised at the people level. It’s also generally not separated from other aspects of criminal behaviour either, for example, money laundering, arms dealing, human trafficking etc. It’s all comingling because it’s so lucrative.

7. Covering the basics – Derek Taylor, Lead Principal Security Consultant at Trustwave

For a while, especially this year, security has been getting worse at the basic level, but now we’re seeing an extra dimension – software developers. Everyone thinks of cyber hygiene as patching and password management, but most medium and large enterprises now have reams and reams of internal software developers or are employing third parties to carry out internal application development for them. However, the vast majority of those developers are not embedding good security development practices so apps that are being published online or on mobile phones have an increasing number of vulnerabilities which can then be leveraged by attackers to gain customer information or commit fraud.

8. Traditional security skills vs. skills for the cloud – Ed Williams, EMEA Director of SpiderLabs at Trustwave

One issue we’re currently seeing is that traditional skills don’t directly map to cloud related skills, specifically within security, so there’s definitely a need for upskilling and technical training in terms of the cloud. If you’re putting something on the cloud, it can instantly be available, the classic examples of this being S3 buckets and Mongo databases. We still see to this day buckets with poor permissions and databases with weak default credentials. Traditionally if you did something internally and it was unsecure, the impact would be quite small and contained.

However, if it’s hosted in the cloud, the impact is massive. I therefore think that moving into next year, we’ll see a number of businesses and security teams investing in technical training for the cloud.

9. Organisations need to start thinking from a data point of view – Derek Taylor, Lead Principal Security Consultant at Trustwave

A current macro trend is that organisations need to start thinking from a data point of view, not an infrastructure point of view. Who should access what data when and how across all of your IT architectures is vital if you’re going to effectively protect your data. If you can answer that, which is a difficult thing to do, then you’re halfway there. For businesses, what’s actually important is not the bunch of servers, laptops or mobile phones across your infrastructure, it’s the data that is on them. Data flows very easily between these architectures, yet most organisations don’t understand how. This is all made worse by cloud adoption, reliance on third-party developers, and the supply chain. Due to the acceleration to the cloud, we’re likely to see an increase in the number of supply chain attacks occurring throughout next year.

10. Top tips for making cyber security posture better – Derek Taylor, Lead Principal Security Consultant at Trustwave

The three main cyber security aspects businesses need to focus on next year are cyber hygiene, meaning the basics such as password management and patching; the cloud/third-party suppliers; and design by default, simply meaning implementing security early on, and not leaving it as an afterthought.
In addition, we’re currently seeing an increasing number of economic forecasters suggesting we may be entering the “roaring 20s” and therefore could experience an economic boom after the pandemic.

As this happens, everyone will suddenly be racing to generate money before their competitors. This year being cost-conscious has caused issues for the security posture of businesses, however it’s important businesses don’t get over optimistic next year and leave security behind.

Corey Nachreiner
CTO at WatchGuard Technologies
www.watchguard.com

WatchGuard's 2021 Cyber Security Predictions

IN 2021 and beyond, we predict that cyber criminals will find new and innovative ways to attack individuals, their homes and devices, in order to find a path to your trusted corporate network. The global pandemic has rapidly accelerated the existing shift toward remote work, where employees operate beyond the protection of the corporate firewall. In turn, hackers will exploit vulnerabilities found in the gaps between people, their devices, and the corporate network.

People and Emotions

Automation Drives Tidal Wave of Spear Phishing Campaigns

Spear phishing is an attack technique that involves highly targeted and convincing malicious emails that include specific and accurate details about a particular individual or role at a company. Historically, spear fishing is a high-investment and potentially high-return activity for hackers that has required manual and time-consuming processes.

That will change in 2021. Cyber criminals have already started to create tools that can automate the manual aspects of spear phishing. By combining such tools with programs that scan data from social media networks and company websites, phishers can send thousands of detailed, believable spear phishing emails, with content customized to each victim.

This will dramatically increase the volume of spear phishing emails attackers can send at once, which will improve their success rate. On the bright side, these automated, volumetric spear phishing campaigns will likely be less sophisticated and easier to spot than the traditional, manually generated variety.

Regardless, you should expect a major increase in spear phishing attacks in 2021 due to automation. What's more, bad actors know that anxiety and uncertainty make victims easier to exploit. As society continues to grapple with the impact of COVID-19, global political strife, and general financial insecurity in 2021, we anticipate that many of these automated spear phishing attacks will prey on fears around the pandemic, politics, and the economy.

Cloud-Hosting Providers Finally Crack Down on Cyber Abuse

Phishing attacks have come a long way from the 419 "Nigerian Prince" scams of old. Threat actors now have an abundance of tools to help them craft convincing spear phishing emails that trick victims into giving up credentials or installing malware. Lately, we've seen them leverage Cloud hosting to piggyback on the otherwise good reputation of Internet giants like Amazon, Microsoft, and Google.

Most Cloud-hosting services like Azure and AWS offer Internet-accessible data storage where users can upload anything they'd like, from database backups to individual files, and more. These services are exposed to the Internet through custom subdomains or URL paths on prominent domains such as cloudfront.net, windows.net, and googleapis.com. Threat actors commonly abuse these features to host website HTML files designed to mimic the authentication form of a legitimate website like Microsoft365 or Google Drive and to steal

credentials submitted by unsuspecting victims. This style of phish is effective because the email links to spoofed forms that resemble legitimate Microsoft, Google, or Amazon AWS links with domains owned by those companies. In 2021, we predict that these Cloud-hosting providers will begin heavily cracking down on phishing and other scams by deploying automated tools and file validation that spot spoofed authentication portals.

Homes and Devices

Hackers Infest Home Networks with Worms

The pandemic forced us all to adopt remote work practically overnight, and the era of home-based workforces will continue through 2021 and beyond. As a result, cyber criminals change their approach and create attacks specifically targeting the home worker.

Malicious hackers often include worm functionality modules in their malware, designed to move laterally to other devices on a network. In 2021, cyber criminals will exploit under-protected home networks as an avenue to access valuable corporate endpoint devices. By deliberately seeking out and infecting the company-owned laptops and smart devices on our home networks, attackers could ultimately compromise corporate networks. Next year we expect to see malware that not only spreads across networks but looks for signs that an infected device is for corporate use (such as evidence of VPN usage).

Booby-trapped Smart Chargers Lead to Smart Car Hacks

Smart cars keep getting smarter and more common, with more manufacturers releasing new models every year. Security researchers and black hat hackers alike are paying attention. Although we've seen plenty of interesting smart car security research in recent years, there hasn't been a major hack for quite some time. In 2021, we believe the dearth of major smart car attacks will be broken and a hacker will leverage smart chargers to do it.

As with chargers for our mobile phones and other connected devices, smart car charging cables carry more than just energy. Although they don't transfer data in the same way phone chargers do, smart car chargers do have a data component that helps them manage charging safety. In the world of mobile phones, researchers and hackers have proven they can create booby-trapped chargers that take advantage of any victim who plugs in. We expect to see security researchers find similar vulnerabilities in smart car charging components that could at the very least allow them to prevent the powering and use of your car, and perhaps demo a malicious smart car charger during 2021. If proven, at attack like this could even result in car ransomware that prevents your car from charging until you pay.

Users Revolt Over Smart Device Privacy

Smart and connected devices are pervasive in our lives. Digital assistances such as Alexa, Google Assistant, and Siri are watching and listening to everything happening in our homes, and products like Furbos even watch and listen to our pets. Smart home systems add value and convenience to our lives by automating our lights, room temperatures, the locks on our doors, and more. We even have virtual reality (VR) systems that 3D map our rooms with specialized cameras and require a social media account to operate. Finally, many of us have adopted wearables that track and sense critical health parameters, such as how often we move, our heartbeat, our EKG, and now even our blood oxygen levels. Add to this the machine learning (ML) algorithms tech companies employ to correlate the big data from users, and it's clear that companies know more about our private lives than our closest friends. Some of these companies may even understand our psychology and behaviors more than we do ourselves.

While all these technologies certainly have very useful and beneficial capabilities, society is starting to realize that giving corporations that much insight into our lives is not healthy. Worse yet, we are also starting to learn that the data mapping algorithms tech companies use to categorize us, and to quantify and analyze our actions, can have unintended consequences for all of society. That's why users will finally revolt and make vendors take privacy for home and consumer Internet of Things (IoT) devices more seriously in 2021. Expect to see the market start to heavily push back against IoT devices that collect personal data, and pressure government representatives to regulate the capabilities of these devices to protect user privacy.

Corporate Targets and Technologies

Attackers Swarm VPNs and RDPs as the Remote Workforce Swells

Working from home has become a norm for many businesses and has changed the profile of the software and services an average company relies on. While many companies lightly leveraged both Remote Desktop Protocol (RDP) and Virtual Private Networking (VPN) solutions before, these services have become mainstays in enabling employees to access corporate data and services outside of the traditional network perimeter. In 2021, we expect attackers to significantly ramp up their assaults on RDP, VPN, and other remote access services.

RDP is already one of the most attacked services on the Internet, but we suspect new companies are suddenly using it more as one strategy to give home users access to corporate machines. While we believe you should only use RDP with VPN, many choose to enable it on its own, offering a target for hackers. Additionally, cyber criminals know remote employees use VPN often. Though VPN offers some security to remote employees, attackers realize that if they can access a VPN, they have a wide-open door to your corporate network. Using stolen credentials, exploits, and good old-fashioned brute-forcing, we believe attacks against RDP, VPN, and remote connection servers will double in 2021.

RDP is already one of the most attacked services on the Internet, but we suspect new companies are suddenly using it more as one strategy to give home users access to corporate machines. While we believe you should only use RDP with VPN, many choose to enable it on its own, offering a target for hackers

Attackers Pinpoint Security Gaps in Legacy Endpoints

Endpoints have become a high priority target for attackers amid the global pandemic. With more employees working at home without some of the network-based protections available through the corporate office, attackers will focus on vulnerabilities in personal computers, their software and operating systems. It's ironic that the rise in remote work coincides with the same year Microsoft has ended extended support of some of the most popular versions of Windows – 7 and server 2008. In 2021, we expect cyber criminals to seek out a significant security flaw in Windows 7 in hopes of exploiting legacy endpoints that users can't easily patch at home.

While Windows 10 and Server 2019 have been out for quite a while, there's no getting around the fact that some people rarely update. Windows 7 (and by relation, server 2008) was one of the most popular versions of Windows before 10. Since many considered 8 and others to be problematic, many organizations chose to stick with Windows 7 and server 2008 for as long as they could. In fact, some organizations may not be able to move away from these old versions easily, since they have specialized legacy equipment that still relies on those older Windows versions. As a result, a significant portion of the industry sticks with old operating systems long past their expiration date. Black hat hackers know this and look for opportunities to take advantage. You can expect that we'll see at least one major new Windows 7 vulnerability surface in 2021 as attackers continue to find and target flaws in these legacy endpoints.

Every Service Without MFA Will Suffer a Breach

Authentication attacks and the data breaches that fuel them have become a daily occurrence. Cyber criminals have found incredible success using the troves of stolen usernames and passwords available on underground forums to compromise organizations using password spraying and credential stuffing attacks. These attacks take advantage of the fact that many users still fail to choose strong and unique passwords for each of their individual accounts. Just look at the dark web and the many underground forums. There are now billions of usernames and passwords from various breaches, widely available, with millions added every day.

These databases, paired with the ease of automating authentication attacks, means no Internet-exposed service is safe from cyber intrusion if it isn't using multi-factor authentication (MFA). We know it's bold, but we predict that in 2021, every service that doesn't have MFA enabled will suffer a breach or an account compromise.

Matt Aldridge
Principal Solutions Architect, Webroot
www.webroot.com

Why businesses need to improve cybersecurity awareness training

AMID CHALLENGING IT environments and changing tools due to the COVID-19 pandemic, phishing attempts and attacks have accelerated and sit high on the list of serious business and IT disruptions. In fact, a recent report revealed that over 1 in 5 employees in the UK have received a phishing email related to the pandemic. Yet, despite this, only 24% of UK employees say their company has increased cybersecurity training this year.

As employees continue to work from home and cyber criminals continue to develop and hone more sophisticated attack methods, the need for businesses to implement effective, accountable and relevant security training for all employees has never been greater.

Heading into 2021, organisations should urgently prioritise training programmes tailored to remote workers that contain education on key need-to-know actions such as how to spot phishing scams. To properly evaluate business' security training needs, it is important to understand the current threat landscape and changing workplace experiences so business leaders can plan effectively to protect their entire organization, staff and customers.

Remote Workforce Considerations

With an increase in distractions at home and fatigue around email and virtual meetings, it's never been more critical that training be engaging, consistent and prioritised by business leaders to ensure it's embedded into company culture. Additionally, it will prove beneficial from a cybersecurity perspective for organisations to monitor challenges around employee morale, engagement and even mental health over the next year. When exhausted or disengaged, employees are more prone to making mistakes, often unintentionally or unknowingly, that can lead to dangerous security issues or expose vulnerabilities.

Without a controlled network and traditional, onsite IT support that employees feel comfortable using, businesses need to focus on implementing training that specifically supports workers in the home environment and that accounts for stressors caused by working from home.

The WFH Threat Landscape

Cybercriminals are constantly shifting their focus and tactics to illicit maximum damage and will certainly be innovating new methods over the coming year to more heavily target remote workers, as the home network is often poorly secured and more vulnerable than an office.

This may involve attacks that target other devices on individual's home networks, and employees who rely on shared network access may be at risk from successful attacks on other people in the household. Business email compromise (BEC) attacks – which trick employees into clicking on dangerous links or transferring money by imitating someone seemingly legitimate, like a trusted colleague or boss – will also continue to be rife and take on new forms in 2021.

As new cyberattack scenarios continue to emerge, training courses will need to be constantly updated to reflect the changing threats.

Designing a Training Programme

Simply put, the level of effort to set up, update and run a program of cybersecurity training courses, compliance accreditations and phishing simulations can be daunting. However, it doesn't need to be, if understood and prioritized throughout an organization. The first step toward setting up a successful programme is to get buy-in from company stakeholders by making the need for cybersecurity awareness training apparent.

The majority of organisations are likely to already have a security strategy that includes endpoint protection, DNS or web filtering and anti-spam. These are smart investments, but the primary tactics used in successful, modern cybersecurity breaches like ransomware attacks are phishing and social engineering attacks. A little education can go a long way in

ensuring stakeholders understand that technology is not a magic catch-all when it comes to preventing or stopping attacks and that cybersecurity training and awareness deserve strategic consideration.

When introducing a training program to management, explain the importance of educating users and measuring and mitigating your risk of exposure to these threats, and share details around the training schedule and expected timeline for the campaign.

Each schedule should begin with a ‘baseline’ phishing test prior to training, administered to all employees without any type of forewarning or formal announcement. This provides a starting point for measuring improvement over time and helps leaders and training administrators to get an accurate perspective on how good (or bad) employees are at identifying phishing attempts so they can customize training that will be most effective. Once an organization has taken these steps, compiling the training programme curriculum will come next. Examples of typical key programme components include training on how to understand and spot phishing emails, how to stay cyber resilient whilst working from home, as well as any compliance courses (e.g., GDPR, PCI) appropriate for the organisation or for specific employees who need them.

The keys to a successful cybersecurity awareness program are that it is continuous, relevant and engaging and it should seek to help employees appreciate how the training benefits them in both their work and personal lives. When done right, security awareness training dramatically improves an organisation’s security, keeping employees vigilant to the constant threat of scams and other attacks that prey on human error.

> When done right, security awareness training dramatically improves an organisation’s security, keeping employees vigilant to the constant threat of scams and other attacks that prey on human error

Prabath Siriwardena
VP and Deputy CTO – Security Architecture, WSO2
www.wso2.com

Four customer identity and access management predictions for 2021

AS BUSINESSES LOOK AHEAD, many anticipate that the rapid digital acceleration experienced this year will continue in 2021. We have already seen a surge in e-commerce customers, with transaction volumes from new online shoppers during the first half of 2020 at twice pre-COVID levels. Such digital interactions will remain important as restrictions on in-person shopping, dining, and other activities are set to continue until vaccines become widely available. Even then, the convenience of conducting business online means some customers may never return fully to brick-and-mortar establishments. As a result, businesses that have previously resisted launching digital customer channels will find that it is essential for survival. From multimillion-pound High Street retailers like Primark to local restaurants and artisan businesses, building a COVID-resilient business requires online channels.

As organisations pivot to serving customers digitally, they will face challenges as demands for ensuring customer trust and privacy pull against the importance of providing an exceptional user experience. These factors will have a profound impact on how businesses build, manage, and maintain relationships with customers. The following are four trends that we will see gathering momentum in 2021.

The mass pivot to offering online services will drive demand for intelligent customer identity and access management (CIAM) solutions

Businesses that have previously operated only in the physical environment pride themselves on knowing regular customers as they walk through the door, putting a face to a name, and remembering their preferences. However, now they are faced with trying to achieve the same level of customer knowledge in the virtual environment through online ordering and delivery services. They will need to build customer profiles that turn anonymous website visitors into well-known, valued customers to whom they can offer personalised services.

Customer types will fall into broader subsets, too. Many are innately comfortable with buying online, but their expectations have been shaped by the highly sophisticated experiences delivered by Amazon, putting pressure on digital debutants to reach these high standards of user experience. On the other hand, many new online users will be unfamiliar with digital channels, so they need an intuitive, secure experience that safeguards their data privacy if they are to build trust with the retailer. This imperative will drive demand for high-performance, cost-effective customer identity access management solutions. These greenfield development projects will see strong demand for third-party cloud-based IAM solutions as businesses opt for this approach rather than developing proprietary systems.

Privacy concerns will impact demand for data sharing across service aggregation platforms

As businesses aim to launch online services quickly, many are drawn to service aggregation platforms that allow them to reach an online customer base fast. Examples include Just Eat in the

UK and Grubhub in the US, which enable restaurants to take orders and payments online. The trade-off for this simplified approach is that the business has less direct visibility into customer data. Vendors using service aggregation platforms to provide an online channel for their business will want access to customer buying patterns and behaviour data so they can create personalised offers and identify key trends. However, this presents a problem for the platform provider around how they can share this data while preserving customer privacy and ensuring they do not infringe data protection laws. As a result, privacy and consent management delivered through CIAM solutions will be a priority for platforms that build and maintain profiles of customers.

The challenges around sharing data will be significant not just in geographies where privacy laws are advanced, like the UK, Europe, and the US, but also in developing areas. The global privacy gap will narrow and having a robust way to secure and manage customer consent for data handling will be critical for anyone with an online presence.

Adaptive authentication will emerge as a must-have

As network boundaries are diluted, people will be accessing an organisation's services from anywhere. It won't be possible to authenticate users based on single factors, such as their location. Instead, authentication will be based on numerous interdependent factors, including behavior analysis, time of access, location, and more.

These will be analysed by a machine-learning algorithm that is furnished with large amounts of behavioural and network access data to calculate a risk score. Based on that score and the organisation's risk posture, an automated decision is reached on how a particular user should be authenticated. This avoids the need to ask the user for multi-factor authentication every time and thereby creates a better user experience. This will be equally true for employees accessing multiple applications from home working environments in the new hybrid work set-up.

COVID-safe "no-touch" services will drive demand for online interfaces

Along with a general acceleration of digital transformation, the pandemic will have specific impact on the customer journey. Already, organisations have adapted their operations to be COVID-safe by limiting face-to-face interactions, and many of these adaptations are likely to remain long term due to the convenience they provide. Increasingly, we will see companies develop approaches to serving customers with zero physical interaction and promote these "no-touch" services as a competitive differentiator. Consider the example of car repair. The owner arranges the repair online, books an appointment, and provides details of what is needed. They leave the car at the garage, and they are updated on the progress with video and text alerts during the day. When the repairs are complete, they settle the bill online and pick up the car, without directly interacting with anyone.As customers display a preference for safe and convenient services, businesses will be inspired to innovate to provide better experiences.

This will require an initial investment in digital solutions, but that investment should pay off, not only in helping the business navigate immediate challenges but also by shaping future strategies. For example, a restaurant that finds it is taking most of its orders online could afford to reduce its real-estate footprint and alter its business model to become more cost-effective.

Building trust in an uncertain world

Ultimately, winning customer trust and confidence will be the key for all businesses launching or expanding online services. Against a backdrop of disruption, uncertainty, and the stress of having to constantly adapt to new situations and restrictions, customers want to be reassured.

This is a critical time for businesses as they aim to continue serving existing customers, while also capturing a share of the millions of new potential consumers. Customers who are trying out a new online service want it to be safe, secure, and effective. Consumers have Amazon-level expectations of every business, which means those launching new online offerings have a high bar to clear to gain wallet-share and loyalty. Organisations need to get CIAM right if they are to protect their customers, deliver great services, and inspire confidence.

> Consumers have Amazon-level expectations of every business, which means those launching new online offerings have a high bar to clear to gain wallet-share and loyalty

DW INNOVISION
INSIGHTS + PERSPECTIVES

DATA ANALYTICS

Data is the new oil – this may be a tired phrase, but the excitement shown over the potential to do all manner of things with huge data sets (as with the rapid development of Covid-19 vaccines) shows no sign of abating.

IN ASSOCIATION WITH
DW DATACENTRE SOLUTIONS
DW DIGITALISATION WORLD

ISSUE II 2021
digitalisationworld.com

Andrew Daniels
CIO and CISO, Druva
www.druva.com

Become the master of your data: Don't wait for change to happen, prepare for it now

DATA COMES in many shapes and forms. In years gone by, we used to talk about our data in terms of the number of CD's we were storing in a CD wallet, or the files saved onto USB memory sticks back in the days where computer storage wasn't always large enough. Whilst the rules of data have been evolving significantly, but somewhat silently over the past decade, the challenges thrown up by the pandemic have rewritten more than just our daily routines, but businesses use and application of data too.

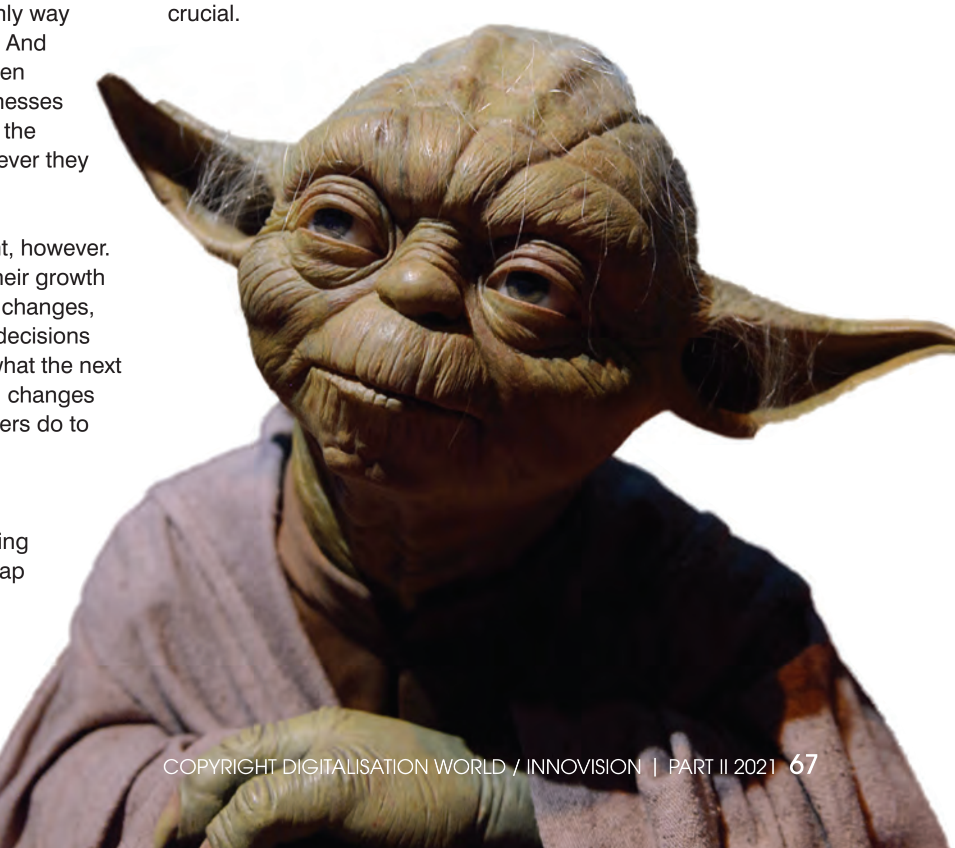
Digital transformation is a process. One, that for many businesses, had only just begun. Multi-year development plans have fallen completely off the wayside. The only way for businesses to compete, is to adapt. To innovate. And to move quickly. This means that this year, we've seen cloud migrations begin to accelerate, as more businesses think ahead to ensure that its remote workforce has the capabilities to work safely and efficiently, from wherever they may be.

Migrating to the cloud doesn't just happen overnight, however. Whilst data is critical to supporting businesses on their growth journeys, it is important that as they embrace these changes, the lessons learnt from this year sit at the centre of decisions being made. There is still a lot of uncertainty as to what the next few years will look like. But the coronavirus-induced changes are here to stay for some time. So, what can IT leaders do to prepare for this evolution of data?

Trust in data

Data driven decision making is fundamental to helping businesses develop strategies and plans that will reap rewards in a number of areas of the business. This is something that has been acknowledged, but not actioned as well as it could have been, at least for some. However, things are changing and according to new research from Druva, 79% of IT decision makers in the US and UK now see data management and protection as key to competitive advantage. What's more, 73% say they rely more heavily on data for business decisions while 33% believe its value has permanently increased since the pandemic began.

In a short space of time, data-driven decisions have moved from a 'nice to have' to a 'must have'. You must have data to improve operational decision making. You must have data to improve the customer experience. And you must have some mastery of the data in order to grow. Being able to analyse this data in real-time next year, and make data driven decisions quickly will be crucial.



Risk and reward

Like everything, this change comes with a certain level of risk. The same Druva research found that 73% of IT decision makers have become more concerned about protecting their data from ransomware. And who is to blame them? This year alone, we've seen a huge increase in malware, ransomware and phishing attacks. Cyber-criminals are looking to target vulnerable, overworked systems reliant on processes not prepared for this disconnected world. This isn't something that's going to disappear next year or the year thereafter.

As we look to the new year, we should expect to see threat actor's laser-focused on targeting any organisation associated with the healthcare industry. Be it medical research laboratories, big pharma or biotechnology companies, they all store some kind of patient data that is highly valuable right now with the ongoing vaccination efforts.

That's not to say that everyone else is off the hook. All organisations need to step up their cybersecurity posture in order to prepare for the next wave of attacks. Criminals will continue to search for the tiniest crack in your business's tools, processes or people. Without data protection solutions in place, it is safe to say that there is considerable risk of attack.

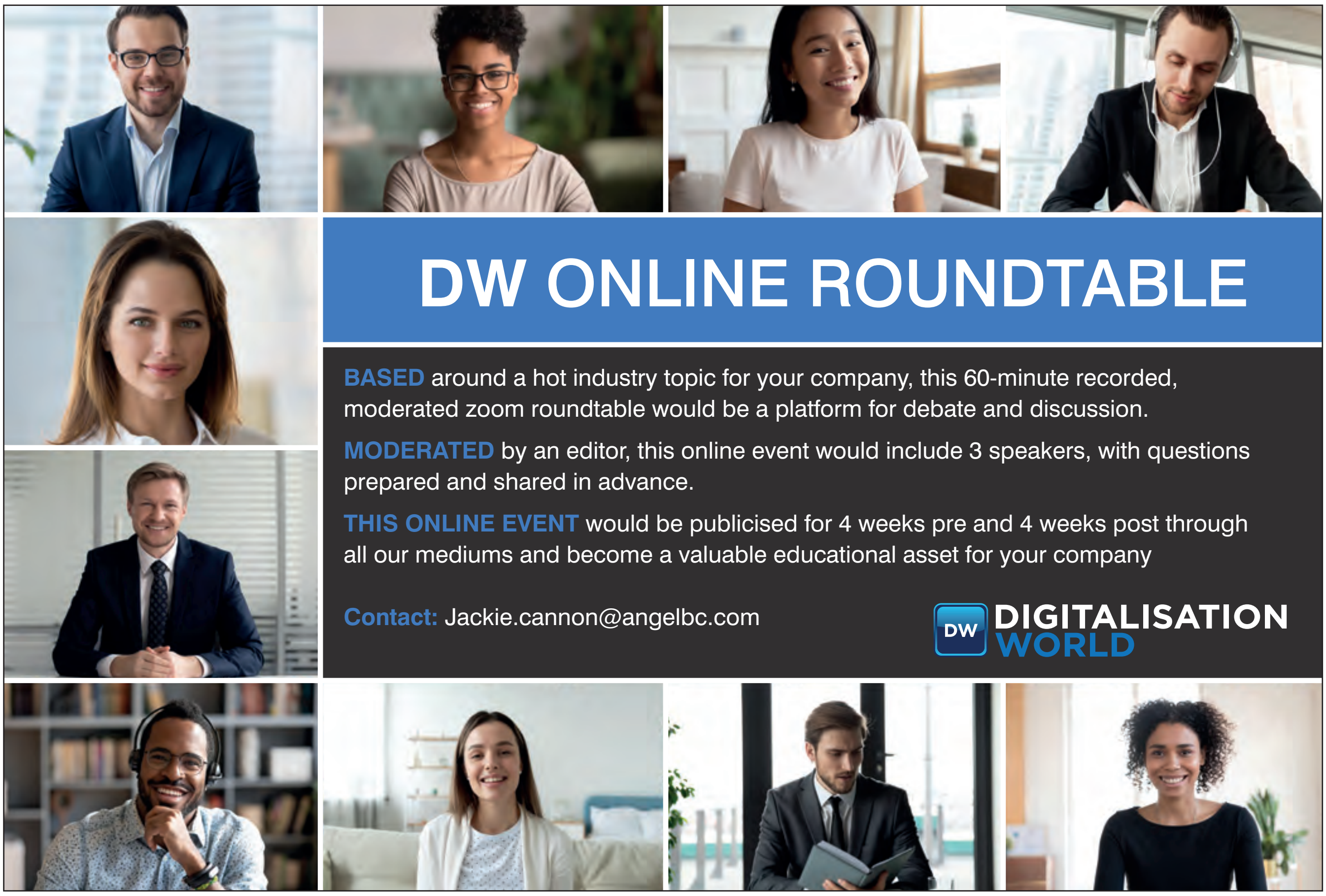
Continuity and Resilience

It's not just cyber-criminals that businesses need to be wary of. In fact, since the pandemic struck, IT leaders report a 43% rise in data outages and 40% uptick in human error when handling information. Whilst these errors are not the result of malicious activities or insider threats, the impact they have on the business – be it reputation, or financial – can and likely will still be significant.

In 2021, we expect to see the reliance on private cloud companies grow. It should not just be the IT departments responsibility for securing the organisations data, but a collaborative effort. Data security is the responsibility of each individual user. The organisation, however, does need to supply the required training, support and tools to make this possible. There is also going to be a shift towards protecting data in the public cloud. This is because more of us are relying on the cloud in order to quickly gain access to documents for remote working. The ability to rely on the cloud for this wherever we may be will be vital to the operational efficiency of every organisation as our ways of working continue to evolve.

With vaccine distribution now well underway in the UK, the public remains hopeful that life will return to normal. That said, remote working is going to be a part of our 'new normal' for the foreseeable future. As such, no matter what 2021 has in store for us, we can be sure that we will be relying on data.

The ability to act upon this data and access it from a central location will be the difference between a successful 2021, or an increasingly difficult new year.



2021 predictions for data classification

In the digitally accelerated COVID-19 environment of 2021 what are the top data security trends that organisations are facing? Here is HelpSystems Data Classification Specialist, Adam Strange's take on the outlook and trends for 2021.

Prediction / Trend 1

Ongoing growth in remote working will create data security threats

The far-reaching impact of COVID-19 includes the intensified threat of malicious cyber attacks as well as an escalating number of damaging data breaches across almost every sector of business. The rapid shift to remote working during the pandemic left many employers exposed to hackers and highlighted multiple examples of serious network and data vulnerabilities. For example, in a recent article, Infosecurity Magazine quotes research finding that attacks on the biotech and pharmaceutical industry alone rose by 50% in 2020 compared to 2019. And in the defence sector, The Pentagon is seeing a huge rise in cyber attacks through the pandemic, where unprecedented numbers of employees are forced to communicate through their own devices.

As more companies move to facilitate a semi-permanent remote workforce, data security ecosystems will evolve to become more complex and advanced data management and classification solutions will be a critical technology investment.

'Insider threat' will be categorised as the most prominent tier 1 data security risk in 2021, necessitating stricter corporate guidelines and protocols in data classification, as well as comprehensive employee education programmes around data security.

HelpSystems' recent research interviewed 250 CISOs and CIOs in financial institutions about the cybersecurity challenges they face and found that insider threat - whether intentional or accidental - was cited by more than a third (35%) of survey respondents as one of the threats with the potential to cause the most damage in the next 12 months.

Further, the latest Information Commissioner's Office (ICO) report confirmed that misdirected email remains one of the UK's most prominent causes of security incidents, demonstrating the need for all organisations to control the dissemination of their classified data.

HelpSystems' technologies in data security and classification are enabling businesses to regain control of sensitive data, identify sensitive data by scanning and analysing data at rest and classify and protect personal data by detecting PII at creation.

Prediction / Trend 2

A **security culture needs to be embedded into organisations, especially as insider breach risk continues to grow**

In 2021 data governance will take centre stage in data security and privacy strategies. Companies will create Centres of Excellence (COE) to embed a solid data security culture across teams and corporate divisions and to formalise in-house data management processes, rolling out divisional best practice and placing data classification at the foundation of their data security strategy.

Employees play a vital role in ensuring the organisation maintains a strong data privacy posture. For this to be effective, organisations need to ensure that they provide regular security awareness training to protect sensitive information. In terms of how they go about doing this, they must invest in user training and education programmes.

The security culture of the firm must be inclusive towards all employees, making sure they are continually trained so that their approach to security becomes part of their everyday working practice, irrespective of their location, and security becomes embedded into all their actions and the ethos of the business.

Data classification solutions will allow businesses to protect data by putting appropriate security labels in place. HelpSystems data classification uses both visual and metadata labels to classify both emails and documents according to their sensitivity. Once labelled, data is controlled to ensure that emails, documents and files are only sent to those that should be receiving them, protecting sensitive information from accidental loss, through misdirected emails and the inadvertent sharing of restricted documents and files.

Prediction / Trend 3

Supply chain ecosystem risk will get bigger

Accenture quote that 94% of Fortune 100 companies experienced supply chain disruptions from COVID-19, and that as much as 40% of cyber threats are now occurring indirectly through the supply chain.
· 2020 has been the year where businesses realised more than ever that data security across the supply chain was only as strong as its weakest link, where exposing a business's network and sensitive data to its suppliers had the potential to carry significant additional risk.

HelpSystems' recent report interviewed 250 CISOs and CIOs from financial institutions about the cybersecurity challenges they face and nearly half (46%) said that cybersecurity weaknesses in the supply chain had the biggest potential to cause the most damage in the next 12 months.

But sharing information with suppliers is essential for the supply chain to function. Most organisations go to great lengths to secure intellectual property (IP), personally identifiable information (PII) and other sensitive data internally, yet when this information is shared across the supply chain, it doesn't get the same robust attention.

The demand for greater resilience across supply chain operations in 2021 will require businesses to move quickly to overhaul existing tech investments and prioritise data governance. Organisations must ensure basic controls are implemented around their suppliers' IT infrastructure and that they have robust security measures in place. Advanced data classification capabilities will deliver assurance and control to numerous industries including finance, defence and government. HelpSystems advises organisations to ensure their suppliers have a robust approach to security and information risk with security frameworks such as ISO 27001 and Cyber Essentials in place.

Organisations should implement a data classification scheme and embed data risk management into the procurement lifecycle processes from start to finish. By effectively embedding data risk management, categorisation and classification into procurement and vendor management processes, businesses will prevent their suppliers' vulnerabilities becoming their own and more effectively secure data in the supply chain.

Prediction / Trend 4

Data privacy regulation set to increase

An increased focus on data privacy and protection of personal data and the continuing shift in privacy law, as reflected in the EU's landmark GDPR in 2018 and, this year, the US's CCPA, and the CPRA set to take effect in 2023, has changed the data regulatory landscape. We can expect to see similar US compliance rulings come into force beyond California through 2021.

In addition to individual state privacy rulings, we can expect to see federal US-wide regulation come into force. This new phase in privacy regulation will be complex and enforcement will demand changes in people, process and technology - proper corporate data governance programmes, employee training and solid data management systems in every organisation to counter reputational risk and hefty fines.

Data automation will also be a priority as companies struggle to deliver relevant data protection strategies for every level of business and its users, across all platforms and infrastructures to conform with individual state and international laws. · HelpSystems' unified security, compliancy and data classification solutions simplify compliancy reporting enabling business to easily generate the documentation necessary to identify security issues, give auditors the information that they need and prove compliance.

Alex Smith
Global Product Lead for iManage RAVN
www.imanage.com

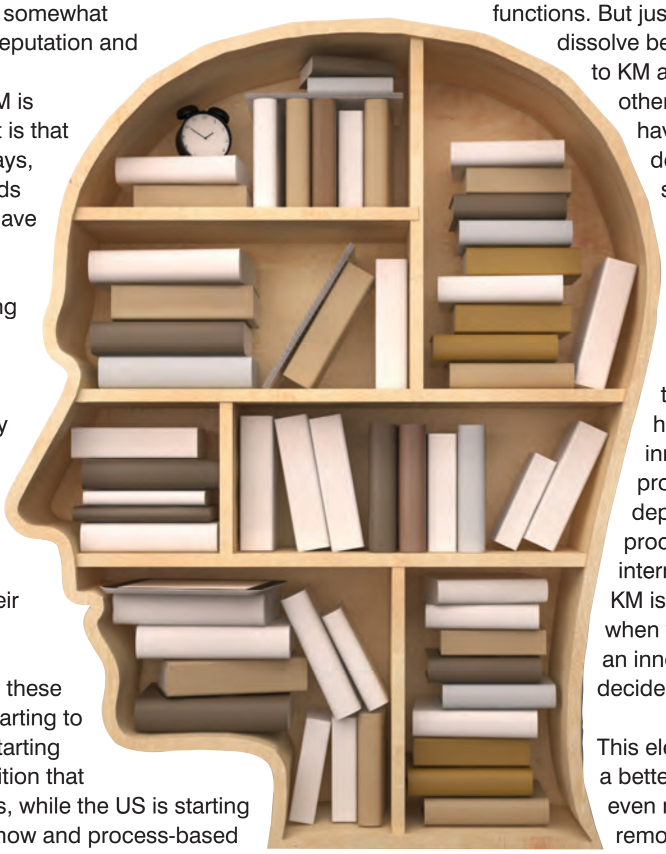
Knowledge Management is ready for a breakout year in 2021

KNOWLEDGE MANAGEMENT (KM) has always been essential to high-performing enterprises, but it hasn't always been viewed in a glamorous light or received enough fanfare. Instead, it has generally been seen as a utilitarian aspect of business that performs a function, supports a process, or memorialises how to do something -- somewhat like the pipes that quietly carry water throughout a building without drawing much attention to themselves.

In 2021, KM may finally shed that somewhat unglamorous, "under the radar" reputation and step onto center stage.
There are several reasons why KM is ready to have a moment. The first is that KM itself is evolving in exciting ways, bringing together different methods and approaches that previously have largely been separate.

Geography has long been a strong determinant of what kind of KM approach an enterprise followed. In the UK, Europe, Australia, and other regions, KM has traditionally centered around creating and curating content and know-how. The United States, by contrast, has a history of using technology, search, and databases as the backbone of their KM efforts.

What's interesting is that globally, these different approaches to KM are starting to merge. The UK and Europe are starting to liberally borrow from a US tradition that includes technology and analytics, while the US is starting to incorporate more of the know-how and process-based approach long favored by its overseas colleagues. This merger of methods sets the scene for KM to have a breakout year.



More Essential Than Ever

For starters, KM is poised to grab some of the buzz and glamour typically reserved for areas like innovation, AI processes and initiatives.

Innovation and KM have historically been entirely separate functions. But just as the walls have started to dissolve between the US-based approach to KM and the approaches followed in other corners of the globe, so too have the walls started to come down between the formerly separate units of Innovation and KM.

Why? Because there is an increasing recognition that Innovation doesn't happen on its own, in a bubble, and to be successful, innovations have to be able to scale. Scaling innovations is part of a wider process and it requires an in-depth understanding of internal processes. This understanding of internal processes is something that KM is well equipped to serve up, and when viewed through the lens of being an innovation enabler, KM takes on a decidedly more glamorous sheen.

This elevated stature couldn't come at a better time, because KM has become even more important in the age of remote working that the COVID-19

pandemic has spawned. No longer can office workers serendipitously bump into each other in the halls and ask how a project is going. Gathering around the water cooler is out, as is popping into someone's office to ask them a question that you know they have previous experience with or deep expertise on.

These are not short-term issues, because while vaccines for COVID-19 are becoming available, it will be months before they are fully rolled out. And even after the public health emergency has dissipated and "normal" life has resumed, working patterns might be substantially altered. That is, there might continue to be large swaths of the workforce who choose to work remotely rather than from the office.

This is where KM comes in. Effective KM ensures that knowledge continues to flow unimpeded throughout the organisation, regardless of where people are physically working from. The goal is to deliver the right insights to the right person at the right point in time.

One way organisations are doing this is via a deep understanding of their existing curated content and best practices, delivering it to the people who need it to carry out their jobs. Increasingly, however, technology is playing a role in delivering the right insights to the right person at the right time. This is why that merger of KM approaches – the combination of the US, technology-based approach and the UK content-based approach discussed earlier – has been so vital and is yielding serious dividends.

We're all familiar with the uncanny intelligence of the Amazon and Netflix recommendation engines, which tell you "Customers who bought this, also bought that" or "If you watched this, you'll probably like that." Increasingly, KM is able to draw on an underlying knowledge graph that maps all of the knowledge assets to deliver similar recommendations. For example, an employee searching for the ideal template to use as starting point for an M&A deal in EMEA might automatically be presented with the document that has been downloaded and used most frequently by other members of the organisation.

Better yet, an employee doesn't even have to specifically know what it is they should be searching for. Instead, AI can help surface the information that will be most relevant or useful and present it to the employee. The information finds the person, rather than the person finding the information.

Whether knowledge is curated or served up via underlying analytics, delivering this knowledge is essential to enterprises as they navigate the remainder of the COVID-19 pandemic and whatever lingering effects it leaves behind. But no matter how you slice it, 2021 will be a time for knowledge management to shine, gaining the recognition it so richly deserves for the value it has always provided.

ALEX SMITH, Global Product Management Lead for iManage RAVN, has over 20 years of experience in product management and service design, including new and emerging technologies such as artificial intelligence, semantic search, and linked data, as well as content management. Prior to iManage RAVN, Alex has held positions at Reed Smith LLP and LexisNexis UK.

From left to right: Franz Aman and Sameer Tiwari from MariaDB Corporation

2021 – the year of the database?

Sameer Tiwari, CTO of Infrastructure; and Franz Aman, Chief Marketing Officer at MariaDB Corporation, discuss their predictions for the tech industry and database ecosystem in 2021.

The impact of COVID-19 in 2021
The big stories in tech in 2021 will revolve around managing remote workforces, cost-cutting by consolidation of empty buildings, and adapting to changes in consumer behavior.

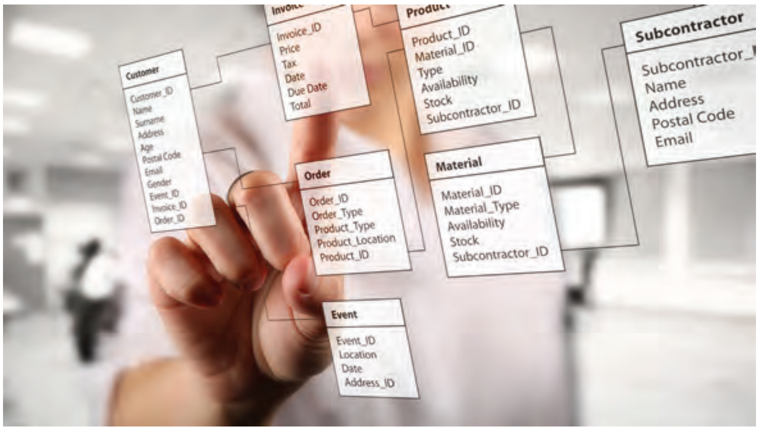
This year has challenged every company in the world one way or the other. Companies that had already migrated to the cloud had an easier time transitioning and competing in the pandemic economy. COVID's impact has sped that trend up significantly, with 40% of IT leaders in a recent survey admitting they are accelerating their move to the cloud in order to keep up with changing times.

We expect this acceleration to continue in 2021 because the cloud's intrinsic benefits - such as a more flexible investment model, reduced infrastructure and personnel costs and its easily scalable nature - have never been more powerful. While we will all be thrilled to put 2020 behind us, many IT challenges will remain, and the cloud's role in overcoming them will only continue to grow.

COVID will also have a marked impact on the IPO front by creating new industry favourites. Companies like DoorDash are going to make a killing in the tech IPO front, and following in their footsteps will be the tech vendors that make technologies that are needed by these companies. They are going to be cloud-based and offer solutions for compute, storage, automation, databases…you name it.

The year of the database?

Despite the fact that IT budgets have been tight in 2020, businesses have adapted to the changing consumer behaviours. As a result, we will see the database ecosystem flourish in 2021. This is especially true for cloud platforms; no one wants to walk in and maintain their own data centers or co-locations anymore. There is now an exodus of engineers from highly populated tech centers, and it just makes so much more sense to move to the cloud where things can be managed from a terminal.



While we expect to see an accelerated use of cloud databases as more applications move to the cloud, we also expect to see a dramatic shift toward multi-cloud support becoming a requirement in 2021. The key is giving companies the ability to source cloud services from more than one big player to gain leverage and insulation from the large-scale outages we have seen.

So, which databases will come up trumps?

360. That's the number of database systems out in the wild. And while choice is good and finding the right tool for the job is smart, it also adds major complexity. As companies move to modernise in the cloud, they will seek simplification, which will lead to massive consolidation in the database market.

Database vendors that offer multi-functional capabilities will win, rather than a multitude of niche databases that need to be stitched together and require different ways of accessing data.

Matt Yonkovit
Chief Experience Officer, Percona
www.percona.com

Predictions for 2021

Prediction One: The move to DBaaS will lead to job changes for DBAs as well as technology inheritance problems

The number of classic operational IT roles such as sysadmins, database administrators (DBAs), and web admins will continue to shrink. Why? The drive towards "easy hosting" and "as a service" models for running databases. Behind this is the trend for IT architects, developers, and non-infrastructure experts to pick the backend stacks used by applications. For these roles, selecting a database is less about specifics and more about ease of use and getting started quickly.

This furthers what I like to call the technology inheritance problem, where you have to support and run tech stacks that were chosen for you. While they might have been picked for good reasons then, those reasons might not be the same now. Those sysadmin, DBA, and web admin roles will evolve into ones covering site reliability engineering (SRE) and more dedicated application database experts.

The demand for specialized expertise on how to build, design, and architect databases will grow, and that expertise will be needed most at the start when things are designed and when things malfunction. This will force businesses to fill the gap either with consultants or on-staff expertise, or risk increased costs and lock-in over time.

Prediction Two: Open source will see movement around lock-in, with alternative options becoming available

Cloud companies like Amazon are taking an approach based on using versions of open source projects as part of their proprietary services, while traditional open source vendors like MongoDB, Elastic, Redis and others are implementing more restrictive licenses and "as a service" offerings that actively lock people in.

Ironically the push to retain market share by so-called "open source" vendors will actually drive people away from their platforms. The introduction of price hikes, lock-ins, and other restrictive and expensive methods, will force people to look for alternatives. Ironically, they may choose proprietary and "open source compatible" services from the cloud rather than supporting those original providers.

Prediction Three: Databases will move towards a run-anywhere-on-anything reality

After DBaaS will come a "run data on anything" approach, where developers and IT teams will be able to run their workloads anywhere and still get the same experience and results.

Enterprise companies (Nutanix for instance) are looking to bridge database deployments across cloud providers and data centers. Open source companies like Red Hat are pushing to run databases in a cloud-native way. The cloud providers have launched their own approaches to this with Google Anthos, Azure Arc, and AWS EKS all supporting more hybrid cloud deployments.

What makes this even more interesting is that database providers can offer "single database" and "any hosting provider" as a service offering. This means that more friction will materialize between the two groups.

Users will want the flexibility of running their databases in the cloud, but they will also want the easy route out of using a particular cloud service if they choose. For cloud providers, facilitating this open approach will allow them to meet the needs of their customers, and ensure the relationship is based on mutual respect. Open source approaches and technologies such as Kubernetes will be needed here.

Prediction Four: Innovation will come from the data management space

We have seen rapid growth in the number of technologies developed to deal with the increase in databases and data technology. For instance, growth in the troubleshooting and observability space over the last five years has been unprecedented. Over the next twelve months, this will continue to develop rapidly.

No company ever says; "I want to have less data." Instead, technology teams will need to ensure they can get value out of their data more efficiently, to justify the cost of managing all that data over time. Optimizing this spend, and how the data is stored, will go hand-in-hand.

Dan Sommer
Senior Director, Qlik
www.qlik.com

Five data trends that will shape 2021

THERE IS A SENSE THAT, having enjoyed a relatively stable period of prosperity following the 2008 financial crisis, we have seemingly been hit by one crisis after another in the last few years. It is the nature of our interconnected world – what once might have been a news item about the other side of the globe is now having a direct impact so many organisations. In such an environment, no one can truly predict what is going to happen. Yet they can be prepared for these transformative events; ready in such a way that they could even thrive on anomalies in a way that the competition will struggle to keep up with.

In what economists refer to as a K-shaped recovery, what the past year has proven is that those enterprises that have committed to being digital are best placed to adapt, and even thrive in whatever comes their way. In doing so, they are able to both react and pre-act, with digital as the driver that allows them to switch at will. For the rest, they need to pivot now.

But what enables this digital switch? Data and analytics. And some trends have shifted in imperative from gradual to immediate.

Being able to identify and accommodate those critical data trends, or pivots, is closely linked to being able to use it effectively. So, what are these pivots, and how will they affect the market, and indeed enterprises themselves?

○ SaaS is everyone's new best friend

Cloud computing has been one of the major lifelines of 2020, helping many businesses keep the lights on in virtual environments. Where once there was reticence to invest heavily in cloud and other as-a-service solutions, now many are embracing the approach, benefiting from scale and elasticity, as well as fast access to the likes of augmented analytics. This trend is going to continue, with a greater migration of databases and applications from on-premises, legacy infrastructure to cloud environments. In turn, this will drive a need for technologies that can access, move and harmonise data from multiple places.

Containers and serverless infrastructure hold great potential for running applications in the cloud, but using them at scale requires significant organisational maturity and know-how.

○ Self-service has evolved to self-sufficiency

Compelling user interfaces are no longer a nice-to-have, but an imperative. At the same time, it is not a given that users always want to self-serve; increasingly, they want insights to come to them. As a result, we'll see more micro-insights and stories for the augmented consumer.

This will also help overcome the all too frequent issue of data being overlooked. Empowering users to access data, insights and business logic earlier and more intuitively will enable the move from visualisation self-service to data self-sufficiency. Artificial intelligence will play a major role here, surfacing micro-insights and helping us move from scripted and people-oriented processes, to more automated data preparation and analytics. If data self-sufficiency can occur earlier in the value chain, anomalies can be detected sooner, and problems solved faster.

Shared data, visualisations and storytelling are consumed by the masses

Now more than ever, we've seen the importance of delivering the last mile in data storytelling and infographics. There has been a massive up-levelling in the conversation around data. This development help millions of people on the journey toward data literacy. But data is too often becoming politically fraught. How do we double-click beyond the picture? Get to the point behind the data point? Surface lineage and easily bring in new data sets? Technically, an expansion of context will be supported by more common data models and more business logic, accessible in catalogues and data marketplaces.

Up-to-date and business ready data are more important than ever

Since the pandemic arrived, we've seen a surge in the need for real-time and up-to-date data. Alerts, refreshes and forecasts will need to occur more often, with real-time variables. On a macro level, we've seen disruptions to supply chains, with hospitals scrambling to procure PPE and consumers stockpiling toilet paper. Surges like these are accentuated in a crisis, and we have to build preparedness for them into operations. As the velocity of data increases, the speed of business needs to follow. Can we make "business-ready" data – information that is not only curated for analytics consumption, but which has timely business logic and context applied to it – accessible earlier? And can we automatically trigger either automated or human-based action?

Advanced analytics need to look different

In the wake of COVID-19, there has been an increase in interest in advanced analytics. But in uncertain times, we can no longer count on backward-looking data to build a comprehensive model of the future. Instead we need to give particular focus to, rather than exclude outliers. We saw this in the results of the A Level exams in England, where an algorithm was used to determine scores, and cemented existing trends while locking out outliers. Simulations introducing unexpected inputs don't predict the future, but they can reveal how a system will react to the unexpected. What-if analysis presents options upon which we can build contingency plans, while AI will increasingly reveal anomalies outside preconceived hypotheses, which can then be evaluated by humans.

As disruptive events become increasingly common, enterprises should be looking at the lessons of 2020 and applying them to their own organisation. That means accelerating their digital transformation and making sure they have data and analytics at the heart of it. Only through doing this will they have the capacity to react more quickly, read signals more clearly and outline options for action. It's a matter of survival, certainly, but in the right hands it can also be an opportunity to thrive.

Christian Kleinerman
Senior VP of Product, Snowflake
www.snowflake.com

The Power of data analytics in a COVID-19 landscape

IT'S TIME TO LOOK FORWARD to the coming challenges in 2021. Uncertainty is our only guarantee, but three trends in data offer hope and insight for business leaders who are looking to take advantage of more sophisticated data-driven strategies. Data should work to produce better business outcomes, and this can be achieved by ending data silos once and for all, establishing customer personalisation, and in more advanced data platform operations, exploring data monetisation.

Breaking down data silos within the organisation

To tackle the great unknowns in the year ahead, organisations of all sizes must embrace all available data to better understand customer trends and demands, personalise offerings, and ensure that they are remaining competitive in a COVID-19 landscape. Those that capitalise on their data insights can pounce on opportunities or pivot to avoid issues that the pandemic may cause businesses in the coming months. Cloud data platforms are spurring this demand.

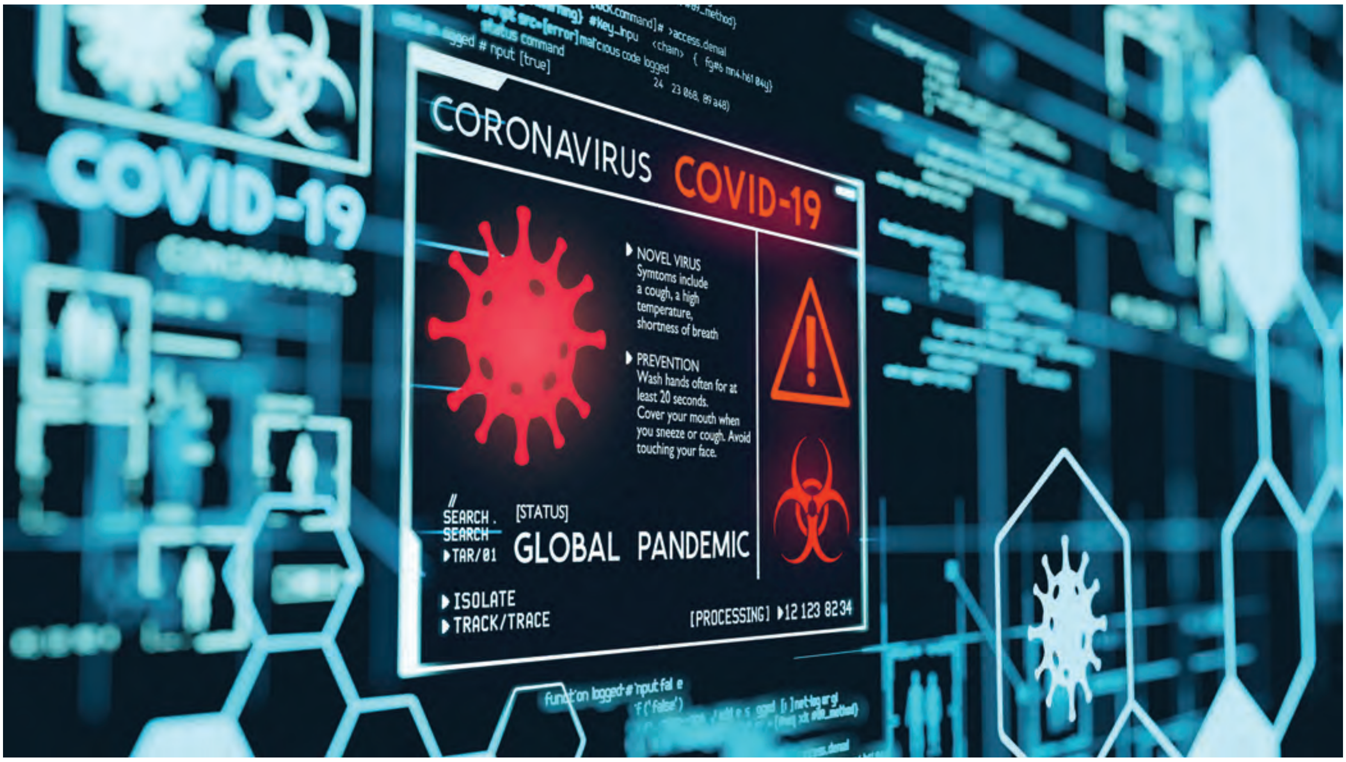
These systems offer both elasticity to manage customer demands, and enhanced data governance so that organisations have a clear inventory of where their data assets reside. With more businesses requiring to operate from a work-from-home environment, it has become increasingly important to improve visibility and understanding of data accessibility, and having systems that are designed for business continuity and disaster recovery to protect organisations against any unpredictability in the year ahead.

This new working environment will also fuel a growing demand for data external to an organisation through a wider connected network of data sharing systems. Having an acute awareness of data from the entire business ecosystem including partners, customers, and the wider industry will be key. In short, to go after big fish in 2021 by ramping up the role of data and insights in the business, data silos have to go. In their place should be a single common layer of data that offers greater governance and accessibility to teams, and a platform for data-driven endeavours, including customer personalisation.

Greater customer personalisation

In 2020, the previous models for predicting consumer behaviour became almost obsolete overnight, meaning that businesses had to lean more than ever on real-time data to give their customers the customised, digital experience that they have come to expect.

Given the ever-changing nature and volatility of consumer trends, analysing data in real-time will be a key differentiator for companies looking to stay ahead of competitors in the year ahead, with increased cloud adoption driving this trend. The cloud offers companies the opportunity to house all their various types of data in one secure place, enabling them to access all customer data. Companies get a consolidated and governed location for all types of data (for example, clickstream, transactional, and third-party) that can ingest data from new


COVID-19
CORONAVIRUS
CORONAVIRUS COVID-19
NOVEL VIRUS
Symtoms include a cough, a high temperature, shortness of breath
PREVENTION
Wash hands often for at least 20 seconds.
Cover your mouth when you sneeze or cough. Avoid touching your face.
SEARCH
[STATUS]
GLOBAL PANDEMIC
ISOLATE
TRACK/TRACE
[PROCESSING] 12 123 8234

sources such as IoT devices. This enables organisations to gain a 360-degree view of customer behaviours and preferences from multiple inputs.

New revenue opportunities in data sharing

Making data work harder by offering more people within the company deep access to insights is not the full picture of what's possible with data. Some data is valuable not just to your business, but to the rest of the world, too, and such is the case for data exchanges.

We've already seen the early signs of a shift towards people no longer just searching for data but also curating it for others to access. It's a well established truth now that data is an organisation's most valuable commodity, and in many cases more valuable than the technology that generated it. Harnessing data for external usage will drive business potential and unlock new revenue streams that otherwise wouldn't have existed. For example, a clothing retailer may have a sophisticated team of analysts who know everything there is to know about what happens within the four walls of its retail locations and understand every click on its website. Imagine what they could do with data that breaks down how people travel around a city, changes in household spending on clothing, foot traffic to specific locations and preferred payment methods.

In order for businesses to maximise the potential of their data there must be an internal shift in how their IT and data teams operate. What we'll see in the year ahead is that IT leaders will seek to free up their data and IT teams from patching upgrades or infrastructure issues so they can focus on extracting the value of data. This won't necessarily cause roles to disappear, but we will see IT teams evolving to adjust to the new changes and prioritising business relevant objectives, such as data curation.

As organisations continue to advance their cloud strategies, they must consider the tangible benefits of data sharing capabilities. Data silos, bottlenecks, and concurrency issues will become a thing of the past as modern data sharing ushers in a new era of collaboration and communication between organisations. It's an era where data is at the center, and data capability is informed not by the ability of the infrastructure, but by business needs.

In order for businesses to maximise the potential of their data there must be an internal shift in how their IT and data teams operate. What we'll see in the year ahead is that IT leaders will seek to free up their data and IT teams from patching upgrades or infrastructure issues so they can focus on extracting the value of data

Iain Chidgey
Vice President EMEA at Sumo Logic
www.sumologic.com

Data will make us faster and more secure, but more reliant on toolchains and analytics

AFTER ALL THE UNFORESEEN PROBLEMS that emerged in 2020, it might seem obvious that predictions are tricky. No-one will want more of the same over the next twelve months. Instead, we should look at how we can get things done faster and take advantage of all the good work that our teams did coping with COVID-19.

More companies adopted cloud services during 2020 to keep up with what their customers needed. At the same time, our systems created more and more data on how those applications were performing. This growing tsunami of data will carry on in 2021.

What will change in 2021 is how we make use of that data, and specifically in areas like security, software development and IT operations. Rather than each team running their own different sets of data, companies will look to consolidate how they gather data and get their teams to collaborate more effectively. Not only will this help teams look at the same data in the first place to avoid arguments, it should also reduce costs around storing that data over time.

In turn, IT teams will become more data hungry. Once you get used to having more insight around your activities, it is hard to go back. IT leaders have told their business counterparts that having more data can help them make better decisions, and this same thought process will be adopted in software supply chains. This will be based on getting more data from the tools across the software development lifecycle (SDLC), and bringing that data together so it can be understood and used.

This approach should help developers prioritise their efforts alongside any business goals that the organisation has in areas like performance or security. With real-time data from the continuous integration/continuous deployment (CI/CD) pipeline, developers can respond to changes continuously as well. This data can also be used for security purposes to flag any new issues in applications around security or compliance problems. Alongside this there will be some follow-up changes that will have an impact. As an example, developers will have to understand the economics of the cloud services that they use. As more data is created, it has to be stored and this has a cost.

Any increase in the volume of storage used will increase the bill for cloud storage too, and any expenditure like this will have to be justified over time. In response to this, developers can look at ways to reduce their future bills in advance, by understanding topics such as data cardinality and how much data they have to store over time. By planning ahead, developers can keep their costs under control while getting all that value out of the data they create.

The growth of data can also make developers more reliant on analytics tools. As developers have more and more data available to them, it becomes harder to manually query that data. Instead, developers will have to rely more on analytics tools to manage and store all the unstructured data. This will lead to changes in work practices too, focused on how teams will use and understand the data they have coming in. This should help improve productivity but also help teams focus and keep agile.

The main goals for 2021 will be security and reliability of applications and services. After scrambling to get more services online and adopting more online business processes, the next twelve months will be a combination of hardening new implementations and keeping up with new requirements. Using this new influx of data, developers will be able to improve application reliability by preventing problems or fixing issues before they affect service levels. At the same time, IT security teams can track that all the necessary processes have been followed in pre-production environments as a precursor to full deployment, which should reduce the potential for later issues.

Data lakes and data scientists to the fore

Teradata's Martin Willcox, Vice President of Technology, on how he sees the next 12 months looking as the world continues to navigate through the pandemic and specific trends and challenges that could be on the horizon as we leave this tumultuous year behind. He elaborates on data lakes, enterprise data operating systems and data scientists below but let me know if there are any other topics you're keen to cover in any related coverage and I can share additional insight.

Data Lakes

"2021 will be the year that we see large numbers of European organisations exit their 1st generation, on-premise, Hadoop-based Data Lakes. Whilst many Data Lakes have been qualified successes, many more have been expensive fiascos that support few production applications and deliver little business value - as Gartner famously predicted would be the case as far back as the end of 2014. With a "V shaped" economic recovery looking increasingly unlikely in the EU - and as organisations increasingly shift investments away from their own data centre and to the Cloud - many Data Lakes will either be quietly retired or will be re-architected for Cloud deployment as "Enterprise Data Operating Systems"

Enterprise Data Operating Systems

""…long live the Enterprise Data Operating System! Durable and flexible Cloud Object storage is already providing organisations with "any data, any format" flexibility. And it's doing so economically, enabling organisations to retain "cold" data indefinitely – or at least, for as long as the business requires and the regulator allows. But reliable and durable object storage will also enable radical architectural simplification at petabyte scale - by, for example, dramatically simplifying high availability and backup and recovery solutions and operations – and as a consequence, Cloud Object Stores look increasingly likely to become the "Enterprise Data Operating System" that the Hadoop ecosystem once aspired to be. Data and analytic platforms will continue to maintain local copies of integrated and modelled data in formats optimised for scalability and performance, rather than for durability and economy – but increasingly those platforms will need to plug-in to the Enterprise Data Operating System backbone. However, organisations that failed with 1st generation, on-premise, Hadoop-based Data Lakes because they allowed themselves to be persuaded that data management and integration were "old skool" will also fail with Cloud-based "Lake House" replacements, as a new generation of architects, developers and users comes to understand the truism "garbage in, garbage out"."

Data Scientists

"Lots of Data Scientists may need to polish their resumes… Organisations have been shovelling money at Machine Learning (ML) and Artificial Intelligence (AI) initiatives for several years now – and in too many cases have precious little to show for their efforts beyond swanky innovation labs with a high espresso machine count. In recent weeks I have spoken to a CIO in the Finance industry whose 30-strong team of expert Data Scientists has built 25 useful predictive models in the last 24 months – and got exactly two of them as far as production. And to another CDO in the same industry with a team of 40 Data Scientists who have developed 50 analytic models in the last 24 months, none of which are yet in production.

The problem is not, in general, the Data Scientists – many of whom are doing excellent work. The problem is that leadership and management have framed what is essentially a data problem as an algorithm problem, have paid insufficient attention to thinking about the business problems that the technology should be applied to in their organisations - and have thought even less about how to deploy and scale models in production. As COVID recessions start to bite and CEOs look for savings, many innovation labs will start to look like expensive luxuries."

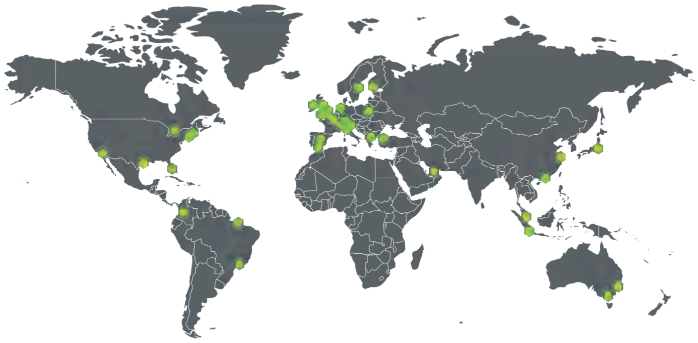
HYVE
MANAGED HOSTING

SCAN ME

The UK's Leading Cloud Hosting Provider

We are Hyve, your cloud experts. Combining our small team ethos with a passion for technology, we provide fully managed, global cloud hosting services.

We are serious about service and take pride in our commitment to personal support culture. Alongside our team of highly-specialised cloud experts, we guarantee scalability, security and unparalleled performance for your business.



Private **Cloud**

Created by cloud experts with over 15 years of industry experience, Hyve's Private Cloud provides dedicated resources for your organisation, ensuring the ultimate in security.

Dedicated **Servers**

A Dedicated Hosting solution with Hyve gives you the autonomy to decide what is, or isn't, allowed on your server. We only deploy the best hardware and the fastest storage available.

Enterprise **Cloud**

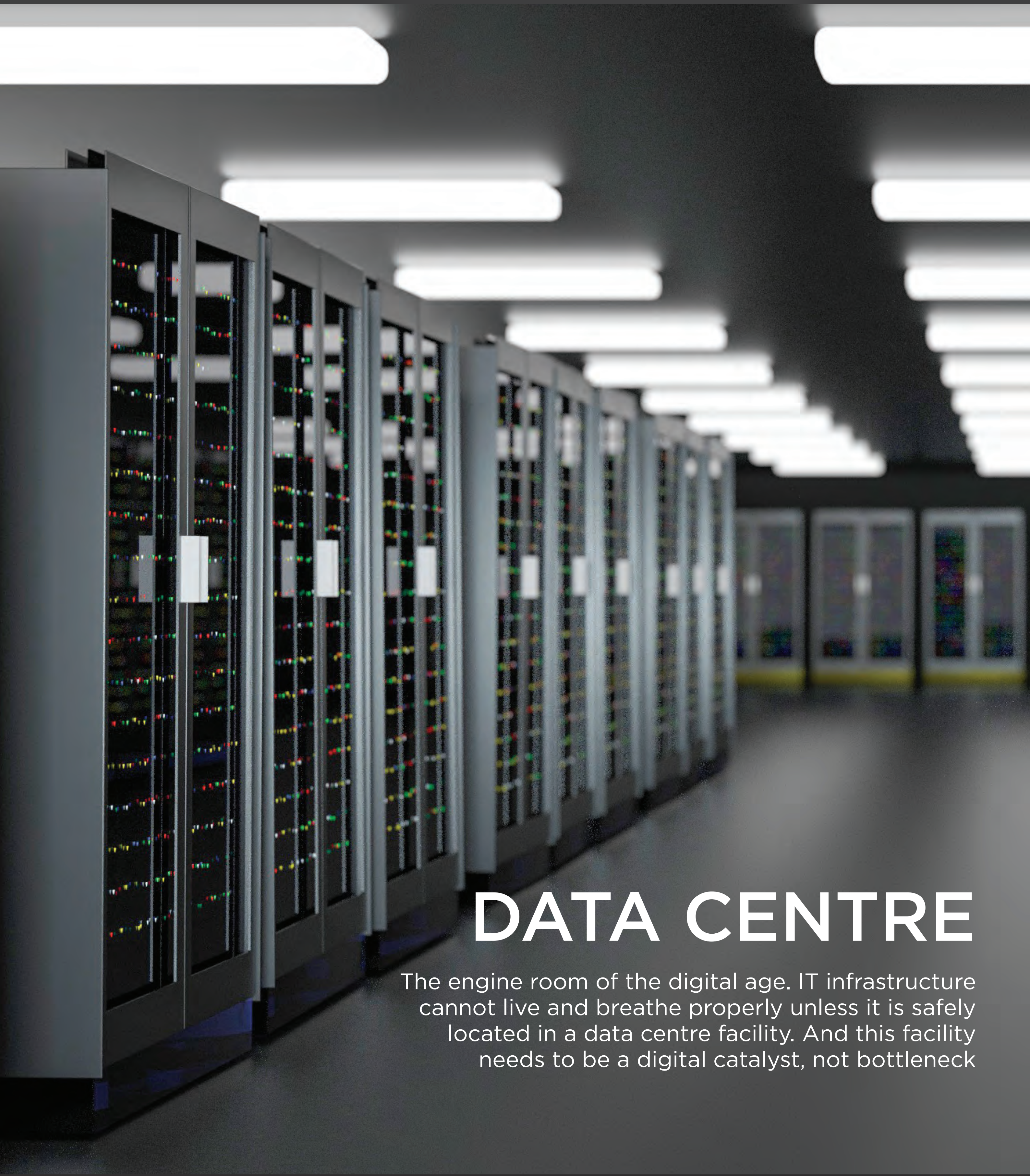
Hyve's Enterprise Cloud is a multi-tenanted cloud, providing the ease of scale and cost savings of a Public Cloud infrastructure, but with added security and monitoring.

Managed **Colocation**

We provide fully managed Colocation on a global scale, spanning across 35 locations worldwide. You can maintain complete control of your hardware, whilst we take care of the management.

www.hyve.com sales@hyve.com 0800 612 2524

INNOVISION
INSIGHTS + PERSPECTIVES



DATA CENTRE

The engine room of the digital age. IT infrastructure cannot live and breathe properly unless it is safely located in a data centre facility. And this facility needs to be a digital catalyst, not bottleneck

IN ASSOCIATION WITH
DATACENTRE SOLUTIONS
DIGITALISATION WORLD

ISSUE II 2021
digitalisationworld.com

Tony Crathorne
CEO of Bamboo Systems
www.bamboosystems.io

It´s all about Arm

2020 has been a year of massive upheaval for everyone around the globe. The threat of the Covid-19 virus has impacted people in different ways, but one common denominator can be seen; we have all had to do more with less. Less on the supermarket shelves, less time in the office, less interaction with our friends. In this climate, the tech community has continued to innovate and seek solutions that provide benefit and in a way that can be supported during these unprecedented times. With this in mind, here are a few of our thoughts on what is to come, technologically speaking, in 2021.

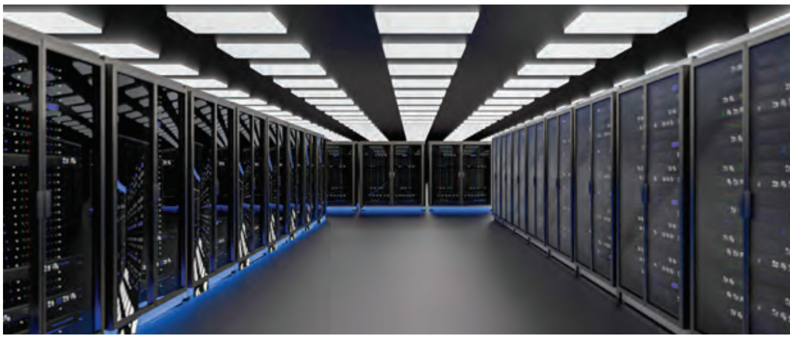
It's all about Arm in the data center for 2021

As we head into 2021, we see several significant moves in the Arm market, including announcements by Apple, Microsoft, AWS, as well as the recent NVIDIA acquisition of Arm Holdings. Even though Arm has been on the scene for years, we see 2021 as the year that Arm will for the first time be seen as a legitimate alternative to Intel for the data center.

As we leave 2020 behind, we see an $80B on-premises server market ripe for disruption. Throughout the past year the interest in Arm servers has grown tremendously and are now poised to go mainstream for a number of reasons, including their high throughput capabilities, sustainability and cost savings. Up until recently, server design has been dominated by a 40-year old, stagnant x86 architecture. While Arm has dominated the embedded and mobile markets for years, these latest moves highlight the technology's penetration into the enterprise data center. In fact, we predict Arm servers will achieve mainstream adoption within 5 years. Whoever dominates the Arm server marketing will become a category-defining, multi-billion dollar company. We are still in the midst of a pandemic and we are living through a time of "belt tightening.' Arm servers directly address this, reducing Cap-ex and Op-ex.

Modern software design requires different supporting platform architecture

Containers and Kubernetes-based applications such as seen in AI and ML need an underlying architecture that delivers the throughput necessary to optimize performance. We predict that increasingly this architecture will be Arm-based to leverage the energy efficiency it provides. Arm processors are made to complete fewer types of computer instructions. This enables them to operate at higher speeds where they can perform more millions of instructions per second. Arm processors support high throughput at a fraction of the power demand of other computing devices. The increasing dominance of PCIe over Ethernet is also a reflection of this trend and will continue.



Power consumption is increasingly presenting a worldwide problem

Data centers are expected to use over 4% of the world's power and produce 2% of the world's greenhouse gas emissions by the time 2020 has concluded. Data centers are regularly named as one of world's highest polluting industries and as our need for data only continues to grow, their energy consumption is predicted to grow 3-5x in next 5-10 years. Additionally, legacy server architecture has caused the cost of operating data centers to far exceed the cost to build them. More energy efficient data centers are a pressing economic, ecological and legislative priority.

Modern software design and data centers need high throughput, low power consumption, high density computing platforms. Arm servers provide an agile, cost effective alternative. Arm servers can run any open source software that x86 servers can, in fact better and more cost-effectively. They deliver more I/O bandwidth and memory per CPU to deliver a massive reduction in power consumption and generated heat, enabling more compute density at a lower cost. Arm servers will help turn the trend of the ever-expanding power needs of the data center.

Lewis White
VP Enterprise Infrastructure at CommScope
www.commscope.com

Key Data Centre Trends for 2021

THE EUROPEAN DATA CENTRE power market is expected to grow at a CAGR of 7.46% in the next five years. 2021 will see the accelerated deployment of new and evolving technologies in the industry and key global trends influencing these deployments include the growing demand for higher-performance networks, increased management efficiency, and the impact of the COVID-19 pandemic.

Stay-at-home orders and a big drop in on-site retail shopping has prompted a major increase in online sales and significantly impacted data centres. Let's take a closer look at these trends below.

Cloud Migration will Accelerate

In the absence of "business as usual," enterprises and small businesses are moving to the cloud, and this trend will only accelerate no matter what happens with the COVID-19 pandemic. Companies that were eyeing an eventual migration are now quickly moving to adopt a cloud-based paradigm for their businesses. Indeed, many companies that told workers to stay home have adopted remote working policies that rely on cloud-based applications, while retailers are following the lead of industry giants like Amazon and Alibaba in shifting sales tools to the cloud. In fact, these online retailers are seeing triple-digit profit growth thanks to the pandemic.

Another cloud-related trend we've observed is accelerated adoption of private cloud infrastructure. Not too long ago the prevailing wisdom was that everything would ultimately move to the public cloud. However, many companies have realised that they need to keep financial, healthcare and other sensitive information in private clouds. Some applications simply can't be converted to the public cloud, while companies that maintain large data centres are finding private clouds less expensive than public clouds.

That said, we're also seeing most enterprises adopting hybrid mixes of public and private clouds for their applications and data as a standard form of practice.

AI Adoption will Increase

Incorporation of artificial intelligence (AI) applications has been an ongoing trend for data centres, and we see no sign of this slowing down. Much of this will be related to COVID-19, although applications rolled out during the pandemic will likely remain once it passes. AI is being used to drive safety

and security applications like automatic temperature checks, touchless authorisation, payment and control systems, and traffic monitoring, for example. AI is also being implemented for building management systems such as HVAC control and lighting.

Sophisticated AI algorithms are developed by processing large amounts of data, or ML training sets. For example, millions of faces could be scanned to provide an algorithm with a comprehensive understanding of the nuances of human expression. Once created, these completed algorithms could be tasked with reacting to massive amounts of real-time information such as facial tics, furrowed brows, and pupil dilation. AI/ML data is typically housed in very large data lakes. Specialised servers equipped with accelerators, GPUs for example, are ideally suited to processing AI/ML tasks. Data centre networks are ramping up bandwidth to feed these systems with very large data pipes, enabling the cost-effective development of AI tools.

IoT Deployments will Ramp

IoT applications are rapidly proliferating as companies seek to better manage facilities and occupants. Newer connectivity protocols like LTE-M and Zigbee are enabling wireless sensors for temperature, water use, room occupancy, HVAC control and other applications, while Power over Ethernet (PoE) is enabling everything from Wi-Fi access points to surveillance cameras. IoT provides critical data that drives the optimisation of manufacturing for example, feeding a trend to apply AI to process controls. In cases where the communication is between machines, data communication systems must provide very low delay or latency. Latency is a primary reason that new smaller distributed systems or edge data centres are deployed in close proximity to their supported systems. This trend is accelerating the deployment of distributed network facilities to support a large number of edge DC applications.

As IoT applications continue to multiply, the amount of data that will be generated is expected to grow exponentially. Processing this data locally, close to the edge, is perhaps the most effective way of dealing with IoT data. Gartner has predicted that approximately 65% of all servers will be deployed in edge DCs by 2025.

The Drive to Single-Mode Fibre

Remote workers and shoppers demand immediate response times, and this will drive widespread adoption of single-mode fibre. Single-mode fibre has been around for years, but as data centres ramp adoption of 400G Ethernet in 2021, we will see deployments accelerate. Adoption was somewhat slowed in 2020 due to the difficulty of obtaining components from China, but this is expected to change this year.

Data centre capacity must continue to grow, however there must also be a continuous improvement in DC efficiency. This is precisely why fibre networks are shifting the bandwidth of network optics up – creating a need for more efficient network switching elements and driving the use of "fibre to the server" as previous generations of copper cabling reach speed and distance limitations. The IEEE 802.3db task force is targeting 100, 200 and 400Gbps speeds for short reach server connections which will aid in the development of lower cost VCSEL based optics.

Accommodating remote workers and customers, making facilities safer and more efficient, and driving higher performance will be the hallmarks of data centre trends for 2021. Companies that pursue these initiatives will be at the forefront of digital transformation as the industry's evolution continues.

IoT provides critical data that drives the optimisation of manufacturing for example, feeding a trend to apply AI to process controls. In cases where the communication is between machines, data communication systems must provide very low delay or latency

Data centre predictions for 2021

The data centre industry has witnessed significant changes over the past year. COVID-19 has accelerated demand for the cloud as Internet usage swelled in most major cities around the world as a result of consumers spending the majority of the year working, learning and entertaining from home like never before. By CyrusOne Europe.

Growth in Demand for Cloud Services

While there are indications that the crisis will ease next year, the changes that the pandemic created – most notably, remote working - will be here for the foreseeable future so as we look to 2021, we anticipate that investment in and adoption of the cloud will continue to increase.This will result in an increased spend in cloud technology to ensure the smooth and efficient running of businesses.

The shift in demand for cloud services has accelerated data centre construction projects as data center colocation providers look to build more capacity to accommodate this burgeoning traffic needs as workers continue to access applications and workload remotely. However, what does this mean for the next phase of data centre construction? It is possible that this will result in some of the largest facilities ever built.

Enterprise Migration to Cloud & Colocation

The cloud will continue to evolve into hybrid and multi-cloud forms. This will enable a far greater choice for users between cloud providers and their services. It will mean the expansion of cloud exchange facilities which can provide the infrastructural capability to deliver multi-cloud.

This may see the colocation facility return to its position as the 'default' option from which it is possible to access cloud, facility, Edge and transformation services and as the basis of hybrid IT architecture. To achieve this, the colocation facility of the future will need to build on the basis of hyperscale and interconnectivity.

Furthermore, the pandemic has sped up enterprise migration out of their on-prem data centers. The acceleration of this trend is due to concerns from enterprises about managing their own on-prem data center in times where mobility of staff is compromised, there is uncertain supplier support and a need to access the greater depth of skills and resources typically found in larger serviced data centers.

The upswing in demand that has occurred since the beginning of 2020 has put the focus on the principle of scalability. This will benefit both cloud and colocation data centers that offer hyperscale as enterprise struggles to deliver necessary levels of agility and scalability inside their own data centers.

Sustainable Design, Build and Operation

We have seen sustainability issues climb up the agenda within the data centre industry over the last few years, but this has been expedited in 2020. The current pandemic has resulted in a significant increase of public awareness of the data centre industry and its impact on society and the economy. With that, comes additional pressure and scrutiny - particularly with regard to sustainability - which will continue to grow in 2021.

Our hyperscale (cloud service provider) customers have some of the most ambitious sustainability goals of any industry, the best thing we can do for the environment is to help them succeed. In Europe we already operate highly efficiently, it's in our industry's interests to do so, but there are always further improvements to be made working with customers, suppliers and M&E teams to bring the power usage (PUE) down, conserve water through design and operation and find alternative uses for the heat, for example.

One particular sustainability challenge for companies looking to increase their renewable procurement across Europe as we go into 2021 comes in the form of energy contract terms. Many companies purchase brown power with short term agreements of a year or less, whereas many of the available green power projects that actually result in additional power require much longer timeframes – sometimes as long as 10 years or more. These contracts can expose organisations to market volatility they may be unfamiliar with. As the renewables market continues to mature and energy buyers familiarise themselves with renewable power, we must find strategies such as forming groups like the Renewable Energy Buyers Alliance (REBA) to overcome these hurdles.

There is no doubt that data centres can get better in regard to sustainability and that the industry is committed to rising to the challenge.

We have also seen several new guidelines and pieces of legislation setting sustainability targets for the industry emerge

in 2020, meaning it is becoming increasingly important in 2021 to work together as an industry, through organisations such as the EUDCA and techUK, to educate governments and ensure recommendations are fit for purpose.

CNI Risk / Opportunity

The pandemic has put the importance of data centers into focus. In Europe, several governments, including the UK, formally recognised the data centers sector as critical infrastructure during the height of the pandemic in the early half of the year. Going forward, there is potential for the industry to leverage its position on key decisions concerning land and power permits for future developments.

However, this could also lead to greater legislative oversight in the future. The government may take a greater role in determining the standards on emission, power usage and planning permissions and utility permits for future facilities.

Delays to Delivery of New Capacity will Continue

Data center capacity consumption patterns have changed over the past year. Before the pandemic, cloud customers in colocation facilities typically utilized 75-80% of their capacity outside peak times. During the Covid-19 crisis, they have regularly drawn 100% of their available capacity for extended periods to meet public demand for applications and services. This poses a long-term challenge for data center operators and may directly impact their ability to maintain resilience. In these situations, there will need to be some examination of contracts to realign the costs of maintenance, resilience and expected life cycles of facilities.

Investment

We have seen exponential growth in the cloud this year and as we look to 2021, we anticipate that investment in and adoption of the cloud will continue to increase. While there are indications that the crisis will ease next year, the changes that the pandemic created – most notably, remote working - will be here for the foreseeable future. This will result in an increased spend in cloud technology to ensure the smooth and efficient running of businesses.

We anticipate that budgets will increase in 2021 to account for the additional investment necessary in technology. While this will be somewhat offset by write-downs in other business costs such as travel, office leases and equipment, CIOs will need to invest heavily in hardware and applications to enable businesses to survive and compete in a challenging economy.

Looking at the data centre industry specifically, we expect overall costs to increase. This will be driven by increased costs of construction, materials and operations as a result of COVID-19. At the same time, reliance on data centres will continue to grow as companies become more liberal in their adoption of the cloud and 'work from home' becomes the norm.

New Market Growth

Through the pandemic, we've observed increased customer demand outside of Europe's four major markets (London, Paris, Frankfurt, Amsterdam) and exploring growing EMEA hubs such as Berlin, Madrid, Milan and Warsaw. These new markets provide access to major cities, a growing client base, available land and power and utility access, all necessary resources that the major markets may no longer be able to provide.

Ed Galvin
Founder and CEO, DC Byte
www.dcbyte.com

What's ahead for the data centre sector

A FEW MONTHS AGO, in October, The Data Centre Report was released. Prepared by DC Byte, in partnership with Knight Frank, the report was the first of its kind, covering all types of data centre activity across twelve key European markets. The content of the report got a great deal of attention, as it mapped out the growth of hyperscale self-build activity, showing a sector undergoing a dramatic transformation. I'm confident that 2021 will see further twists and turns.

The Data Centre Report also found that the sector was much bigger than previously reported with 4,505MW of live IT power across Europe. At this time there is also over 1,032MW of new data centre space under construction which is nearly a quarter of the total of all data centre space that has previously been built – ever. All of which is due to come online in the next 12-18 months. Beyond this, a further 2,801MW of phased capacity, the equivalent of over 62% of all previously built IT power, is planned for development within 3-5 years. Some may start to ask where all this new power going.

Until this point it has been generally accepted that, except for a few fringe cases, the bulk of enterprise hyperscale development has happened in Ireland, whilst in the UK and mainland Europe wholesale colocation dominated. In 2017, hyperscale development in Denmark exploded. Apple launched a data centre in Viborg estimated at 160MW; Facebook followed with a 72MW facility in Odense and now Google is moving forward with its own development in Fredericia, estimated at 120MW.

Rapid change is happening elsewhere too. In 2019 Amazon Web Services secured planning consent for the biggest data centre development that Spain (and the Iberian Peninsula) has ever seen. Over 300MW planned for development across three sites. In Belgium, Google's St. Ghislain campus has increased its IT power to now represent over 75% of all data centre space built in the entire country. The realisation here is that there is now more development underway outside of the traditional core markets than there is within.

In 2021, and of course beyond, I expect this trend of regionalisation to continue. Spreading data centre space more evenly of course reduces data transit costs, whilst diversity of location also helps mitigate the impact of any changes in data sovereignty laws.

There will no doubt also be a continued trend for hyperscale deployments to favour self-build over colocation. This is a natural part of their evolution and dominance of the market; watching the internet giants further increasing and evolving their business models. The sector has never been so exciting from a rapidly changing landscape, and potential opportunities, perspective. To this end we are starting to see 'land grab' as the supply of suitable sites stalls but demand continues to increase.

The cost of getting the land buying decision wrong is negligible however, when compared to wider reputational risk. Having access to, and being able to rely upon, the close to real-time data has never been more critical both for those procuring the sites, and equally those advising them.

Colocation will continue to play a role in meeting short-to-middle term demand for hyperscale space. Edge-type colocation operators, and those built around 'carrier hotel' type network hubs, will benefit from increased consumer demand - we are in fact already seeing reports of increased demands for 'micro' data centres to service content demand associated with the adoption of 5G mobile.

In short, demand for data centre space is increasing substantially and there are notable trends. The move towards self-build by the hyperscalers is having a significant impact on the levels of competition for available space so the tendency is now for data centre developments to be more evenly spread around Europe rather than concentrating purely on the large 'Gigawatt' markets. We will of course see continued investment within the Gigawatts, currently on course for a vintage year; and will see strong investment across a greater number of locations than was traditionally the case.

Investment activity will increase more broadly as buyers seek alternatives to the office market which has been hammered by COVID. While data centre investment used to be the private equity, venture capital and alternative asset classes, 2021 will see the continuing transition to investment from more mainstream real estate and infrastructure funds. This weight of money is likely to push down borrowing costs and push up company valuations… great for those already in the business, not so good for new entrants.

Looking further ahead, whilst at present most of the market activity is in Europe, we expect APAC to benefit as investors see Europe as an increasingly crowded market.

Mark Seymour
CTO at Future Facilities
www.futurefacilities.com

Make your sustainable data centre goals water-tight

2020 has heightened the world's environmental concerns. From David Attenborough's bleak outlook on what happens if we continue without change, to Biden's change in direction for the US environmental impact, people are starting to act. To meet this consumer demand in the data centre sector, great environmentally-focused strides have been taken with fresh impetus in areas like liquid cooling. In addition, the Digital Twin has been making further inroads into the data centre industry. By creating a replica of a data centre to use for simulation, the Digital Twin enables owners and operators to achieve higher capacity at a reduced cost and lowered risk while offering cost savings and environmental benefits.

Next year, however, the data centre industry has the opportunity to take leaps and bounds, rather than strides, if it seizes the opportunity to use the Digital Twin and liquid cooling together.

Move over air cooling

Liquid cooling is a topic growing in importance within the data centre industry. It is well known that liquid is a better medium for transporting heat than air because waste heat in air systems is typically low grade. Air too is difficult to transport effectively, making it difficult to target hotspots. Liquid cooling on the other hand has none of these shortcomings, while also bringing advantages too. This includes higher IT performance and productivity, less facility space requirements, faster heat recovery and better sustainability. The challenge lies in quantifying these for different businesses.

At present metrics are limited or simply don't exist. For example, the power usage effectiveness (PUE) measurement isn't ideal for liquid cooling. PUE is improved for air cooling by the inclusion of IT fans in IT power requirements, while for liquid-cooled systems these fans aren't present at all.

Liquid cooling is on the brink of becoming the mainstream, but there are hurdles to overcome. Many organisations have invested heavily in the air cooling infrastructure, and it's difficult to retrofit liquid into sites without spending twice. Further to this, it may not make environmental sense to throw away these air cooled data centers spending energy and materials replacing them for only a marginal performance improvement. Therefore, it's likely in the future liquid cooling will feature more in new designs where it is incorporated from day one. In order to implement this within the next year, operators need to break down the perceived risk of liquid in the data center. One way to achieve this is by conducting more research into liquid cooling – like The Green Grid which is working on a white paper on liquid cooling energy effectiveness. By showing the industry how it can use liquid cooling for its advantages, it's possible the industry could move beyond simply just looking at metrics like PUE.

Making these arguments in such a way that the business case is clear is a challenge that when solved will result in liquid cooling being quickly adopted across the industry.

Ride the wave of liquid cooling

It's clear liquid cooling in data centres can boost sustainability efforts, and the market is growing. In fact, by 2024 the data centre liquid cooling market is set to be worth $3.2 billion as it grows at a CAGR of 22.6%. However, to unlock the full potential of liquid cooling and allow the growth of high-density requirements such as AI, operators will need to make sure they're making use of technologies like the Digital Twin. This technology provides operators and designers with the exact visibility and analytics on capacity needed to minimise risk, keep a tight rein on costs and maximise the business potential that is demanded. The Digital Twin's expansion into liquid cooling modelling will enable data center designers and operators to incorporate it into their plans, and hit important environment-focused goals.

The new year brings an opportunity for the data centre industry to hit refresh on its sustainability efforts. In doing so it will result in both reduced operational costs and increased efficiency, with consequences for a positive environmental benefit. As an industry, let's join together to make 2021 a year where we work to facilitate positive change.

> The new year brings an opportunity for the data centre industry to hit refresh on its sustainability efforts. In doing so it will result in both reduced operational costs and increased efficiency, with consequences for a positive environmental benefit

Steven Carlini

VP Innovation and Data Centre for Schneider Electric

www.se.com

Looking back over 2020: data centre and edge computing predictions

WHEN ASKED what was most likely to cause a change in a government's direction, a famous British Prime Minister once famously answered: "Events, dear boy!" An unscheduled, if not entirely unforeseen, occurrence of sufficient magnitude will always cause a realignment of priorities and force actions along a different path to what was intended.

For the IT sector in general, and for the data centre industry in particular, the spread of the Covid-19 pandemic caused a significant refocus of digital transformation objectives. One that without fundamentally changing the general direction of the industry, certainly accelerated some existing trends, and reinforced the need for greater visibility of distributed, critical infrastructure systems.

As digitization becomes a key priority in public spaces, such as in retail and public transport, there has already been a shift towards automation and disruption. With the emergence of self-service kiosks in fast-food restaurants, at supermarket checkouts and in petrol stations, for example, the implications of the pandemic have reinforced the need for digital technologies that steer society towards a more touch-free, contactless mode of operation.

Although contactless payments from credit cards and Apple Pay are already familiar features, we expect that many touch-screen kiosks will soon be phased out, and will be replaced by new forms of contactless interaction. This may be based on pre-ordered items from a phone, from scanning menus in restaurants, or via high-definition video to recognise motion or personal features. Nonetheless, smarter features, such as contact tracing to limit the spread of the Covid virus, will likely be built into retail and public-transport systems, as well as in many building management systems (BMS).

The surge in edge and remote monitoring

For the data centre and IT sectors, all of these developments will further drive the growth of edge computing, as the demand for local transactions will force more and more data processing to the periphery - close to where the data is created, processed and consumed.

Further up the chain this will have implications for both infrastructure deployments and remote management. In the former case, the rollout of business-critical IT systems at the edge will require that the systems are quick to deploy, easy to maintain and manageable from remote control centres.

Accessibility has been a key challenge for many businesses and sectors throughout the year, so critical IT equipment located in areas with few technical support staff must be robust, secure and easy to service.

The effects of the pandemic also brought to the fore the issue of data centre remote monitoring and management. As the ever-changing situation forced large numbers of people to work from home, the demands placed on data centres, energy grids and digital connectivity networks only increased. Many operators realised that, although they may have had some kind of on-premise DCIM or remote monitoring system in place, it may not have been sufficient to provide the level of visibility that was needed.

Many companies have therefore realised a greater need for improved visibility of the data centre's electrical and mechanical assets, as well insight into what's happening in the IT room. As we look forward I believe this will only become more crucial, and the need to monitor your infrastructure from anywhere, or securely on any device will only increase. Here the deployment of next-generation, or vendor-agnostic DCIM will see a surge.

The need for a sustainable edge

For deployment at the edge, a focus on standardisation is crucial. This is the best way to keep costs down, exploit economies of scale, improve speed of deployment, and simplify the tasks of servicing and remote monitoring. In practice, there will be a significant increase of micro data centre deployments to support geographically dispersed edge applications. For the most part, it is likely they will remain multipurpose systems, due to a lack of a compelling business case for single-application installations.

s the demand for 5G accelerates, the issue of energy efficiency, or sustainability at the edge becomes paramount. While it has become more important to have visibility across edge environments, now operators must also ensure that pre-integrated power, cooling and IT systems operate efficiently. This not only offers users a lower operating cost via reduced energy usage and with it, a far lower carbon output, but it enables them to manage the performance of the network, servers and workloads more efficiently.

In the data centre sector we expect to see some ramp up of liquid-cooled systems although it is likely that for now at least, it will remain a niche area - predominantly used in high performance computing or supercomputing applications, OCP-Ready™ colocation data centres and in high-density edge environments. There are obvious advantages of liquid cooling in terms of sustainability, with some studies showing greater energy efficiency and CapEx savings of up to 14%. Yet the complexity of deploying liquid cooled solutions in legacy facilities, compared with air cooling, is an inhibiting factor.

We expect to see liquid-cooling continuing to be deployed in individual racks for niche applications, rather than seeing entire facilities equipped. However, as with other infrastructure, as the industry figures out a way to standardise and create liquid cooling facilities to scale, it could be a winner in the medium term.

5G and hyperscale demands

With many construction projects now well underway again, we expect to see continued growth across the full spectrum of data centre service provision - from colocation providers all the way to the hyperscale community. With hyperscalers now becoming known as the 'core of the network', we expect to see service providers reacting to the movement of more processing at the edge by re-engaging their sights on storage at the core. Here, the market will continue to segment between "hot", or frequently accessed data, and "cold" storage for archived information that is less business-critical. It is likely that there will also be different pricing models applied to each.

The disruption this year has also affected much of the anticipated rollout of 5G communications. In reality, most carriers have been rolling out low-band 5G, operating at about 600MHz, which is similar in performance to 4G, rather than the GHz spectrums offered by higher band 5G. In 2021 we expect to see 5G emerging in more industrial applications in private networks, where large companies can operate at whatever part of the spectrum they like and use the technology to increase performance, productivity and avail of compute intensive applications like AI and Robotic Processing Automation (RPA). In the public domain, we expect to see a significant increase of 5G deployments as a "last-mile" solution to bring "fibre-quality" 5G connectivity to the home. This has the obvious advantage of making high-speed connectivity available to areas not currently served by fibre in a cost-effective way, and one that is far quicker to deploy.

As we look forward, it is crucial that our sector remains agile and focussed on adapting to ever-changing times. This year has shown the determination and tenacity of data centre professionals and our role in supporting the mission-critical needs of customers who are dependent on digital infrastructure.

Giordano Albertazzi

EMEA President at Vertiv

www.vertiv.com

Trendspotting: Data centre efficiency at the edge

2020 resulted in the world transitioning online overnight. This has taken data centres beyond just business-critical, they are now an essential component of the way work and leisure operate. This reality will manifest in new ways in 2021. Data centre capacity will gain utility-level criticality and centrality, being seen as important as the likes of other strategic supplies for a country, city, or household (e.g. electricity, broadband, etc..). Here are my thoughts on three key trends that will dominate as this unfolds in 2021:

Edge: Small spaces, big capabilities

Today's edge is more critical and acts as a functioning extension of the data centre – differently from the glorified IT closet of the past. Cost and complexity have traditionally prevented implementation of data centre best practices in these spaces, but that is changing. I believe we can expect to see a continued focus on bringing hyperscale and enterprise-level capabilities to edge sites. This includes greater intelligence and control, an increased emphasis on availability and thermal management, and more attention to energy efficiency across systems.

Wherever there is a high density of data processing, there will also be a demand for edge computing. We are already seeing expansion of the edge in many countries and that will eventually extend to emerging markets. Edge deployments are also closely aligned to other key trends such as 5G and environmental sustainability, and the integration of edge sites with energy grids can support the transition towards renewables.

Conversations around 5G will be about energy and efficiency

In this year's early stages of 5G planning the discussion has focused on the ultimate benefits of the technology, which are increased bandwidth and reduced latency, and the applications it will enable.

However, as many countries begin their 5G rollouts in 2021, we will see the focus shift to the significant energy consumption increases brought on by 5G. The network densification necessary to fully realize the promise of 5G unavoidably adds to the increased energy demands. This is currently estimated to be 3.5x more than 4G. The coming year will see greater focus on managing that significant increase in energy consumption by exploring more efficient products and practices.

Sustainability Comes to the Forefront

5G is just one chapter in a broader sustainability story. As the proliferation of data centres continues and even accelerates, especially in the hyperscale space, providers are facing increased scrutiny for their energy and water usage. The amplification of the climate change conversation and shifting political winds in the United States and globally will only add to the focus on the data centre industry, which accounts for approximately 1% of global energy consumption.

The coming year will see a wave of innovation focused on 5G, edge and energy efficiency across the data centre ecosystem, and the benefits for data centre operators are clear. Starting with cost reduction, compliance with existing and anticipated regulations, these developments will also build a brand's reputation as a leader in the global sustainability movement if they play their cards right.

DW INNOVISION
INSIGHTS + PERSPECTIVES

STORAGE

Data storage continues to grow in importance, alongside the data analytics explosion. You can't crunch data, if you don't know where it is, or haven't stored and backed it up properly.

IN ASSOCIATION WITH
DW DATACENTRE SOLUTIONS
DW DIGITALISATION WORLD

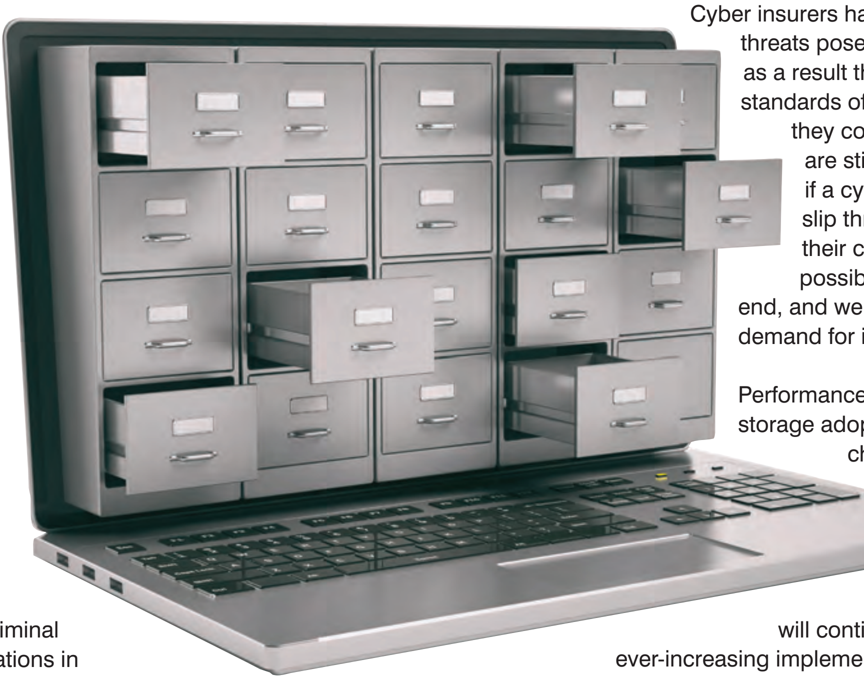
ISSUE II 2021
digitalisationworld.com

Neil Stobart
VP Systems Engineering Sales, Cloudian
www.cloudian.com

How will 2021 look in the world of data storage?

2020 was a transformative year for IT. Almost every company on the planet had its IT infrastructure disrupted to a significant extent by the pandemic, and regardless of how things evolve from here, it would be foolish to think the aftereffects of these events will not reverberate well into 2021 and beyond.
When it comes to data storage, here's what we expect to see in the coming year.

Ransomware will continue to define IT agendas
Ransomware rose to the forefront in 2020, and organisations everywhere will continue to seek more reliable ways to ensure they're protected in 2021 as a result. Research from Crowdstrike shows that 71% of the cybersecurity experts they surveyed are more worried about ransomware attacks due to the COVID-19 pandemic.



The National Cyber Security Centre (NCSC) also recently reported that it had handled more than three times as many UK ransomware incidents as in the previous year. In addition, a majority of European Law Enforcement professionals deem ransomware to be the biggest criminal threat to organisations in Europe, according to Europol's most recent Internet Organised Crime Threat Assessment – but this doesn't necessary have to be the case.

We expect ransomware attacks to become more manageable in 2021 as organisations opt for immutable backup data repositories on top of perimeter security solutions. Data immutability renders backup data invulnerable to manipulation by hackers, thereby enabling users to restore a clean copy of data in the event of an attack. This means organisations will suffer only a relatively brief period of downtime, rather than facing a defining event where a crippling ransom needs to be paid.

Cyber insurers have also taken notice of threats posed by ransomware, and as a result they are demanding better standards of data protection from those they cover. Though cyber insurers are still willing to back enterprises if a cyberattack does manage to slip through the net, they expect their customers to take every step possible to minimize risks on their end, and we expect this to further fuel the demand for immutable backup.

Performance demands will drive flash storage adoption but raise scalability challenges
In 2021, the growing demand for high-performance storage will continue, fueled largely by the ever-increasing implementation of performance-

intensive workloads such as artificial intelligence, machine learning and data analytics (which is only set to continue). While this will drive further adoption of flash storage, it will also present challenges as organisations seek solutions that not only provide high speed – flash storage's main strength – but also massively scalable capacity. With flash storage providers struggling to re-architect their platforms, we expect to see increased adoption of flash-based object storage, particularly for data analytics workloads that require high performance capacities. This will also reflect object storage's increased usage beyond just backup and archive.

Container adoption will drive change in storage infrastructures
Deploying containers has many benefits for IT teams, such as the increased simplicity of deploying microservices, or the ability to enable faster application creation and deployment, allowing organisations to be more agile in response to the rapidly changing demands of modern IT. IDC expects container instances to reach 3 billion by 2021, meaning they have transcended their original audience of hyperscalers and other large cloud providers to move firmly into the IT mainstream. Until recently, these container environments have been supported primarily by public cloud due to its fluidity and scalability. However, despite these strengths, public cloud can also present issues when it comes to keeping storage overheads predictable and avoiding surprise costs.

As a result, we expect to see further use of containers on-premises, capitalizing on new storage solutions. In particular, cloud-native, S3-compatible object storage platforms are an excellent option in these instances, as they provide a cloud-like experience that can deliver the needed scalability and durability across a range of geographically distributed locations without incurring unexpected storage costs in the process. The S3 API is the "lingua franca" of object storage and is by far the most dominant API. This means having all your data stored in a way that is natively S3 compatible will make the road to container implementation smoother, due to the data portability this enables.

> C loud-native, S3-compatible object storage platforms are an excellent option in these instances, as they provide a cloud-like experience that can deliver the needed scalability and durability across a range of geographically distributed locations without incurring unexpected storage costs in the process

Scality predicts containerisation and cloud-native apps will define the 2021 data storage landscape

Containers will transform solution architectures; their impact will be comparable to that of server virtualisation and cloud computing. Hybrid cloud DR will save millions of dollars.

SCALITY has published its data storage predictions for 2021, focusing on the rapid growth rate of cloud-native apps and containerisation. According to IDC, by 2023, over 500 million digital apps and services will be developed and deployed using cloud-native approaches. That is the same number of apps developed in total over the last 40 years.

From left to right: Giorgio Regni, CTO and Chief Product Officer Paul Speciale at Scality

"The accelerated growth of next-generation cloud-native digital apps and services will define new competitive requirements in every industry. Cloud native and containers are rapidly turning into the new blueprint for application development and underlying cloud infrastructure services," explains Giorgio Regni, CTO at Scality. "For the storage industry, the container trend represents a significant inflection point that will transform deployment architectures leveraging Kubernetes and container-native storage APIs. Its impact will be comparable to that of server virtualisation in the 2000s and cloud computing in the 2010s."

Scality's Chief Product Officer Paul Speciale added, "2021 will see a number of trends emerge as enterprise IT teams and storage vendors adapt in order to support the rise of cloud-native apps and the subsequent change in application and cloud infrastructure models."

Scality's predictions for 2021

New container-centric storage solutions will emerge
Storage vendors in 2021 will create solutions to address the increasing scale and agility demands of container-based services, including boot volumes and logs, transactional databases, application data over traditional file and new object APIs, as well as backup and long-term archives. New container-centric storage products will be developed to enable traditional data-centric applications, as well as object storage and backups, to access Container Storage Interface (CSI)-type persistent volumes and radically reduce the complexity of large-scale Kubernetes deployments.

Hybrid cloud data management will be adopted for disaster recovery

Disaster Recovery (DR) across two physical data centres will no longer be required in 2021. Instead, hybrid cloud DR solutions that manage synchronized copies of critical data on-premises and in the public cloud will enable IT leaders to avoid the costs required to maintain and service two remote locations for DR, thereby saving thousands, if not millions, of dollars.

Flash media will be embraced for high-capacity storage

A new generation of high-density flash storage will become widely available in 2021. The optimal combination of high performance and lower prices makes it suitable for scale-out high-capacity file and object storage. Until now, flash storage has been deployed in smaller capacity applications and latency-sensitive use cases, while high-density spinning disk has been the preferred storage medium for large volumes of data (for example, media files or medical images). With the introduction of lower-cost, higher-density flash media in 2021, these use cases will adopt capacity-optimized solutions that maximize these benefits in density, scale and agility for multiple workloads.

Object storage will become a de facto storage model for data lakes

Research and Markets estimates that by 2025 data lakes will grow into a $20.1 Billion market. To fully analyse and take advantage of the wealth of information and insight in these massive data repositories, organizations require a foundational storage layer that makes data accessible and useful. In 2021 object storage will fulfil this role, becoming the dominant storage interface for analytics applications, such as Cloudera, Elastic, Spark, Splunk, Vertica, Weka and many others. This is because analytics applications leverage the AWS S3 API, the standard API for object storage; large semi-structured and unstructured data sets are a natural fit for object storage; and performance and capacity resources can scale independently since object storage decouples the application compute tier from the storage tier.

2021 will see an increased convergence of object and file storage for unstructured data

Organizations today are prioritizing data storage that scales both in capacity and in the breadth of applications that it supports. Cloud-native applications, which naturally consume and interact with object storage over S3 API, are increasingly deployed in the enterprise alongside long-standing applications that access file system storage. As a result, solutions that combine file and object models into single unified systems will prevail in the enterprise starting in 2021.

The service mesh will be adopted to connect and secure workloads

Complex cloud-native applications that straddle cloud regions, on-premises core data centres and edge locations are becoming increasingly popular. Yet secure communication between these services remains a challenge, particularly as the rise in remote working strains legacy network and firewall designs. In 2021, 'service mesh' approaches to secure network communication will be broadly adopted. Such approaches will enforce Transport Layer Security (TLS) and authentication and access control for both workload connectivity as well as towards the edge. This gradually introduces 'zero-trust' networks (spearheaded by Google's BeyondCorp framework) where network policies can be codified and systematically deployed and enforced.

Spectra Logic 2021 predictions

Spectra Logic forecasts the trends in the storage industry for 2021. By David Feller, vice president of product management and solutions engineering, Spectra Logic

THE NEW YEAR will see storage vendors shift from a purely hardware-focused approach towards more of a “consultancy style” relationship with customers. These discussions will highlight how to integrate cloud, protect against cybercrime, and take the long-term view of data storage whilst optimising budget.

New data storage lifecycle management capabilities will help organisations take further steps towards deriving value from their data, properly protecting data, and optimising data placement for cost savings.

Data growth and the rise of tape

Organisations have had to re-evaluate their storage strategies to ensure infrastructures can adequately support continuing exponential data growth and digital transformation, both cost-effectively and efficiently. Technology will evolve as data sets continue to rise, along with the data storage requirements (including regulations) of content owners.

These factors will increase the pressure and urgency for organisations to ensure all existing data is properly stored for potential future use, thus bringing the need for cost-effective archiving and retrieval strategies higher up the agenda.

Tape storage will remain a major contender as manufacturers continue to double down on features and capabilities while being mindful of customer budgets. Many organisations will reach exabyte levels in 2021, with data-hungry vertical industries such as high performance computing (HPC), large government agencies, medical and AI research organisations, autonomous vehicle companies, etc., continuing to heavily invest in and rely on tape libraries (taking advantage of its high capacities and interoperability advancements) to adequately handle future data growth and stay within budget.

The redefinition of hybrid cloud

2021 will see the redefinition of what hybrid cloud really means. Data centres may consolidate but they are not going away. Whatever the market segment, organisations can create a workflow to utilise cloud in tandem with on-premise workflows.

The perception here would be that the amount of work has been doubled. But next year we will start to see deeper discussions on the new trend of cloud and on-premise integration as part of one workflow. It will be the task of organisations (with vendors in support) to understand how to manage multiple clouds as part of its workflows and integrate that with on-premise services for the long-term. This will be an exciting space to watch.

Storage Lifecycle Management

Increased demand for improved data access, control and protectionin the long-term will drive interest in storage lifecycle management capabilities. By leveraging the two-tier storage model to “smartly” move data off of primary storage and onto perpetual storage (freeing up the more expensive tier-one storage capacity), customers can not only make substantial savings, but with less data sitting on the high-performance storage tier, more organisations will benefit from efficiency and performance improvements to the entire system.

The resurgence of the archive

The pandemic has resulted in media and entertainment (one of the industries hardest hit by COVID-19), becoming almost completely dependent on reusing pre-existing content, making access to archive absolutely critical.

For these organisations, an understanding of what digital assets they own is crucial, but it is also a question of how quickly that content can be retrieved, and whether it can be accessed by other stations from any location, if need be.

This capability has created a resurgence in the value of the archive in long-term storage strategy planning. When robust protection is enabled by multiple copies in various locations, the archive is very well protected.

The "ransomware-resistant" organisation

With cybersecurity threats (such as ransomware) exploding in 2020 and showing no signs of abating in 2021, organisations must assume (especially with the increase in remote working due to COVID-19), that they will get targeted at some stage and, therefore, it is critical they are fully prepared.

In this next year, the enterprise will learn from other companies that have undergone attacks, and implement steps to become "ransomware-resistant". With ransomware attacks encrypting not only servers but also backups, our prediction is that the strategy of backing up to tape, with its unique air-gap protection (meaning data is out of the network stream), will play a big part in organisations confidently protecting themselves.

> The pandemic has resulted in media and entertainment (one of the industries hardest hit by COVID-19), becoming almost completely dependent on reusing pre-existing content, making access to archive absolutely critical

Florian Malecki

IPM Senior Director at StorageCraft

www.storagecraft.com

Four ways data storage will be different in 2021

2020 has taught us that absolutely nothing is predictable. With that in mind, we're not swinging for the fences with our data storage predictions. Instead, we believe the following four observations will continue to gain traction in the coming year. Despite this, we believe the following four observations will continue to gain traction in the coming year:

COVID-19 will change the data-management paradigm for years to come

Security, backup, and recovery issues across remote locations have been exacerbated by COVID-19, and remote working has compounded vulnerabilities. With many businesses looking to embrace remote working for the long term, it's clear we won't be returning to the office anytime soon.

As a result, companies must manage and protect data at edge locations effectively. They will need to put greater emphasis on simple-to-implement, cloud-based solutions that effectively backup and protect data in remote environments.

"Zoomification" will put unexpected strain on storage capacity

In the COVID-19 era, companies are generating more data than ever. With the rise in Zoom calls being recorded, shared, and ultimately stored, many organisations are unknowingly running millions of dollars of video storage costs annually. They will soon face a wake-up call as they outgrow existing storage space and scramble to meet far greater data-storage requirements. The same is true for other sectors, including education and healthcare, which are increasingly embracing digital and, as a result, exponentially increasing the amount of data being created.

To expand storage needs and improve data backup and recovery, a new scale-out approach to storage will be essential. This enables organisations to purchase storage upfront at a reasonable price and then scale-out that storage cost-effectively over time.

Data storage will embrace zero trust

Businesses of today embrace a zero-trust approach to security. They entirely remove trust from the equation and assume that everything, including users, endpoints, networks, and resources, is untrusted and must be verified.

A similar approach will soon be embraced when it comes to data protection. Indeed, a study found that due to remote working, 60% of IT buyers have fast-tracked zero-trust policy and technology over the last seven months.

Take an employee who is requesting to have data recovered from their laptop. What are the real-time credentials certifying that this particular employee can restore a specific machine? What permissions were contained in the backup image? If IT is restoring a machine that was set up a month ago, who is ensuring that no one else has access to that machine? A zero-trust approach to data backup and management will help answer these questions while further protecting enterprise data.

Data storage and backup will get more intelligent

Organisations are collecting and analysing massive amounts of machine learning and IoT data. Tesla, for example, is currently collecting data from its vehicles on the road as part of its effort to deliver autonomous driving. But, if your company depends on collecting and analysing data to operate, what happens if that data is not fully backed up and easily recoverable? What happens if any of that data is lost? For a company like Tesla, any issues with data could result in inaccurate algorithm engines that could potentially put lives at risk.

Most companies are thinking about data analysis and much less about data backup or security. But as data moves from analysis to production environments, that's when protection becomes critical. Storage tools increasingly rely on AI and machine learning to automate the data backup process. Given the size of enterprise data, these intelligent tools will become vital for maintaining an efficient backup process that can react to changing requirements while saving untold hours on manual backups.

Final thoughts

In an increasingly distributed work environment, immediate access to data and online collaboration is a must. In 2021, organisations must evolve and enhance digital environments to operate successfully. The challenge is that remote work environments generate massive amounts of critical data that needs to be adequately protected and stored. By adopting a modern approach to data storage, organisations can effectively thrive in this new normal.

Toshiba outlines key data storage trends for 2021

Toshiba Electronics Europe GmbH (TEE) has a longstanding reputation as a leader in data storage technology, and its team of experienced professionals possess a deep understanding of the fundamental dynamics that define the market. In the following text, Rainer W. Kaese - Senior Manager for HDD Business Development of the company's Storage Products Division - gives his insight into what the year ahead holds.

THROUGH A BROAD cross-section of use cases, each with their own particular nuances, the expectations currently being placed on data storage technology are proving to be greater than ever. Our society's data consumption is already way beyond what could have even been imagined in the past. Projections from IDC suggest that our annual data generation levels will have exceeded 175 Zettabytes by 2025. Furthermore, the expansive array of new applications that are now starting to emerge mean that the exponential growth rate we are already experiencing is only going to continue.

As we go into 2021, dramatically heightened data access activity is going to start being witnessed at the edge, as well as at the core. Thanks to the huge production volumes supported, coupled with characteristically attractive price points plus ongoing innovations, hard disk drives (HDDs) are certain to continue to have an important role to play.

Although solid state drives (SSDs) seem to get the vast majority of media attention, the value of HDDs should never be underestimated - especially as data storage demands are getting more and more intense. It must be acknowledged that even the most ambitious estimates about future SSD production output would still only allow this storage medium to constitute a mere fraction of the total capacity that will be needed.

Market Developments Driving Demand

Changes to working culture over the last 9 months, with a much greater percentage of the population now working from home with all-digital connections, has accelerated the migration to cloud-based services. This is putting more strain on existing data center infrastructure. At the same time, the landscape supporting all this activity is changing too. Cloud-based IT, often located in co-location (colo) sites, is set to become increasingly commonplace, enabling the requirements of numerous customers to be attended to using shared resources. This sets new challenges when it comes to storage technology that forms the foundation of data center operations - requiring optimized solutions that match the access pattern as well as performance and reliability requirements.

Alongside what is occurring in the data center sector, the roll-out of Internet of Things (IoT) technology is now starting to scale up considerably. Estimates on the number of connected nodes being put into operation over the course of the next few years vary, with Juniper Research even predicting that this figure could actually pass 83 billion by the middle of the decade. What is definitely assured is that, if IoT is to be truly prevalent, the costs involved need to be as low as possible - especially from a data storage perspective.

Closely interrelated to IoT roll-out, increased interest in Industry 4.0 will be an impetus for the deployment of greater storage capacity in relation to the manufacturing arena. IoT will also be leveraged by utilities and municipal administrations to enable various smart city functions to be benefited from (thereby combatting congestion, air pollution, etc.). As with Industry 4.0, this will result in huge quantities of data being generated by sensors. With only limited on-site storage reserves and processing capabilities available, this data will generally be sent back to cloud servers for subsequent analysis - where cost-effective data storage resources will once again be required. More widespread use of surveillance systems is also

destined to have a major impact on data capacity requirements, as will the move towards greater vehicle autonomy in the years to come.

Cost Considerations

For all the use cases just discussed a substantial ramping up of data capacity will be mandated, while still keeping the financial investment involved to a minimum. Admittedly, a single SSD may be able to outperform a single HDD. However, the applications we are talking about here don't deal in single discrete units - they need large scale solutions. For such implementations, multiple configured HDDs are able to achieve very high IOPS figures, while still being extremely economically viable too.

When looking at what is the most suitable storage medium to utilize, the price/GB is usually the primary concern. Though the costs associated with SSDs have fallen, they remain close to an order of magnitude higher than their HDD equivalents. Moreover, advances in HDD design are translating into further cost savings. It should be noted that tape will have to play a role as well, as it's definitely the cheapest way to store data when it comes to cost per capacity, but tape is not directly competing with HDD and flash, as all data storage mentioned so far is on-line, while tape is not an on-line media.

From an engineering standpoint, continued progression is being made with regard to helium-filled drives. Next-generation technologies like heat-assisted magnetic recording (HAMR) and microwave-assisted ma gnetic recording (MAMR) are also in the pipeline. Through these, there is the prospect of storage capacities being boosted without calling for any cost premium.

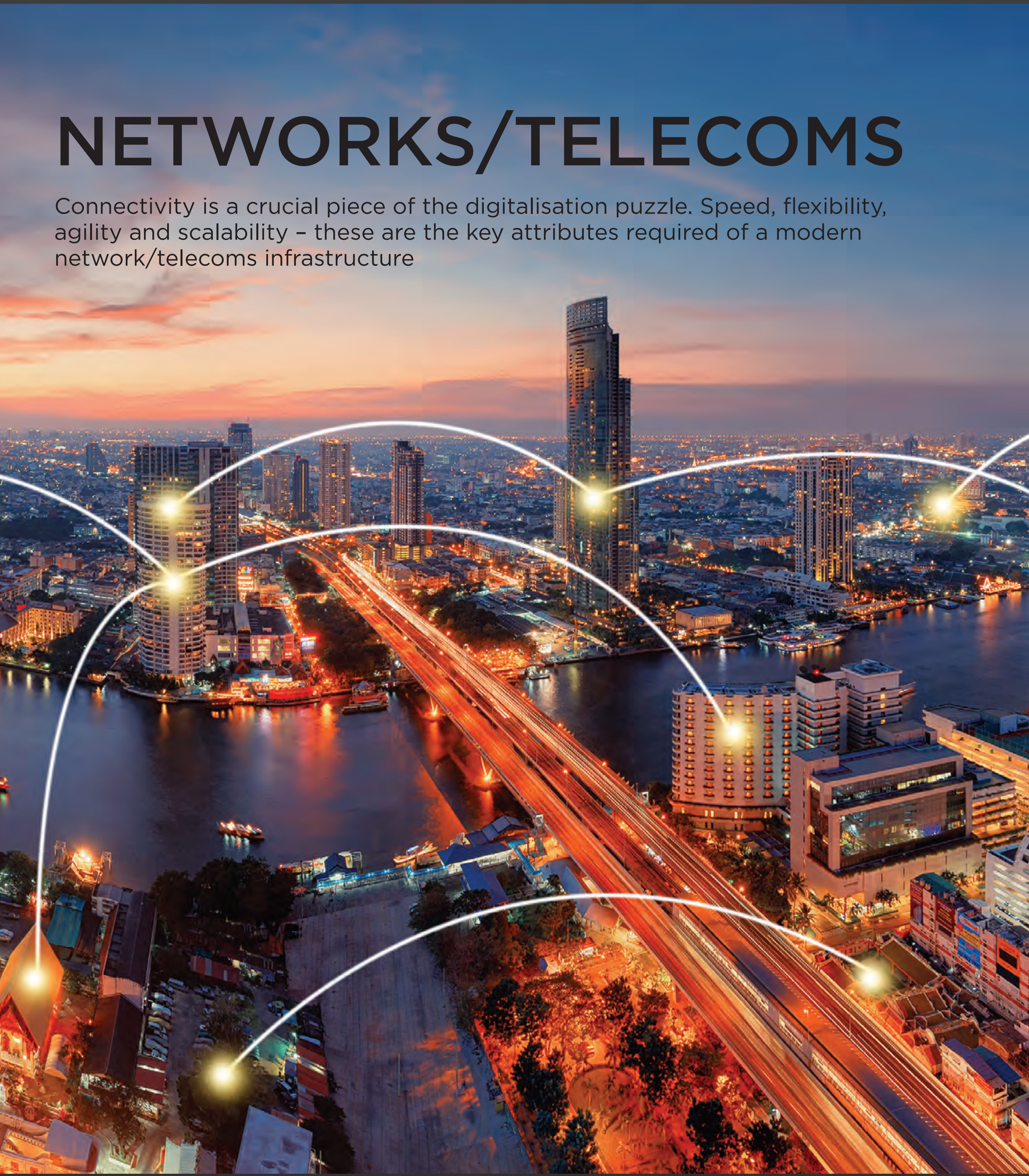
The gap between HDD and SDD implementation outlay will therefore remain sizable for a very long time yet, as will HDD's overall market dominance in terms of deployed online storage capacity.

When looking at what is the most suitable storage medium to utilize, the price/GB is usually the primary concern. Though the costs associated with SSDs have fallen, they remain close to an order of magnitude higher than their HDD equivalents

DW INNOVISION
INSIGHTS + PERSPECTIVES

NETWORKS/TELECOMS

Connectivity is a crucial piece of the digitalisation puzzle. Speed, flexibility, agility and scalability – these are the key attributes required of a modern network/telecoms infrastructure



IN ASSOCIATION WITH
DW DATACENTRE SOLUTIONS
DW DIGITALISATION WORLD
ISSUE II 2021
digitalisationworld.com

Marc Serra
CMO & Head of S&D at Infovista
www.infovista.com

What does the future hold for the telco industry?

Mobile operators accelerate OSS integration and cloudification

Operation Support Systems (OSSs) are often an obstacle to evolving mobile networks as most of them were designed and built in the 2G/3G era. With the rise of virtualised networks and newer OpenRAN technologies, more operators are preparing to move their OSS to the cloud to become more agile while reducing their total cost of ownership (TCO).

A few operators have already started this journey with Rakuten, Elisa and DT as some of the most visible examples, each of them following specific paths and dealing with radically different backgrounds. But they all demonstrate how crucial network functions – such as planning, design, service assurance, troubleshooting and optimisation – can now be delivered from the cloud in support of the 5G rollout.

The network lifecycle gets automated

The promise of SON (self-organised networks) has been around since the early 2010’s but has failed to deliver on its potential. For several years, there have been efforts to automate parts of the network lifecycle through specific use cases and a recent study commissioned by Infovista suggests that half of CSPs intend to deploy or expand automated solutions within the next 12 months. The expansion of 5G networks during the next few years will provide a catalyst for more automation to span the full set of network lifecycle activities.

Over the coming year, more operators will follow the example of disruptors such as Rakuten in Japan, Dish in the US or Jio in India that have started their mobile networks from scratch in the 4G/5G era, with the big advantage of no legacy technology to support.

The headline benefit is that by combining the latest RAN technologies with advanced network automation, these pioneers can produce “GBs” at 40-50% lower cost than leading carriers. This is not going unnoticed by other operators, which are starting to prioritise automation, looking for more interoperability, as well as vendors which can offer integrated solutions.

Consumers will drive 5G adoption

A host of lower cost 5G chipsets released in 2020 along with Apple’s recently unveiled iPhone 12. 5G will lead to a surge in 5G adoption during 2021 with consumers rather than businesses leading the charge. As Covid restrictions ease, video will continue to drive the bulk of data consumption but fixed-wireless access (FWA) technology, which aims to provide “fiber-like” connectivity at homes through 4G/5G will gain more momentum especially in suburban and rural areas.

All this may help counterbalance the uncertainties toward 5G within the Enterprise market, where the pandemic aftermath will be felt in many industries, some harder than others.

The great content migration: Content delivery predictions for 2021

Steve Miller-Jones, VP edge computing and solutions architecture at Limelight Networks, has outlined three key trends he expects to see in 2021 including real-time streaming, 5G migration and content security.

2020 was a dramatic year for OTT content providers and content delivery networks (CDNs). The shift to online living and remote working resulted in a massive surge in demand for content – from streaming services, to online gaming and video conferencing solutions. Yet, despite the strain, the CDNs remained robust when it mattered most. As new content platforms go live, the priority won't just be to deliver content – but to ensure the user experience is as innovative, low-latency and engaging as possible.

As we enter the final month of 2020, Steve Miller-Jones, VP edge computing and solutions architecture at Limelight Networks, outlines three key trends he expects to see in 2021:

Real-time streaming takes the throne

Real-time streaming will make the viewing experience more interactive and personalized

"The content we like to consume is changing. COVID-19 didn't start the trend, but it has accelerated it. People – especially younger generations – are gravitating towards short-form content and real-time, data-intensive OTT services. They are beginning to expect more interactive experiences from their content, and that means larger data volumes and more pressure to reduce latency. The next generation of viewers won't just consume real-time content, more and more they'll interact with it.

“One area where this will be really prevalent is live sports. As sporting events returned to our screens this summer, several broadcasters experimented with new virtual offerings to make the real-time streaming experience more engaging. This experimentation will only increase in 2021. We can expect gambling integration and personalised services that provide alternative commentaries, live audio feeds from the referee’s mic, and crowd sounds for an authentic stadium experience. We will also see more features focused on social streaming, allowing friends to watch together. These features might be short-lived, but those that really engage audiences will remain and change how live streaming experiences are defined. We’re not there yet, but we’re approaching a model where the user controls the content experience for themselves.

“This of course will require real-time distribution of data from service providers. What this means is much more data delivered in a shorter window of time. This is especially true given growing demand for 4K content streaming. Efficient delivery of content will continue to be critical to the viewing experience, so providers will look for the best and most efficient standards and formats for the job. For example, techniques like Content Aware Encoding can create high quality video with lower overheads, helping keep costs under control.”

5G will help content migrate to the edge

5G exits the hype cycle, raising the bar for content delivery at the network edge

“The continued rollout of 5G micro stations and antennas will bring forward the opportunity for bandwidth improvements. Most consumer devices on the market are still heavily 4G-dependent however, so the improvement will not be immediate. But in time, we’ll start to see consumer devices come out that can properly capitalise on the 5G spectrum. When this happens, consumers will be able to enjoy the higher bandwidth that 5G promises.

“The steady uptake of 5G devices will create greater opportunities for more data-rich experiences. There will also likely be an explosion in the amount of data generated by devices connected to the 5G network. This gives rise to the need to process that data closer to the end user, to deliver strong performance and an individualised experience while also reducing the costs of centralised processing.

“5G creates more capacity at the network edge to deliver quality, data-intensive content experiences. However, capitalising on its potential will depend on close collaboration between telecommunications providers and CDNs. Telcos will need to consider where in the network to place the capacity to distribute content and process data most effectively. This will be important where users are demanding radically different kinds of content and using new data rich services. Fortunately, CDNs can enable them to determine the best network locations to service this demand.”

> As sporting events returned to our screens this summer, several broadcasters experimented with new virtual offerings to make the real-time streaming experience more engaging. This experimentation will only increase in 2021. We can expect gambling integration and personalised services that provide alternative commentaries, live audio feeds from the referee’s mic, and crowd sounds for an authentic stadium experience

Content will become a security priority

New technology will help protect streaming infrastructure as well as data services

“COVID-19 has created a fertile environment for cybercriminals. Lockdown didn’t just inspire a spate of ransomware attacks on remote workers, it fuelled attacks on business continuity and service infrastructure. DDoS attacks continue to be one of the most popular tools for hackers. While security priorities used to be confined to the protection of data, the scope will extend to the security of content services, intellectual property and streaming infrastructure in 2021.

“More steps will be taken to protect the infrastructure responsible for content creation. DDoS protection and perimeter security will receive greater investment, alongside new access control and user authentication measures. Zero trust between systems will become the default setting for many organisations to ensure content can’t be compromised from without or within. We’ll also see companies take steps to reduce the pirating of their content and identify illegal credential sharing by users.

Techniques like forensic watermarking will be used to stop pirates from copying and distributing content illegally. CDNs will play an important role in identifying credential sharing, allowing publishers to confidently make decisions like blocking or banning the offending users easily.”

Jonathan Rowan
BDD at SSE Enterprise Telecoms
www.ssetelecoms.com

Predictions for 2021: what's next for the telecoms industry?

2020 will go down as a year that was famously difficult to predict. It's not that innovation stopped as a result of coronavirus - far from it - but it has led to a shift in priorities and innovation in different areas. The pandemic has not just dominated the year but has radically transformed the way we live and work, perhaps permanently for many people and businesses.

What the pandemic has brought into sharp focus, particularly for the telecoms industry, is just how critical digital infrastructure is to our everyday lives as well as to businesses across the globe, and the immeasurable role it plays in crisis management and business continuity during difficult circumstances.

Digital demand has increased significantly in 2020 with Ofcom's Online Nation 2020 report stating that time spent online has reached record levels because of COVID-19. Take video calling as one example, usage statistics have jumped from 35 percent of online adults using video calling at least weekly in the 12 months to February 2020, to double that by May 2020 with 71 percent using these services at least weekly, and 38 percent using them at least daily.

Elsewhere, retailers' primary outlets have been through two lockdowns, while education has become a more virtual experience with whole courses being digitised and Esports has moved from niche to mainstream as we've spent so much more leisure time at home.

Digital transformation has had to be advanced quickly in order to equip employees and solve problems that otherwise may not have been urgent. As a result, many businesses are relying more on connectivity as part of their working day. So what does that mean for telecoms industry in 2021?

Connectivity upgrades for town and cities

Deploying full fibre connectivity to cities and places makes them better connected and will enable smarter applications into 2021 and beyond. Full fibre for the UK by 2025 remains the ultimate goal but there is still a lot of work to be done to meet the Government's aim.

With more data being consumed than ever before, 5G rollouts will also continue at pace next year but cross-industry collaboration and support from local government will be crucial to making this a reality. Investment in digital infrastructure will need to be driven by Government schemes with both in terms of planning and funding; the role of telcos will be to find creative, non-disruptive ways of installing the necessary fibre to make it all possible. Utilising existing infrastructure, such as deploying fibre in the sewers, is one way we could expect to see the telecoms and utilities sectors working together.

Making use of Alternative Network Providers

The rise of the Alternative Network Providers (AltNets) will also help to better connect UK places, including the often more overlooked and underserved rural areas. This will deliver the benefits of lower bandwidth fibre connectivity (sub 1Gbps) for those companies not yet needing higher capacity services like Ethernet, but still wanting to experience the benefits and reliability that come with this type of solution.

A survey carried out in the Spring found that the AltNet sector ended 2019 with 50% growth year-on-year, up from 23% growth at the end of 2018, passing 1.2 million premises with fixed superfast or ultrafast broadband. And in spite of the obstacles that COVID-19 has posed, AltNets look set to announce another promising year of growth. Solutions like these will help to contribute to the Government's full fibre ambitions for the UK, in conjunction with efforts from elsewhere.

Cloud, SD-WAN and Managed WAN

With all being well, Spring 2021 looks set to be a much-awaited return to normalcy, with COVID-19 vaccinations well under way and hope that we will be over the worst of the pandemic. But this version of normality will undoubtedly look very different to

the one of years gone by. Working from home is likely to evolve into an enduringly hybrid solution of home and office working.

This will lead the telecoms sector to rethink their connectivity strategy to best support staff splitting their time between home and office. Increased screen time and reduced in-person interactions brings with it new challenges in mental health and wellbeing which will also need to be a priority on the employer agenda going forward.

Innovative tech responses will be required from the industry as business models adapt to the new normal more permanently – we can expect more digital first approaches when we travel, shop, eat out and go about our daily lives. Cloud, SD-WAN and Managed WAN will be increasingly relied upon to help businesses manage and protect their networks, navigating through increased bandwidth pressure and security threats in equal measure. I expect all of these to increase in adoption next year, along with newer solutions such as Unified Comms as a Service and even conceptual ones like composable infrastructure, all of which have similar intentions of better managing and scaling IT infrastructure and services.

The new normal

As public and private sector organisations look to accommodate permanent shifts in working patterns, 2021 will see the telecoms industry evolve to accommodate these new goals and supply the connectivity infrastructure necessary to make them a reality. The race for full fibre connectivity will be a priority for the telecoms sector but equally, the industry will need to work closely with local government and other third-part innovators to help make progress in the new year.

> Increased screen time and reduced in-person interactions brings with it new challenges in mental health and wellbeing which will also need to be a priority on the employer agenda going forward

Mattias Fridstrom
Chief Evangelist at Telia Carrier
www.teliacarrier.com

The role of the edge

"AS MORE EMPLOYERS continue to allow working from home in 2021, the Internet's role, particularly the internet backbone, will be more important than ever. Beyond this need for a robust and secure internet next year, there are other trends ahead."

"Once 5G services permeate the market, we will see several new players entering the edge game. The current mobile network operators will be challenged by companies that want to offer their services at its very edge. Additionally, the reality of where the edge truly lies will continue to be a debate in 2021. Although these new distributed edges are designed for low latency applications, they will still create enormous amounts of data that will end up being transported to larger, centralised cloud or storage facilities away from the edge."

The continued growth of hybrid networks

"The increasing reliability of the public Internet during recent years has seen it fast becoming a robust network delivery option for business applications. By using the public Internet, cloud services – that have been around for some time in the IT world - are also now much more accessible to everyone. Specific applications will still require dedicated cloud access, but the public Internet is increasingly being used as a pathway to applications and data storage in the cloud. The ease and availability of Internet access will prove to be a significant driving force behind this growing trend as we move into 2021.

As COVID-19 is forcing business to rapidly adapt to survive, the adoption of SD-WAN has become more critical than ever. The public Internet and SD-WAN provide services far better suited to addressing the need for rapid delivery of capacity and greater flexibility than the older "MPLS back-haul all traffic to HQ" thinking."

Network automation and AI

"Automation will get a kickstart in 2021, especially the automation of information flows and ways to access information in a completely different manner than before. The complexity of applications powered by 5G trends such as IoT will see billions of devices connected to the Internet. This will demand smarter network automation from automatic configuration, provisioning, assurance and orchestration of services. We will see growing interest in AI-powered zero-touch deployment of networks because they offer a higher degree of automation and less manual intervention - therefore, less risk of error and service degradation. At the same time, network managers will need a complete view of the "Big Picture" connectivity performance of business-critical applications – to manage key performance metrics and set the baseline for network automation for fault isolation and remediation."

The security of the Internet will remain vital

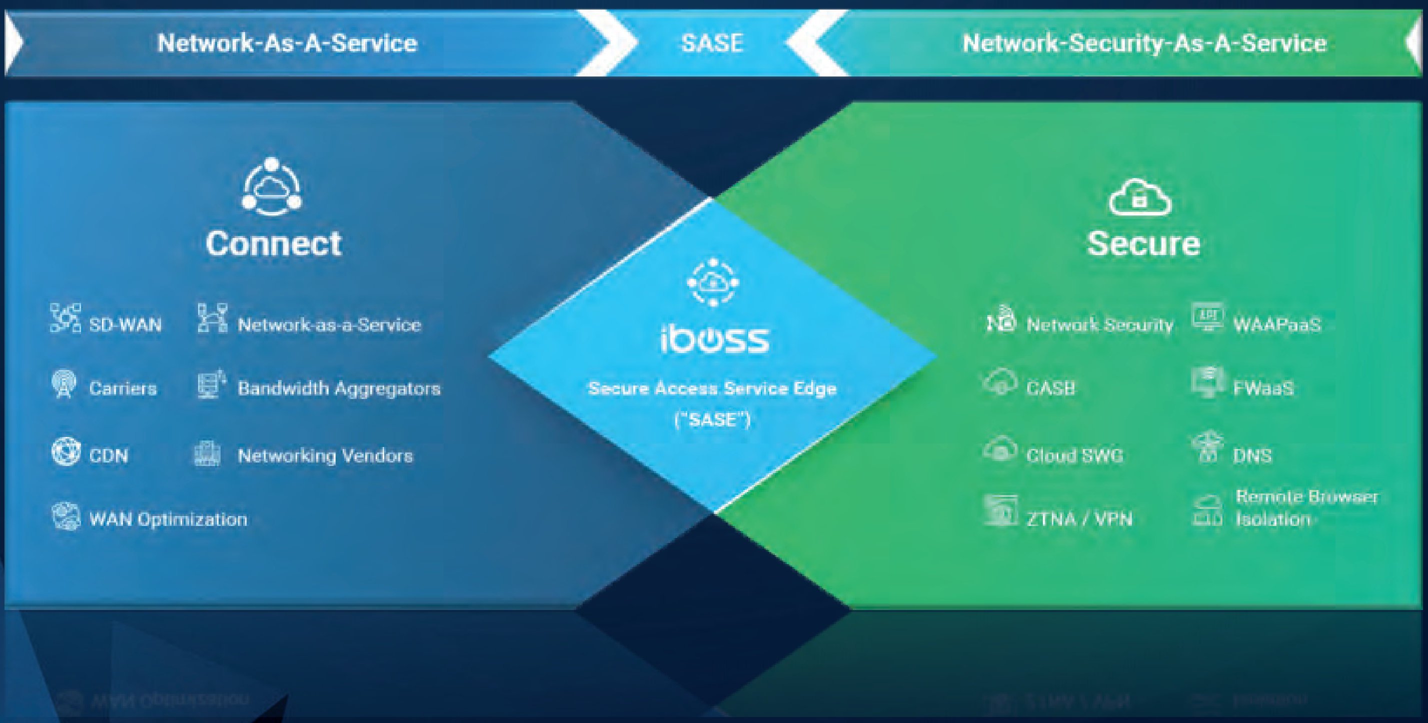
"Cloud technology and SD-WAN have totally transformed enterprise networking. There has been a constant increase of enterprises relying more on the public Internet for certain applications and that trend looks set to increase in 2021. While on-premise solutions, like firewall software protection will still provide one layer of security, it will become ever more important for Internet backbone providers to increase their security solutions.

RPKI will be implemented more widely in larger IP networks in the coming year to thwart attacks where hackers capture network traffic and divert it to unwanted locations. DDoS protection, which provides another layer of security that makes traffic on the public Internet much more secure, will also be enhanced in 2021. Global backbone providers will implement the higher grade of DDoS solutions to combat DDoS attacks with the quality of mitigation."

iboss®

Implement SASE and Zero Trust with iboss

Provide fast and secure connections to cloud applications for all users, including remote workers, with iboss



Network-As-A-Service | SASE | Network-Security-As-A-Service

Connect
- SD-WAN
- Network-as-a-Service
- Carriers
- Bandwidth Aggregators
- CDN
- Networking Vendors
- WAN Optimization

iboss
Secure Access Service Edge ("SASE")

Secure
- Network Security
- WAAPaaS
- CASB
- FWaaS
- Cloud SWG
- DNS
- ZTNA / VPN
- Remote Browser Isolation

DW INNOVISION
INSIGHTS + PERSPECTIVES

FINANCE

Digital finance companies are disrupting all aspects of the financial sector. What are some of the technologies which are giving them this competitive advantage, and how do the incumbents respond?

IN ASSOCIATION WITH
DW DATACENTRE SOLUTIONS
DW DIGITALISATION WORLD

ISSUE II 2021
digitalisationworld.com

From left to right:
Madhav Durbha and
Scott Donnelly at Capital Box

Consolidation, ecommerce and Brexit

"Small and medium businesses have been hit hard by the pandemic. To help the community that bolsters many of our economies across Europe, fintech companies have dispersed into new areas – using AI to help support those SMEs in need.

WE ARE CERTAINLY going to see more of this going into 2021. Finance professionals need to develop solutions to better serve their customers and invest in innovative technologies such as AI that will help them get closer to their audiences.

"In 2021, we will also see an increase in fintech consolidation, giving small businesses access to a broader suite of financial services capabilities. This year we have already seen the likes of American Express buy out Kabbage, and CapitalBox acquired SpotCap Global, one of the largest Dutch lenders. This type of activity will be even more prominent next year, from the lending space to emerging areas such as blockchain. For the smaller start-ups, consolidation will fuel and scale international growth and help them to rebuild, especially after such a challenging year.

"Next up, we have the ecommerce space which has taken advantage over the years of better payment options, from mobile to pay-later, these technologies have shown the industry the benefits they can bring to the business from a profits and customer experience point of view. The industry is growing more digital by the minute – from store closures to concerned customers wanting to stay safe, ecommerce is thriving and this isn't going to change anytime soon.

The use of chatbots, biometrics and blockchain tech have elevated the customer experience for good, and in 2021 fintech companies that facilitate, assist, or fund ecommerce transitions will thrive.

"We can't go into 2021 without of course mentioning the elephant in the room, Brexit. The US has some really big fintech players and in the UK, there are a lot of businesses in the space albeit small to medium sized. The real opportunities in fintech however, come from targeting smaller countries rather than large markets. With markets such as the US and UK, companies tend to trade internally as it is easier than getting to grips with multiple languages, currencies and regulations. The latter, are difficult to deal with, but if your fintech business can navigate multiple regulatory ecosystems, then there are some serious opportunities to take and have a bigger presence across the globe.

Brexit will be a benefit for continental fintech players next year, as it will add more regulatory hurdles for fintech companies looking to enter the market. However, it will be even harder to establish as a fintech in the UK. To get past this, the UK Government needs to connect players in the UK to larger players in the environments it wants to expand, and find a way to work together."

Shamus Rae
Founder and CEO, Engine B
www.engineb.com

Technology to the rescue

I DON'T KNOW ANYONE who will be sorry to say goodbye to 2020. Perhaps because the year has been so hugely challenging, most of us are keen not to look back but are gearing up to embrace the new opportunities presented by 2021. Despite and, in many cases, because of the problems thrown up by the global pandemic, innovation accelerated in 2020 and 2021 looks set to be the year when businesses and end users will begin to benefit from the fruits of this innovation.

As we faced the coronavirus pandemic and grappled with the fall-out, it was technology that helped make the best of a bad situation. According to a new McKinsey Global Survey of executives, companies have accelerated the digitisation of their customer and supply-chain interactions and of their internal operations by three to four years.

At the same time, the share of digital products in their portfolios has accelerated by an incredible seven years. Significantly, these innovations are not merely temporary solutions but are now here to stay.

Once specific technologies become embedded in so many daily interactions it becomes almost unthinkable for us to go back to a time when they weren't regularly and routinely deployed. It is this acceleration of technology innovation and adoption that has become the unexpectedly positive consequence of COVID-19 and its impact on 2021 will be far-reaching. How will this work in practice? Looking at the next 12 months, I think some key themes and trends can be detected, all of which highlight one overarching technology trend – a reduction in friction.

A deep dive into fintech

One industry that has been subject to high levels of tech disruption as a result of the pandemic is financial services. New fintech players have been changing the game for a few years now, but the pace of change has increased in 2020 and will continue to do so in years to come. These are some of the things we are likely to see in the sector in 2021.

The rise of the intelligent chatbot

Chatbots are nothing new. They are, however, becoming better integrated with artificial intelligence (AI) and Natural Language Programming (NLP), providing a more realistic, human interaction with customers, solidifying their place in the financial services industry. Fintech firms and digital banks in particular, have been beneficiaries of this technology by adopting chatbots to serve their customers. 2021 will see this trend accelerate, with innovations including OpenAI's GPT-3 and Google's Duplex leading the way.

AI will disrupt financial advisory

This has been on the cards for some time, but 2021 is going to see a real shift in perception around AI and financial advice. Barriers to the wider adoption of AI used in an advisory capacity were primarily about trust rather than technology and as AI technology develops and Open Banking becomes more deeply embedded in our lives, we will see levels of trust increase considerably as financial products and services deliver better outcomes.

Against this backdrop, the value of human financial advisors will become less clear and the value of AI in giving unbiased, bespoke financial advice will be better understood.

We will see more digitisation in insurance

Accelerated by the COVID pandemic, AI will be used more frequently to look at risk across supply chains and AI and knowledge graphs will be deployed to measure risk. Lemonade, currently shaking up the sector in the US, is likely to find its equivalent in other markets and its impact will be keenly felt by consumers and the industry as a whole.

Micropayments will explode

Concerns around security in this space will be resolved and micropayments will be run by robust systems that will mitigate any outstanding fears around the use of micropayments. We may see AI-based facial recognition technology rolled out as part of this process and the impact will be felt widely. This will put the customer in control, allowing them to pay at a more granular level for what they actually consume. It could also lead to some exciting developments. Could 2021 be the year when we see Teslas hired in 10 minute slots? Maybe!

Benoit Grangé
Chief Technology Evangelist, OneSpan
www.onespan.com

Better banking: OneSpan experts give their view on 2021

BANKS WILL INVEST IN ROLES dedicated to enabling data-driven decision making. We will see a rise in the creation of specific and dedicated roles within banks, such as the chief data officer (CDO), who will be responsible for the execution and delivery of the data-driven strategy within the organization. Chief Data Officers will play a critical role in the next normal that follows, as there’s never been such a vital time for CDOs to provide banks with timely and accurate data. These data leaders will help break down data silos in digital transformation teams to secure buy in from the C-suite and the entire organization.

The future of the banking sector is in the usage of more AI, machine learning, and biometrics and less passwords. A massive transformation is occurring across digital and mobile channels in how banks engage with their customers and use AI. Banks will combine machine learning with biometrics to provide new experiences, such as facial and fingerprint verification instead of passwords. O

ne example we’re already seeing is banks leveraging machine learning to detect and read physical passports to allow for ID scanning. Customers use their smartphones to scan a government-issued ID and then take a selfie. The banks then leverage biometric facial comparison technologies with liveness detection to verify that ID is authentic and unaltered, confirming the individual’s identity.

Digital Identity based on Self-sovereign identity leveraging blockchain will emerge. The development of a decentralized or self-sovereign identity will bring a complete evolution to the digital identity space. We’ll see the development of digital ID fully under the control of the user securely stored in mobile devices within digital wallet.

The complete ecosystem available for both public and private sector will leverage Distributed ledger technology as source of trust. We will also see the development of a standard protocol for issuing, ordering and verifying digital identities. By combining blockchain technology with standardization that can be made by regulators, self-sovereign identities will become the future of what today is a physical identity document.

Michael Magrath, Director Global Regulations & Standards, OneSpan
Digital identities and remote account openings will gain traction worldwide: Regulators in Hong Kong, Pakistan, Greece, Macedonia, Mexico and Turkey approved remote bank account openings in 2020 – a clear indicator that even processes rooted in traditional face-to-face meetings in the branch are now going digital and touchless around the globe.

Open Banking will grow rapidly throughout the world: As third-party providers (TPPs) are allowed to use banking information to help consumers save money, borrow more easily and pay efficiently, banks will increasingly work with TPPs. In the U.S., the Consumer Financial Protection Board (CFPB) issued an Advanced Notice of Proposed Rulemaking on consumer authorized access to financial data, which could be the catalyst for Open Banking in America. Facial recognition will drive the greatest changes to banking regulations: As banks increasingly use facial recognition technology for Identity Verification requirements, they are housing large amounts of consumer biometric data. Standards organizations such as the National Institute of Standards and Technology (NIST) and Fast IDentity Online (FIDO) Alliance and are developing frameworks that could be adopted at the national level and would stipulate how banks protect and store their customers' biometric data.

Regulation is on the way for cryptocurrencies: As digital banking platforms have experienced massive growth, many governments and industry bodies worldwide have begun to look to Central Bank Digital Currencies (CBDCs) and cryptocurrencies in terms of what they might add to the financial sector. This has resulted in new and refreshed conversations around the possible uses of CBDCs and cryptocurrencies.

Mark Crichton, Senior Director, Security Product Management OneSpan

The year the cloud is finally embraced by financial services. In today's turbulent economic climate, banks are looking to deliver secure online services at the lowest possible cost. And this is where SaaS solutions deliver the innovation needed in the most agile way possible. We will undoubtedly start to see banks make the shift to SaaS to remove overheads and refocus on evolving core services. Yet the financial sector is still behind the curve in its adoption of cloud due to its ongoing fear over privacy and data control to meet the stringent standards of GDPR and PSD2. As an industry, technology providers need to reassure banks and give them the confidence that it is possible to protect data anonymity and drive capabilities around areas including authentication, fraud and risk analysis to help them reap the rewards SaaS solutions have to offer.

Security technology has a proactive role in building the "next normal". I see the transformative change of 2020 as a call to action for organizations to view security software as a business enabler. The time is right to see the positive rather than negative in security: it has the capability to drive a frictionless user experience and with it better brand engagement. But to get there we have to stop treating security as an afterthought.

Institutions who set up and build security into their services from the start will empower positive user behavior to deliver improved trust. The arrival of mobile security is just one example of how a digital infrastructure and services will offer the frictionless banking experience the user now demands.

As more users engage on their mobiles, security is more readily received, identities more easily verified, and authentication requests accepted.

INNOVISION
INSIGHTS + PERSPECTIVES

APPS

It’s all about the application. Without the means of interacting with employees and customers via software applications, organisations wouldn’t need compute, storage, networks – any IT!

IN ASSOCIATION WITH
DATACENTRE SOLUTIONS
DIGITALISATION WORLD

ISSUE II 2021
digitalisationworld.com

James Maude
Product Strategy Lead at AppLearn
www.applearn.com

The enterprise software trends set to dominate 2021

WHILE THERE'S NO DOUBT that many enterprises, leaders and innovators have been driving the digital economy for some time, as we look ahead to 2021, the impact of the pandemic has placed digital transformation strategies firmly on the board agenda.

What we've seen over the past 12 months is a rapid acceleration of enterprise software implementation – largely driven by tactical short-term fixes – however, the next 12 months looks set to be defined by a far more strategic approach to digital transformation and adoption. This will be driven by actionable data insights and the desire to create a unified digital experience for employees.

Communication, Communication, Communication

We will continue to see rapid growth in communication tools as organisations try to move away from email marathons and the dreaded 'reply all' and look for better ways to communicate effectively. Increasingly, enterprises are looking towards communication 'in the flow of work'.

Being able to reach employees directly in business applications (in the flow of work) or via messaging apps is far more effective and more likely to succeed than mass emails. This could mean key business communications being delivered by an in-application pop-up or notification. Crucially, these types of communication can be context aware and only alert the user when they start the task you want to give them information on.

Solving the 'tap on the shoulder' challenge

Remote working is set to stay, and organisations will need to close the support and knowledge gap that was once served by asking a colleague on the next desk. Without 'tap on the shoulder' support, IT help desks can become overwhelmed with requests, productivity decreases, and the employee experience suffers.

This is why the Digital Adoption Platforms market is predicted to grow significantly in 2021 as organisations seek to improve the experience and effectiveness of employees with self-service guidance and support in the flow of work.1

Beyond robotic process automation (RPA)

RPA has been the hot topic in enterprise technology over the past few years, and while advancements in machine learning have made it easier to fully automate more complex tasks, many enterprises have found their productivity and ability to automate has plateaued.

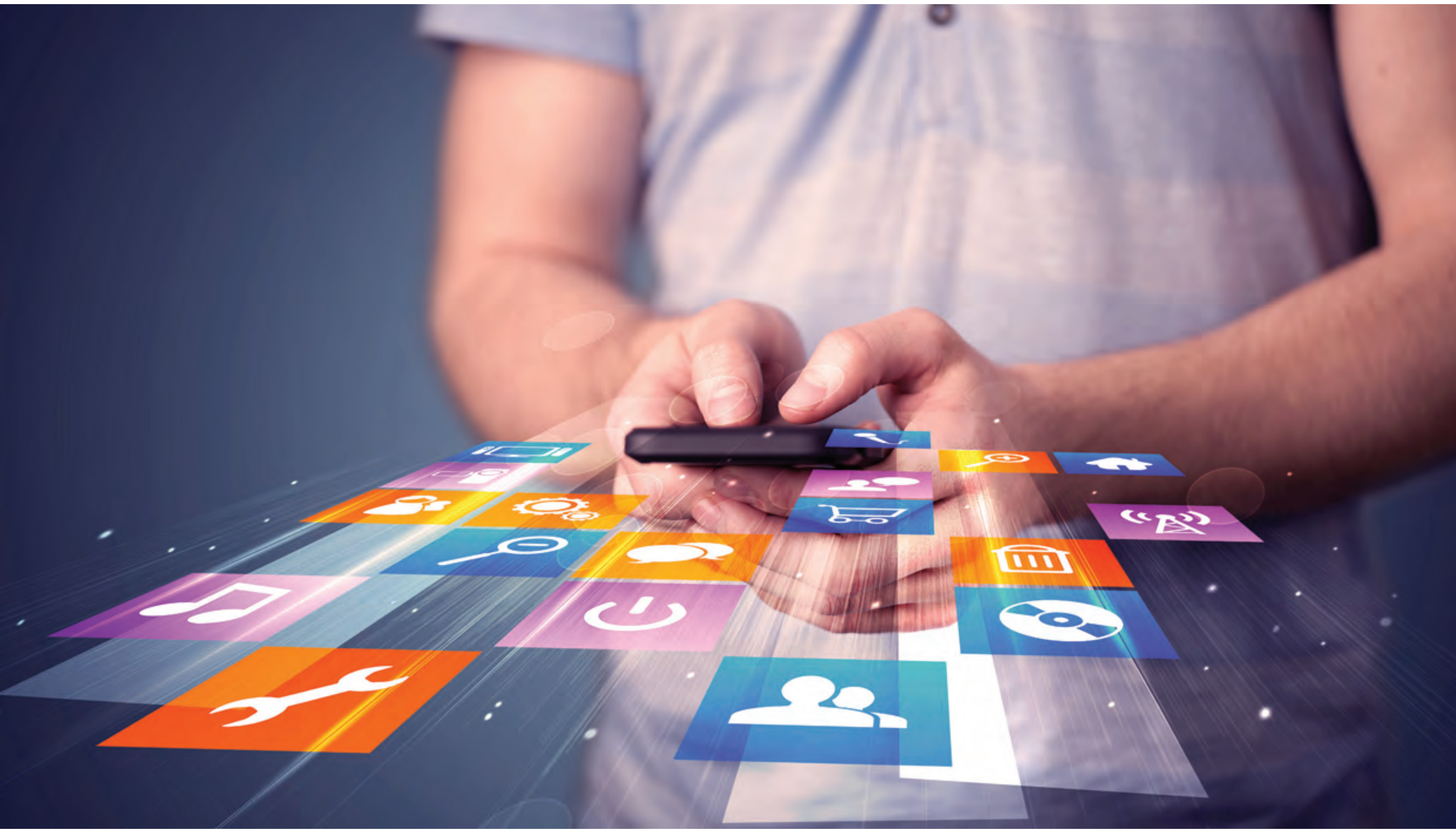
In 2021 the focus will shift from pure technology optimisation to people, as not every process can be automated. A two-pronged attack is needed, which strikes the right balance between automation technology and empowering people by providing guidance and support in the flow of work. Getting this right will be key to unlocking further efficiency gains over the next 12 months.

Insights and actionable intelligence

In an uncertain economic climate, proving the value of enterprise software and aligning this closely with business outcomes will continue to be a focus for business leaders. Most software vendors provide basic analytics based on number of logins or pages visited, however these don't show the true value or the true cost.

Insights such as how much time users are spending navigating to a task, where they need support or which tasks are repeatedly being corrected can make or break the success of digital transformation. With an increasingly remote workforce, it will be more important than ever to be able to track and monitor this user interaction and understand where the points of friction are.

In 2021, enterprises will be looking for ways to measure the ROI of their digital investments with insights and actionable



intelligence that allow them to drive continuous improvements. Providing greater visibility of productivity and cost gains will key to demonstrating how the right enterprise software can support organisations in meeting overarching business objectives.

Enterprises must prioritise a unified experience

If anything stands above the rest in 2021, it will be the need to unify the employee digital experience. The average employee uses over 35 applications for their day-to-day work and interacts with these over 1,000 times a day. The impact of context-switching – the action of flitting between multiple applications throughout the day – on productivity cannot be underestimated, especially when you consider the impact on the digital support experience.

When users are faced with a multitude of guides, chatbots, knowledge bases and support desks which differ from application to application, user frustration can become a significant problem. The solution? Consolidation of the digital support experience. Streamlining the experience and providing more targeted support in the flow of work which empowers users to solve problems quickly will increase productivity, while also having a positive impact on employee engagement and organisational loyalty.

Employee experience will be a key trend in 2021, with initiatives such as 'Experience Level Agreements (XLAs)' being introduced alongside SLAs to focus on outcomes and benefits rather than availability and capacity.

The organisations that will succeed over the next 12 months are those who understand that digital transformation is about people as well as technology and use the right tools to make software work better for their employees.

> If anything stands above the rest in 2021, it will be the need to unify the employee digital experience. The average employee uses over 35 applications for their day-to-day work and interacts with these over 1,000 times a day

What 2021 has in store for the technology and software industry

Philip White, Managing Director of Leeds and London based software developer Audacia, shares his top technology predictions for 2021.

THERE IS NO DOUBT 2020 has been a breakthrough year for software, with the global population becoming increasingly reliant on digital tools for work, social lives and their everyday household tasks, due to the COVID-19 pandemic.

But we have also seen the emergence of new technologies, which will in time benefit our day-to-day lives and businesses alike, from increased practical uses for VR/AR to the rise of no and low code platforms.

Here are some of the key tech and software trends we expect to be hitting the headlines next year:

Increase in citizen development

With businesses having to rapidly adapt to change, especially due to the recent impact of COVID-19 and Brexit, there is an increase in the demand for more individuals within organisations to innovate and implement change: introducing citizen developers, individuals with little or no software development experience using platforms, such as no-code and low-code tools, to build software application.

As the scope and size of citizen development projects grow, organisations will need to implement project management and security practices around these projects to ensure they do not become high-risk shadow IT projects.

Increased awareness of quantum computing

Quantum computing is fast-becoming reality, instead of a ‘technology of tomorrow’ ideal. Leaders in quantum computing are already beginning to launch next-gen quantum systems, with expected quantum volume greater than four million (qubits).

For businesses, these computers will provide next-level calculations and analytics in data, allowing them to identify and solve problems faster and on a greater scale.

More infrastructure as code

Infrastructure as code is the automated provisioning and management of computer infrastructure using code and configuration files.

The ever-increasing need for efficiencies will see this gaining favour across the board. Scenarios that would have previously involved staff manually can now be automated. This will mean fewer physical staff in data centres managing hardware, and an increased need for engineers to manage software-based platforms.

Increase in practical AI

Although AI has been the buzzword of tech for decades, we do predict a significant increase in AI in our everyday lives in 2021.

Practical uses of AI are already starting to make huge strides in logistics, with Amazon warehouses adopting AI automation technology for product collection and tracking stock. Machine learning is becoming mainstream, with technology such as chatbots and image recognition, that were once considered cutting edge, now de rigeur.

We will see this expanding to ever-more scenarios, with AR/VR in particular taking big leaps forward.

These changes and advancements in technology will undoubtedly benefit businesses recovering and adapting from the challenges faced in 2020, but they will also give us a clearer view of what certain industries will look like and operate like further in the future, as they increasingly move to become fully automated and cloud-based.

Martin Buhr
CEO and co-founder at Tyk
www.tyk.com

Key developer trends to watch out for in 2021

AS 2020 comes to an end, many businesses have had to make changes to adapt to the changing working environment. From collaborating remotely to closing customer deals over computer screens rather than face-to-face, the impact of how we work is set to continue in the coming year. As a result, many businesses have had to accelerate and reprioritise technology adoption that they had previously planned to implement in future years and the momentum created by creating technology solutions at pace, will be carried through into next year.

Central to this technology acceleration are the developer teams, who have adapted and innovated quickly to ensure business operations continue to function. This has increased awareness of the importance of the role that developers play in the business – and over the next twelve months, the developer community will start to play an even more strategic role within the business, through implementing new processes and procedures. This includes evolving the uses of APIs, the rise of low code as a developer tool, as well as the growing maturity of microservices. The background of Brexit and political disruption next year, will also play a key role for data sovereignty and business awareness of where data is held.

Here are six trends expected to dominate the developer community in 2021:

- **Organisations will venture beyond REST APIs**
There will be more emphasis on “the right protocol for the job”. We’ll see some distancing from the “REST is the only correct option” solutions emerge as developers embrace other solutions like GraphQL. There will be more Kubernetes adoption and advocacy, conversely a loud minority advocating for lowered complexity from the “anti-k8s” crowd.

- **The time for low-code is now**
There will be an increased emphasis on “low code” integration solutions. This will help developers better use their time on high value activities and empower others within the business to participate in developing technology solutions to meet their needs. Good low-code solutions will not only allow more people to develop their own apps, but shift developers into a more strategic role – moving from the doing to the overseeing.

- **Microservices gains maturity**
2021 will be the year that microservices grows up, becoming less focused on being “cool” and more productive. We’ll see it move from becoming less of a trend, and more of a pattern. Microservice capability and use cases will become better defined and will move through the “hype cycle” into the plateau of productivity, with appropriate changes to how organisations treat these migrations.

- **WebAssembly comes to the fore**
Serverless capabilities will be a focus in 2021, building on Fastly acqui-hiring Mozilla’s the entire WebAssembly (WASM) team this year. WASM as a whole will be a key theme for the year as it starts to move beyond the browser as more non-browser applications emerge.

- **Complex data politics**
Political disruption, including Brexit, will make 2021 a pivotal year for data sovereignty. Local cloud will increasingly be explored by organisations who will need to be more transparent with where their data is held.

- **The boom of APIs**
The impact of 2020’s mass move to remote working for many businesses will push APIs into the spotlight in 2021. Integration and internal use cases for APIs will be a big focus as organisations focus on “cleaning shop”. This year has shown the need for better digital ecosystems, as businesses can no longer afford to not be “digital first” companies in order to have the best chance of survival through the knock-on effects of recession and the pandemic in 2021.

The challenge for developers in the coming year will be to look at how they balance the increased demand from businesses to develop and implement solutions quickly, while at the same time focusing on high-value work that will positively benefit bottom lines.

This will mean we will see developers evaluating the tools and processes they are familiar with to ensure they are fit for purpose and can help them deliver the results they need.

DW INNOVISION
INSIGHTS + PERSPECTIVES

CHANNEL

Some thoughts as to how the
Channel can stay relevant
in an age when more and more
end users are heading
to the Cloud and adopting
managed services

IN ASSOCIATION WITH
DW DATACENTRE SOLUTIONS
DW DIGITALISATION WORLD

ISSUE II 2021
digitalisationworld.com

Keith Jackson

Regional VP Channel, Sales EMEA, 8x8

www.8x8.com

The Channel in 2021:
lessons learnt and a look ahead...

2020 has seen the rapid deployment of digital technology as businesses responded to the challenges the pandemic bought with it. In 2021, organisations will start reviewing these technology decisions, assessing how they align with long-term digital transformation goals.Many organisations will be looking to deploy more sustainable technology solutions to support their business.

Mass remote working this year has led to a significant shift in operations; business leaders will need to consider how this will impact both employee working models and recruitment and retention efforts in 2021. Partners should step in to ensure customers are fully supported when considering these transformations, helping them deploy solutions tailored to their needs. There are also a few key technology areas that will shape partner focus for the next year; cloud-based SaaS products, which include collaboration tools, and connectivity will continue to rise in demand. This will also be combined with further widespread cloud adoption across the public sector amongst other industries.

Stepping up, into the cloud According to Gartner, 48% of employees will work from home, even after the pandemic, compared with 30% pre-pandemic. As such, cloud adoption has seen a significant increase, and will continue on an upward trajectory. In the consumer world, people have been using cloud services in their day-to-day lives for many years, from Apple's iCloud and the ability to store documents online with Google Drive. The business world is only now catching up to pace of adoption, with many forced to invest in cloud technology in the face of the crisis this year. In 2021, partners will need to strengthen their cloud solutions and services as competition intensifies in this space, positioning themselves as trusted advisors who can support both migration to the cloud or those who wish to continue their journey in the cloud.

Connectivity for all

The shift for many organisations to operate from anywhere has driven a clear focus for consumer-based network providers to increase reliable connectivity for all, regardless of location. With remote working here to stay, even in a hybrid capacity, network providers will need to work hard to support a significant uptick in demand for their services with minimal disruption.

The rise of collaboration tools

Collaboration tools have made the headlines this year manu times, but according to the latest 8x8 survey, they're still not helping employees to be their most productive. We recently conducted research into the experiences and habits of SMB employees, a group that has been under particular strain this year. Results revealed

that these workers are experiencing pressures around the work from home environments, which are restricting their ability to collaborate with colleagues and support customers, remotely.

We also found that for just over half (53%) of SMB employees, the communication tools their company has in place isn't actually helping them to do their job more efficiently. The benefits of addressing these issues are clear, as 44% of SMB employees believe that, with effective communication tools, productivity would be the most improved business challenge.

In 2021 we expect to see businesses of all sizes look to further future-proof their communications strategy, in order to stay ahead of their competition, retain and attract new talent, and most importantly, for business continuity.

Transformation in the public sector

The public sector has dramatically transformed in the last nine months. Due to the essential need for many public services, such as NHS helplines and local council support, organisations have shifted to a largely remote operation, but also continued to support their communities at a time of crisis. Sefton Council, one of 8x8's customers, rapidly deployed 8x8 within just 10 days earlier this year during the initial COVID-19 outbreak. The council rolled out several advanced platform features, such as skills-based routing and speech analytics to increase call efficiency and support the increase in call volumes

The Open Communications Platform™ enabled them to achieve not just quick first contact resolution, but broader visibility of the customer experience to factor in future improvements.
We can expect to see more of these transformational stories, which will go beyond the technology itself, but focus on providing a seamless, multi-channel end-user experience, for both customers and workers.

The role of partners in 2021

While cloud communications technology has been around for many years, we are now witnessing exponential growth in the market. As hybrid working becomes a commonplace for many industries, partners will need to work closely with their customers to understand their specific needs, and translate that into finding the right technologies and services for them. It's been a tough time for many businesses this year, and never been a better time for the channel to support clients align their technology goals in 2021 and come out of 2020 stronger, more resilient and ready to embrace a new era.

Karl Roe
VP of CSDT at Nuvias
www.nuvias.com

Time to automate the Channel supply chain

IF THE PANDEMIC has taught us one thing in the Channel it is the importance of resilient and agile supply chains. With factories shutting down and businesses operating at times with reduced staffing levels and working remotely, supply chains have been stretched and tested like never before. Couple this with the extreme fluctuations in demand for products such as security systems which boomed at the start of the pandemic and it has clearly been a very challenging time for the Channel.

However, learning lessons from this, adding automation and increased visibility into supply chains, will enable Channel partners to deal better with future challenges, adding greater resilience into a fundamental component of a good customer experience.

One example of an industry that has met similar supply chain demands successfully is retail, and particularly supermarkets. While we all experienced a short-term shortage of food and household goods in the early days of lockdown, brought on by panic buying, supermarket shelves have remained well stocked since. Supermarkets' ability to rapidly respond to changing market conditions is supported by their investment in digital supply chains, enabling them to maintain a consistent flow of products into their stores.

2021 is the year for the Channel's supply chain to digitally transform

Despite the good example set by supermarkets, other industries still have room for improvement in terms of transforming the supply chain to minimise the risk of disruption. With the pandemic set to continue well into 2021, and a potential no-deal Brexit causing challenges for businesses trading across borders, it is time for the Channel to practise what it preaches and futureproof its business through its own digital transformation.

Integrated supply chains, where vendors, distributors and partners have uninterrupted visibility over the flow of orders, are a priority. For all businesses – including the Channel – intelligent automated systems are what is required to adjust to changing customer requirements. Making the change now, means Channel partners can look to sustained, long-term growth prospects by gaining more effective control and swift management of supplies, generating faster sales cycles, with greater resilience and operational cost reductions.

Leveraging the power of automation will inform the transition to more efficient and productive systems and tools that underpin business growth. As Brian Burke, Research Vice President, Gartner, put it in Gartner's Top Strategic Trends for 2021: "Everything that can and should be automated will be automated"

A matter of survival

2021 is the year the Channel 'eats its own dog food' and digitally transforms itself. This process needs to start with the supply chains, as they have a considerable impact and deliver high value. The pressure to adopt an automated supply chain will continue to grow in 2021; as it shifts from a 'nice to have' to a 'business critical'. Focusing on streamlining and, where possible, automating systems and processes will enable Channel partners to effectively control and manage the flow, have greater resilience and provide a better all-round customer service. Not only will this aid with managing the impact of COVID and Brexit but also ensure Channel supply chains can handle whatever comes next.

Johannes Kamleitner

VP of Global Channel Sales at SolarWinds MSP

www.solarwindsmsp.com

2021 is set to be another pivotal year for the channel

AS THE PANDEMIC SPREAD across the world in early 2020, MSPs stepped forward to support, protect and secure their customers. Many facilitated the mass move to remote working for clients (in tandem with managing this process for their own businesses), combatted the rise in security threats, and migrated business processes to the cloud. MSPs focused on doing the best job possible – and the agility, proactivity, and support they provided shifted the perception of MSPs. Overnight, the pandemic reinforced that MSPs are integral strategic partners for their clients as extensions of business continuity teams, rather than merely "third-party service providers."

Next year, MSPs will have to rise to a new challenge: sustaining

the digital transformation trajectory for clients. As offices re-open, hybrid working policies will be implemented and the focus will move away from technology back towards core business propositions. MSPs must continue to spur clients along their digital transformation journeys, reinforcing the value they bring yet again for the key changes businesses must further embrace including a more direct shift to the cloud and an ever-increasing focus on security.

The “new different” of 2021 will bring different challenges and growth opportunities for the channel. MSPs will continue to prosper as they deliver increased value as a trusted partner, building on the relationships they have strengthened in 2020.

One of the key growth opportunities will be cybersecurity. When employees were working from offices which deployed the highest network security solutions possible, security was still an issue. Now that they are working from home, it’s an even bigger issue. And once hybrid working is in full swing, with people using their homes, coffee shops, and restaurants, as well as their own office spaces, security will become even more paramount. It will be primarily about data protection, and how to keep that data secure amid this new hybrid world.

This opens an opportunity for MSPs to expand their proposition, securing not just offices and a few devices, but home environments and a range of different devices too. And the best part – the tools MSPs already use are made for this extension. The other key area of opportunity will come from businesses making the next big digital leap. We’ve already seen restaurants launching apps to provide takeaway services, opticians experimenting with online appointments, and a boom in e-commerce – this move into the online arena will only accelerate.

With more businesses becoming digitally savvy and experimenting with online innovation to reach new customers, this opens the door for MSPs to guide businesses through this transition. Tapping into their wealth of expertise, MSPs are in prime position to provide digital inspiration to clients, walking them through the process and operationalizing innovation.

However, 2021 will take its toll on the MSPs still using the “break-fix” business model. The break-fix model is rooted in being reactive – it is only once something breaks that the MSP steps in. But given today’s climate, businesses need proactive support and guidance. For example, businesses need partners that can help detect and prevent a security breach from happening, not someone that can try and fix the damage that has been caused after the attack has taken place. As the needs of businesses change, MSPs must align their business models – and this means taking the next growth step and moving to a managed services model.

With businesses now more aware of the importance of cloud migration, leveraging data, monitoring employee productivity and enhancing security, this newfound reliance on technology is creating a crucial role for MSPs as strategic consultants. There is opportunity there for the taking for MSPs to fully evolve into the trusted advisors their customers need which in turn, will help them strengthen the long-term value they deliver and help them reduce customer churn. MSPs must rise to the challenge and act if they are to maximise their value in 2021.

> One of the key growth opportunities will be cybersecurity. When employees were working from offices which deployed the highest network security solutions possible, security was still an issue. Now that they are working from home, it’s an even bigger issue. And once hybrid working is in full swing, with people using their homes, coffee shops, and restaurants, as well as their own office spaces, security will become even more paramount

INNOVISION
INSIGHTS + PERSPECTIVES

MISCEALLANEOUS

Just because these topics don’t have their own section, doesn’t mean they are not important! Here we’ve gathered together thoughts on: transport, DevOps, defence, sustainability, open source, quantum computing, remote working, 5G, edge computing and the supply chain

IN ASSOCIATION WITH
DATACENTRE SOLUTIONS
DIGITALISATION WORLD

ISSUE II 2021
digitalisationworld.com

Daniel Quelch

Sustainability Manager at Epson

www.

The rising importance of green office technologies

There's no denying that the pandemic has changed the face of global business in countless ways – and at an unimaginable speed. The impact of this has been felt by every sector, everywhere – and the IT industry is no exception.

Across the world, health and safety concerns as well as government rulings have enforced a mass shift in the way people do their jobs. As a direct result, workers abandoned offices for months on end, setting up new workspaces and creating brand new working habits.

While much of the news throughout the coronavirus crisis has been unsurprisingly negative, there have also been some positives, one such example being the effects of mass home working on the environment.

With fewer people travelling and many industries forced to pause production, we saw improvements in air quality and lower greenhouse gas emissions, and the planet became an unlikely beneficiary of the outbreak. The positive images of our planet seemingly beginning to reset and recover has created a

resurgence in how consumers and businesses alike think about the impact of their day-to-day habits on the environment.

For the IT sector specifically, these unprecedented changes and a shift in thinking are hugely important and needed – but could equally leave many organisations unable to keep pace with the expectations of an increasingly environmentally aware generation of employees and customers.

Matching eco-expectations

Companies will increasingly be forced to align their IT strategies with new green expectations – or risk losing out. Without an eco-conscious mindset, businesses risk alienating talent and struggling with staff retention, particularly amongst Millennials and Gen Z, who hold such values in high regard.

According to our recent global research into the eco-values of workers, 65% believe that the environmental and social impact of a business will be more important post-COVID. The findings also show that 81% of workers consider the environmental and social credentials of their employer to be important, yet only 24% believe that businesses are actually making an effort to prioritise these things.

In order to bridge this gap in expectations and remain competitive, sustainability has come from nowhere to being third on many business decision maker's agenda when it comes to deciding factors in the buying process of technology, according to the same research.

Office technology has a large role to play in closing this gap and pushing forward the future of business sustainability. By choosing to use 'green' technologies, such as heat-free inkjet printers that reduce CO2, energy and water use, IT teams can help to future-proof their businesses and keep employees happy.

Bigger trends such as pollution and green energy sources tend to dominate the wider conversation when it comes to sustainability, but IT decision makers should not underestimate the power in making smaller sustainable choices to make big environmental changes. Now is the time for those in IT to consider the long-term benefits of purchasing 'green' office technologies, because true sustainability takes time and needs to begin somewhere.

By installing sustainable office solutions such as inkjet printers and cutting-edge technology such as PaperLab – the world's first in-office paper making system – businesses can save on operational costs and reduce their carbon footprint, as well as help to contribute to the creation of a circular economy.

At the same time, these green choices demonstrate a willingness to place environmental matters in high regard, which is attractive to customers and employees – both existing and prospective.

The pandemic has woken us all up to the need for greener solutions for businesses and changes to our buying habits, and 'green' office technologies can help make a significant contribution to brand's environmental and social credentials. More than ever before, it seems that this focus isn't going away. As the world attempts to return to some sort of normality, IT business leaders have the opportunity to reassess their priorities and need to continue this sustainability conversation throughout 2021 and beyond.

By installing sustainable office solutions such as inkjet printers and cutting-edge technology such as PaperLab – the world's first in-office paper making system – businesses can save on operational costs and reduce their carbon footprint, as well as help to contribute to the creation of a circular economy

From left to right:
Johnathan Hunt, VP Security
and Cindy Blake, Security
Evangelist at GitLab

GitLab predicts 2021 to be breakthrough year for DevSecOps uptake

Innovations help enterprises overcome cultural barriers to adoption

GITLAB, the single application for the DevOps life cycle, is predicting a breakthrough year in 2021 for DevSecOps adoption, as EMEA organisations begin to embrace the cultural change needed to truly shift security left in software development cycles – with DecSecOps' emerging capabilities being a key driver in this change.

The company also says that as security shifts left and more companies move their operations to the cloud, developers will begin to claim more and more responsibility over security within teams.

Johnathan Hunt, VP Security at GitLab explains: "At the start of the transition to applications, security was largely left behind. However, as enterprises adjust to new in-Cloud stacks, and IT becomes an application, they will no longer need an IT solution but an application security solution, demanding new approaches to owning security. And while the layers of the stack remain the same, responsibility for who owns security and decision making at the layers in the cloud will change.

Successive research has indicated that internal cultural barriers have often prevented development teams from realising DevOps' full potential: analyst IDC has estimated that by 2021, 80% of European organisations will adopt DevOps, but only 10% will excel in terms of accelerated performance and delivery cycles. GitLab's own survey of 3600 developers released in May this year suggested a lack of clarity within companies as to who is responsible for security efforts – more developers (25%) say they feel solely responsible for security than testers (23%) and operations professionals (21%).

An emerging reason for development teams' embrace of DevSecOps practices are innovations that simplify and automate tasks such as security testing of code. For example, GitLab enables security scans to be run inside its CI/CD pipeline - with security baked in, rather than being tacked on at the end, as so often happens with other solutions. This integration and automation encourages better software development, promotes more effective developer collaboration with security teams, and ultimately allows organisations to innovate faster.

Cindy Blake, security evangelist at GitLab, states: "Shifting security left was previously an ambition for many organisations, but I predict we'll see enterprises make practical and cultural changes to bring this about – in particular, moving farther away from a developer system that relies on security checkpoints.

"I think in the name of efficiency, expediency, and protecting the cloud, developers in 2021 will increasingly own checking for vulnerabilities and adjust accordingly throughout the process and take a more collaborative, top-down approach to security."

Craig Beddis
CEO & Co-Founder, Hadean
www.hadean.com

Why is the defence sector creating the metaverse?

THE METAVERSE is gaining traction. Never before has Neal Stephenson's idea of a virtual world where we communicate through avatars seemed quite so appealing. With many of us unable to attend traditional social outlets, a virtual alternative seems both helpful and logical. So what does the metaverse look like? From one person to the next you'll get a different answer, but these loose definitions all possess certain common threads. The idea of a perennial, persistent virtual world that many of us can connect to is an integral tenet. Such a world will be a social platform, with its own physics, economies and artificial intelligence. Recent advances in distributed computing and networking are making a sort of extended massive scale Second Life seem a very real possibility. Quite how the metaverse will continue to evolve though is dependent on the development and adoption of various nascent technologies, such as VR, AR and XR.

The pursuit of these grand scale virtual worlds is unsurprisingly spearheaded by gaming companies. Those already familiar with building vast open worlds, are looking at how to populate them with ever increasing numbers of interacting players to partake in anything from concerts to sports to graduation ceremonies. What perhaps is a little more surprising is that the defence sector is also at the forefront of advancing the metaverse through its early life. Although on the surface quite different industries, the defence and gaming sectors have somewhat fairly intertwined history when it comes to technology. Simulation and gaming engines play a key role in either recreating historical events or map potential future scenarios. This can refer to anything from disaster planning through to construction projects. The long-term goal is to use gaming tech to create single synthetic environments, capable of accurately modelling geological phenomena, manufacturing processes, cityscapes, and even human behaviour to inform strategic planning and decision making. The immediate appeal of this to those in the defence sector is the opportunity to create interoperable, multi-echelon simulations without the logistical or practical issues typically associated with large scale training scenarios. It would synchronise training efforts, highlighting the impact of anything from the weather and terrain to the movement of people - at the point of need. At the same time, data and credentials could be shared across a geographically distributed network. This of course is somewhat easier said than done. Creating a living breathing simulation of a real-world counterpart that synthesises a huge amount of data into a single coherent viewpoint requires a massive scale robust infrastructure across a distributed network. Most computing models are ill-equipped to handle the computational complexity derived from the volume of entities, data or rapid structural changes.

And yet, the metaverse that the defence industry is looking to design, involves bringing all the varying layers of a simulation including the terrain, satellite networks, IoT devices and human behaviour under a single architecture. Moreover, connecting so many users and entities into a single viewpoint lays the groundwork for iterations of the metaverse that the general public might expect to consume - such as large-scale social platforms inhabited by thousands of people across the world. Ultimately, the strides made in recreating the real-world will have profound implications for the technology that underpins the metaverse. But to be successful, it requires an overhaul in the distributed computing technology stack and infrastructure, whereby access to near unlimited processing power enables immersive, complex and high-fidelity simulations. It is the defence sector, not just gaming or virtual events industries, at the forefront of this innovation.

Roger A. Grimes, Data Driven Defense Evangelist at KnowBe4

Quantum is coming

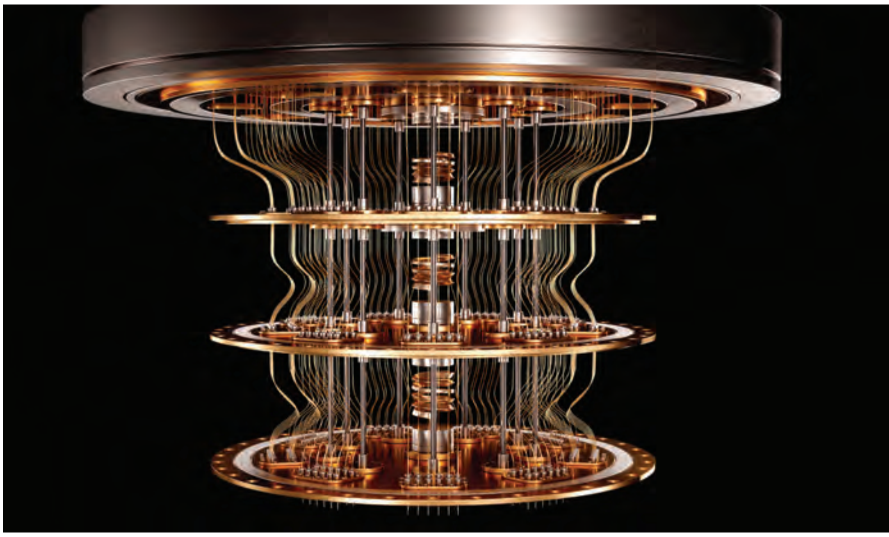
The 26-Year wait for the coming quantum break is likely to be in 2021

IN 1994, Peter Shor figured out that quantum computers, when we invented them, would be able to crack most traditional public key (asymmetric) encryption ciphers. The news of Shor's algorithm hit the computer crypto community like a bomb! Everyone immediately understood the ramifications.

Once quantum computers, with a sufficient amount of stable quantum bits (called qubits), were invented, the encryption and digital signing that 90% of the digital world (e.g. RSA, Diffie-Hellman, TLS, HTTPS, digital signatures, etc.) relied on would be toast. Back then, as amazing as Shor's finding was, it wasn't as threatening because we didn't have any quantum computers. We were not even sure we could make them. Many experts believed that quantum computers were in the realm of science fiction. Then, in 1999, the first quantum computer was invented. All that was needed was a sufficient number of qubits. It takes about 5000 stable qubits to break most of the world's asymmetric encryption keys and under 10,000 qubits to break the strongest.

Publicly, the number of announced stable qubits announced in 2020 is under 100, but there are literally hundreds of separate companies and projects fighting to get to the Holy Grail of quantum computers, with 5000 to 10,000 stable qubits. Once that happens, the "quantum crypto break", as it is known, will irrevocably break most of today's traditional asymmetric encryption (and weaken by half all of our symmetric encryption). The question since 1994 has been when is the quantum crypto break going to happen?

I think it is likely to happen in 2021, if it hasn't happened privately already. Why do I think this coming year will be the year when Shor's thought experiment finally gets proven? Well, it's a few things.



First, the hardest part of quantum computers… inventing quantum computers in the first place and getting a bunch of stable qubits has already been done. The part that, if impossible, would have killed the threat, but it was accomplished! All that's left is to create more stable qubits. And if there is anything that the US (and Asia) is good at, it is taking a few of something and turning it into a million of something.

Second, there have been a handful of algorithms invented since Peter Shor's 1994 algorithm that can more efficiently break ciphers. Shor's algorithm, requiring double the number of qubits as the private key you are trying to break, is a ceiling, not a floor. So, today's quantum computers need less stable qubits than Peter Shor predicted in order to be successful.

Third, there are hundreds of companies and projects working to create very powerful quantum computers. Nations are spending tens of billions of dollars a year (in just what we know about) to be the first nation to powerful quantum computers. It is a moonshot-level of international resources built to accomplish a single objective first. We landed on the moon. We will soon have powerful quantum computers…and not just to break asymmetric encryption. Quantum computers will impact every industry and give us solutions and inventions we cannot imagine right now. Quantum

computers will change our world in the same way, or more, than the Internet already did.

Fourth, new quantum inventions are appearing and being announced all over the place. Quantum computers are just one type of device relying on qubits. Outside of the quantum computing world, quantum networking devices, quantum networks, and quantum random number generators are appearing with more regularity and versatility. Several projects and universities continue to make symbiotic improvements that will soon lead to quantum-on-a-silicon chip. The days of quantum computers needing super-cooled, extremely isolated, conditions will be coming to an end. You can even already get a quantum random number generator included on a regular cell phone today. Am I supposed to believe that the rest of the quantum information sciences world is making significant, consistent, advances, but the quantum computer vendors aren't. Sorry, it's a bridge too far for me.

Fifth, I have many friends and acquaintances who are actively working on quantum computing projects. Some of them have shared with me that they expect to have tens of thousands to hundreds of thousands of qubits within a few years. If that is the case, it makes sense that the first few thousand could be achieve this year. Quantum computing power has been somewhat irregularly, but overall, consistently following or exceeding Moore's law that has successfully predicted traditional, binary, computing power for three decades. Using Moore's Law on quantum computers predicts that 2021 would produce a few thousand qubits as compared to past accomplishments.

Sixth and last, the quantum computing world, after years of nearly public monthly bragging announcements, has gone suspiciously quiet. For years I could tune into multiple web sites to learn what quantum computing vendor had accomplished what when. Did they improve error correction or increase gate decoherence time? Did they move from 64 to 72 qubits? Did they achieve quantum supremacy yet? After years of lots of public information from the vendors themselves, most have gone quiet. It's as if the industry has collectively achieved or on the cusp of some huge announcement, and we are some sort of quiet period.

To be clear, I don't know when the coming quantum crypto break will happen. No one has teasingly told me that it is about to happen. If someone knows, they aren't sharing publicly with anyone. But at this point, with all the continued quantum advancements, I'd personally be more shocked if the quantum break wasn't accomplished and publicly acknowledged in 2021, than if it was.

By Job van der Voort
CEO and Co-Founder, Remote
www.remote.com

Remote working: 2021 and beyond

2020 has undoubtedly been a year of change. Covid-19 and social distancing measures have encouraged businesses to adapt to new ways of working. In particular, many adopted remote working — something they likely hadn't even considered before.

Looking ahead to 2021, I predict that this culture of remote work, which is brand new to many, will not only continue as it currently is, but elevate even further.

For example, next year we will see more professionals choosing to work from anywhere, rather than simply working from home. And this is inclusive of everyone — not just digital nomads.

Remote work means that professionals can choose to move countries, move back to their hometowns, or get out of the city and into the countryside. In fact, recent research has revealed that 71% of UK tech employees would move to a different country and 8% would move to a different region if they were able to work remotely and retain the same job and remuneration. As a result of this, it's likely we'll also see more remote businesses hiring overseas, enabling an even wider talent pool as geographical restrictions are removed. This will benefit the end user, because businesses will be able hire the best talent available, regardless of where a person is based.

In 2020, many businesses turned to remote working in order to survive the pandemic, but it's vital businesses don't view this as just a temporary fix. Looking to the future, businesses will have to choose to make remote working part of their longer-term strategy if they truly want it to be successful.

I believe the remote working model can only be successful if everyone is remote, so if some employees choose to return to the office in 2021 while others continue to work remotely, this will inevitably have implications on the company's efficiency, productivity, and overall culture. This hybrid model is very hard to maintain: the threshold for asking a colleague something when walking by — and not ever documenting it or sharing it in a way that is accessible to remote workers — is very low.

Remote first means providing all employees with the necessary tools and equipment to do their job from wherever they want to work. Remote working must infiltrate team culture, perks, and benefits. In 2021, businesses must decide whether they're enabling a remote-first or a remote-friendly culture.

What's more, businesses will have to rethink what they offer to attract and retain talent. An on-site gym or free office breakfast won't work with remote teams. HR managers will need to consider teams who work across multiple countries with different cultures and expectations when it comes to benefits. This will become even more important in 2021 as more businesses adopt remote models. Research from earlier this year revealed that almost half of organisations believe that positive workplace culture is essential to success. To create an appealing culture for remote workers, businesses must embrace benefits designed for a remote-first culture. These could include home office stipends, flexi-time, or asynchronous working. Healthcare, home office allowance, and personal development plans or learning development allowances are the most sought-after perks.

Some may be concerned about the impact of wider remote working in 2021. For instance, how will impromptu "water cooler conversations" be replaced when working remotely? But as long as companies make a conscious effort to employ methods of social connection and wellbeing, those conversations are not lost. In fact, we find that working remotely can improve an employee's wellbeing because they spend less time commuting and less time away from their families, so tend to be happier at work and more productive. That will lead to better experiences for customers and end users. Of course, remote working will introduce other challenges in 2021. There is the debate around wages for remote workers: should companies offer a flat-rate salary across the world, or tailor salaries according to location? And businesses which attempt a hybrid work model will need to address the inevitable friction between office-based and remote workers who may receive different salaries and benefits.

But these are challenges worth overcoming. While many companies adopted remote working out of necessity in 2020, in 2021 they will do so by choice, because they recognise the benefits that remote working offers.

Wolfgang Wörner
CEO, Sixfold
www.sixfold.com

Three reasons why businesses must embrace real-time supply chain visibility in 2021

THE SUPPLY CHAIN and logistics sector has faced some significant challenges in 2020. Supply chains have continued to become increasingly sprawling and complex, making it harder than ever for international businesses, shippers and carriers to gain accurate insights into what's going on across their networks.

This is an issue that has been enhanced by the disruption caused by Covid-19. At a time when transparency and agility are more important than ever, many businesses have been left with no overview into the movement of goods.

That's why it's time for operators to rethink how their supply chains operate. As we look ahead into the new year, success will depend on how effectively businesses are able to gain accurate insights into the location and status of shipments and use data to make informed decisions.

This is what will drive adoption of real-time visibility in 2021 and beyond. Businesses must be prepared to embrace the technology and unleash its power for three key reasons.

Driving efficiencies

The pressure on supply chain and logistics businesses to optimise their processes will only grow in the future. This will put an increasing emphasis on enhancing efficiency – both from a cost and an operational perspective.

Issues such as inefficient freight tracking have traditionally caused businesses problems. It can be very time-consuming and labour intensive to get an accurate status of a customer order, often requiring staff to make repeated calls and manually send requests by email and fax for status updates.

Real-time visibility eliminates these issues by making the location and status of shippers and carriers instantly available, thereby enabling businesses to automate processes and optimise their supply chain operations. In turn, this feeds into the cost-efficiency challenge by giving businesses the tools to manage people and resources more effectively – creating savings that have a direct impact on the bottom line.

Amidst so much uncertainty, driving efficiency and productivity will be a key priority for businesses in 2021. By providing access to comprehensive insights into what's happening across their logistics networks, real-time visibility will have a vital role to play.

Dealing with disruption

One thing Covid-19 has clearly demonstrated is the importance of supply chain resilience. Businesses must have the flexibility to

adapt to changes as they appear and quickly adjust to whatever new challenges come their way. This flexibility is heavily dependent on having complete visibility into operations. For example real-time visibility eliminates blind spots and identifies issues – such as shipments delays, loss or damage – before they result in more costly disruptions further down the line.

We've seen how government measures can have a knock-on effect for logistics and supply chain operations, when restricting the free movement of goods during the pandemic caused significantly longer border crossing times in many countries. With Brexit on the horizon and delays already mounting up at UK borders, this challenge will likely intensify for European businesses in 2021.

But, by accessing real-time data and predictive insights into which trucks are running late or likely to get blocked at borders, businesses can react – such as by rerouting trucks – in a fast and informed way. These operational insights will be crucial for more robust, flexible and agile supply chains.

Empowering execution

Finally, businesses will see the greatest added value of real-time visibility come when visibility data is integrated with transport execution, and when AI and machine learning capabilities are applied to improve and automate decision-making.

In 2021, this form of 'predictive transportation' will create value for the entire ecosystem - suppliers, retailers, shippers and carriers. For example, it will let transport orders be assigned to the best-equipped carrier based on big data analytics, as well as enabling dynamic rescheduling of time slots with the help of AI. It will also reduce empty mileage, helping businesses cut CO2 emissions and hit sustainability targets.

Ultimately, businesses can't afford to have a partial view of what's going on in their supply chain networks if they want to drive growth in the future. Businesses can no longer afford to ignore the benefits of real-time visibility. With the potential to fundamentally change logistics operations, we will see the technology come of age in 2021.

> We've seen how government measures can have a knock-on effect for logistics and supply chain operations, when restricting the free movement of goods during the pandemic caused significantly longer border crossing times in many countries. With Brexit on the horizon and delays already mounting up at UK borders, this challenge will likely intensify for European businesses in 2021

Sheng Liang
President of Engineering & Innovation at SUSE
www.suse.com

The journey of open source in 2021

MANY BUSINESSES TODAY are grappling with the impacts of COVID-19, forcing them to evaluate their infrastructure and raising the question of digital transformation. Enterprises of all sizes may be dealing with a newly-remote workforce and shifts to traditional workflows, all while navigating a rapidly changing technology landscape.

As IT strategy becomes even more significant to overall business success, attention is now being paid to the technology and applications that will enable companies to modernise, while boosting efficiency and productivity. The drivers of successful transformation will largely depend on the agility and flexibility of an enterprise's IT infrastructure.

Today more than ever, open source is playing a significant role in helping businesses to build flexible IT systems. Meanwhile, open source communities are learning from the past to drive their own growth. As IT leaders consider strategies for 2021, let's take a look at the key learnings from 2020, and how these trends will shape the way businesses operate next year.

Developers innovate anywhere and everywhere

While cloud solutions enabled businesses to survive in 2020, business that continue to embrace agile transformation will win in 2021. With a rise in remote working due to the ongoing COVID-19 pandemic, hybrid cloud will be a huge focus for the enterprise, allowing workloads to move between private and public clouds, as computing needs change and require increased IT flexibility.

One of the key benefits of working in open source is that it is borderless, allowing innovation and collaboration to happen regardless of where the developer sits. From the perspective of developers, containers will be the primary building blocks, connected via service meshes, and extended everywhere through Kubernetes orchestration and operations. Kubernetes delivers truly portable and consistent infrastructure for developers.

This infrastructure gives developers more flexibility when deciding where and when an application may be deployed. New innovations and quick turnarounds will be delivered globally to any infrastructure: public cloud, on-premise cloud, or edge-native cloud.

Working alongside open source developers, it's important to remember what the "open" in open source means. Freedom of choice allows customers to deliver innovation everywhere, at the pace that complements their workflows.

Business resiliency & agility dominating boardroom discussions

IT leaders can continue to expect a level of uncertainty for the year ahead. The ability to pivot quickly will be crucial for businesses as they adapt to continuing change and economic fluctuation. We will see investments continuing to be made in IT, particularly in areas that saw growth during the COVID-19 response. This requires the ability to innovate from anywhere and deploy everywhere, often without a specific local presence. As leadership teams evaluate new technology, finding the right fit can be challenging. For many "traditionalist" enterprises, a hybrid approach will be key to digital transformation - adopting new cloud-based solutions that integrate with legacy systems and allow them to modernise at a comfortable pace. This choice is made possible by open source, and freedom to build unique systems free of vendor lock-in.

Cloud-native application models utilising containers and Kubernetes, as well as infrastructure modernised to distributed-cloud scenarios, are the necessary enabling pillars. Industry suppliers will greatly simplify adoption and increase scalability of these technologies to accelerate and expand usage.
This is an important characteristic to have no matter how robust your business strategy. For businesses looking to accelerate their application delivery with containerised and cloud native workloads, Kubernetes plays an integral role, and with more IT leaders now getting a seat at the boardroom table, we can expect to hear more push for deploying enterprise-wide Kubernetes platforms like SUSE Rancher.

The future of open source

Open source will continue to thrive in 2021, and we will see this community of innovators grow as businesses embrace the freedom to modernise without the confines of a single vendor or solution.

A growing number of companies and people will join one or more open source projects in 2021, and not only from IT and tech companies, but from other industries as well. Innovation will continue to come from open source and expand, improve and morph from there too. While businesses might be looking to shift budgets based on shorter-term objectives thanks to COVID-19 uncertainties, in the past few months we have clearly noticed an accelerated investment focus on innovative areas, from cloud and cloud-native, to AI/ML and Edge, and we anticipate this to continue for 2021.

Devin de Vries
CEO at WhereIsMyTransport
www.whereismytransport.com

How infostructure will transform public transport in 2021

ACCESSING RELIABLE public transport information is difficult for citizens of emerging-market cities. 92% of the world's largest lower-middle income cities lack full network maps, let alone data on frequencies or fare levels. The defined routes and timetables of formal modes - like centrally managed bus networks - often don't match up to the lived experience of commuters. And there is rarely any digitalised information on the routes of informal modes - the smaller, independently run vehicles typical of emerging-market cities - nor fare information or departure frequency.

At WhereIsMyTransport - the mobility technology company I lead - we're working, at scale, in emerging-market megacities to change that. Our technology and data-collection methods have matured during the COVID-19 pandemic, proving that we can now collect accurate data on the complete public transport networks of emerging-market cities in an efficient and scalable way. More importantly than ever, we can maintain that data as networks respond to change.

Big business in emerging-market cities

This new glimpse will help open one of the world's great remaining business opportunities. The combination of huge size and complex challenges in emerging markets means there is scope for business growth at scales no longer found in developed markets.

Emerging-market cities are home to 3.2 billion people, of whom nearly 2 billion rely on public transport at some point each month. The largest 30 cities alone have over 300 million daily commuters. These commuters have proven hard to reach. Most mapping tools aggregate data from public sources, but for informal public transport networks, there is no data to aggregate, and for formal networks, the ground truth can differ greatly to available information. Building out data in a way that's truly valuable means collecting it yourself.

Scaling data collection for emerging-market megacities is tricky The difficulties in collecting this data mean it hasn't been done before at scale, despite the opportunity. Successful initiatives have mapped networks for several large cities, including MIT's Digital Matatus project - a beautiful visualisation of informal transport in Nairobi.

But myriad barriers have meant data-collection efforts still miss nearly all emerging markets. Internet can be spotty, making mobile connections and data uploads unreliable.

Informal transport also takes on different forms in different cities. Operators in Mexico City run three types of vans, with varying capacities. In Dhaka, Bangladesh, there are at least five types of vehicles: beyond size differences, some offer air-conditioning and seating, while others are open air. Accounting for diversity of offerings in data collection requires a bespoke approach.

New technology to find new customers

Recent technology advances mean we're finally cracking the code of digitalising public transport networks in emerging

markets, and doing so at scale. At WhereIsMyTransport, we recently announced our intention to collect comprehensive data from the public transport networks of the 30 largest emerging-market cities.

Our data collection app underpins these processes, working offline and using GPS coordinates to establish route locations. Information is uploaded when mapping is complete, providing security in a context of unreliable connectivity. Our data production software snaps routes to the road network and identifies clusters of informal transport stops as hubs.

Dynamic fields in our app mean that data gathering processes can be easily tailored to the unique circumstances of each city. In Dhaka, these dynamic fields allow data collectors to record which routes have buses with air conditioning. In Mexico City, fields are tailored differently, including reflecting the city's three vehicle sizes.

WhereIsMyTransport translates data for both formal and informal networks into General Transit Feed Specification (GTFS) files - the gold standard for mobility data used by service providers all over the world. To ensure we're getting the right information to people, we built our own GTFS extensions tailored for emerging markets. These fields allow us to accurately represent complex fare systems not seen in developed markets.

While collecting comprehensive data can be challenging, keeping it up to date is even harder. Informal transport networks change rapidly, responding to demand shifts. WhereIsMyTransport keeps on-the-ground data-collection teams in every city where we work, maintaining data accuracy and reliability. Recent work in Gauteng - South Africa's largest and most densely-populated province - found that 30% of informal transport routes in some regions of the city had changed during the COVID-19 pandemic.

The next frontier on urban information

From new vaccine technologies to seamless video conferencing technology, startups and NGOs have responded to the COVID-19 pandemic by pushing innovation forward. Looking ahead for cities in 2021, data-collection innovation will reveal new worlds for the first time, opening up huge markets for businesses and expanding opportunities for citizens.

Joseph Hammer
EVP, Business Development AlefEdge
www.alefedge.com

What's going on at the mobile edge?

A NEW YEAR may be dawning, but for most businesses the legacy of a difficult 2020 lives on. Last year saw organisations in just about every corner of the globe forced to implement remote work policies on a huge scale as the pandemic swept through economy after economy. As we head into 2021, it looks like a lot of these workers will be staying remote. COVID vaccines and falling infection rates will not serve to restore people's faith in sharing communal office space just like that. Besides, many of us have got used to home working and are revelling in its advantages. Many of our bosses feel the same.

All this remote working has already served to massively boost the importance of mobile networking and the transfer of computing tasks to the network edge. As 2021 progresses it seems likely that enterprises will continue to show a strong appetite for new and better ways to securely enable access to critical workloads, keeping workers wherever they might be as productive and connected as possible. Network managers will already have figured out that you can't just tweak the old office-based way of doing things and hope it will serve this purpose. Instead they will be looking for dynamic edge-centric solutions, formulated from the ground up to support the 'new normal'.

It will also come as no kind of surprise to CIOs or CISOs that all this activity at the edge comes at the cost of added vulnerability to the multiple security threats that spring out of shifting essential services and data away from the centre. What is called for is a new kind of secure networking and performance-optimized routing at the application edge.

One approach whose time may have arrived is the software-defined mobile edge, or SD-ME. This is an idea that springs out of advances in edge computing, and is closely tied into the ongoing rollout of 5G. It means opportunities for enterprises, and for the developer community that serves them, to take advantage of the kind of software-defined, zero trust, low latency connectivity that can be the basis of tomorrow's innovative edge applications. The right kind of SD-ME platform brings together a rich set of application enablers that will developers to create secure applications for the new mobile edge. An example of such a platform is AlefEdge's Software-Defined Mobile Edge (SD-ME) which has been integrated with NetFoundry's architecture to offer enterprises an way to develop secure 5G-like applications. This sort of development is desirable for a number of reasons, not least the fact that mobile applications are getting faster, and their latency requirements more stringent. It's not just people that 5G is liberating. We're living at the start of the age of IoT and IIoT. Then there is the rise of the software-defined network, another game changer that is making new things possible in enterprise connectivity.

SD-ME is as much about security as it is control. Moving essential workloads to the edge means new ways of securing that locally held data. This will need to be done at scale too. A business that once had a handful of branch offices to arrange connectivity for now in effect has thousands of 'branches' in the form of a widely distributed workforces. A good SD-ME platform solves this by providing secure local mobile breakout and doing that in an open and programmable way.

It will also run on zero trust principles. With zero trust, you are able to control any endpoint regardless of location, all in a highly secure fashion. By trusting no person and no device that isn't authorised, loopholes are eradicated. Plug in a new CCTV camera or tablet that's not authenticated, and it won't work. An SD-ME platform will play a part in keeping data safe and local, by tracking it according to need. This is useful for both private and public sector use cases, especially where regulation mandates how data must be handled. Things are not going to return to where they were pre-pandemic. They may, let's face it, never truly be the same again. But it looks like the software-defined mobile edge can be a part of adjusting to this new reality.

Larry Williams
Distinguished Engineer, Ansys
www.ansys.com

2021 will be the year of 5G

5G in 2021 will be all about deployment – the infrastructure and handsets are available and is being rolled out as we speak. This will lead to some very exciting possibilities in 2021 and beyond, because the technology has remarkable potential.

5G essentially has three major differentiators to 4G: it's much faster, it can connect more users simultaneously, and it's low latency. This is analogous to cars – there was a time when you bought a car to get from A to B. Today, cars can still get from A to B, but they also come with entertainment systems, smart navigation systems, automatic braking, cruise control, a choice of electric or petrol fuel, and soon, the ability to drive themselves. Until we're further down the 5G road, we won't know how to best make use of it. Again, it's similar to phones and GPS; there was a time when we had data on our phones and GPS, but no-one thought about services like Uber until we were further down the road towards 3G. However, alongside the pandemic, it's likely that we'll see great leaps in both telemedicine and how our education system runs. Doctors will be able to perform surgery from miles away, or even in different countries, as long as the right remote access equipment is in place. Similarly, remote studying will really bed in – why study at a national university, remotely, when you could be studying with the best professor in the world, in another country? When you remove location from the equation, the possibilities are almost endless.

The other exciting potential for 5G is the CBRS band, which allows organisations to deliver a 5G signal privately, independent of operators / carriers, across a large area. This would allow a council to deliver a mobile signal to a remote village, for example, or a large hospitality provider to deploy 5G services across its site, replacing two-way radios with rich multimedia services. The infrastructure for these kinds of services is already available, and we expect to see the first sites rolling out in 2021. However, in the next twelve months, we'll see telecommunications providers working to deploy 5G technologies and lay the infrastructure that will support the applications. Carriers have taken a very diverse range of approaches to this deployment. For example, some have used long range, low frequency bands that don't add that much bandwidth to mobile user download speeds, compared to the low-range, high frequency, high speed bands that are also part of 5G. This means that in effect, a consumer could purchase an expensive 5G phone and not necessarily experience a superior connectivity speed to the one they enjoyed with 4G / LTE.

On the other hand, there will also be some areas that will be able to access the breathtakingly fast speeds that 5G is capable of. 5G deployment is also very complex. Some carriers are completely ripping out and replacing their 4G infrastructure with 5G infrastructure that is backwards compatible – but this is a very expensive approach. Other carriers are installing 5G equipment on 4G masts and either working to avoid interference, or actively looking at dynamic spectrum sharing – and yet more are creating two separate systems for 4G and 5G, which means buying two sets of equipment. In short, there's no right or wrong way of doing it. 5G is a difficult technology to deploy – the full promise of 5G must include the millimeter-wave bands that require near line-of-sight and a lot of masts and infrastructure for complete coverage.

The full gamut of technologies that carriers need to manage to deliver 5G effectively is incredibly complex, making it vital that they make the most of the tools and systems that are available to help make sense of it all, and in time, master them. Overall, we'll see some disillusionment in the short- to mid-term as consumers pay for 5G handsets and don't receive the experience they were expecting – particularly outside of dense urban areas – but in the mid- to long-term, we'll see 5G getting closer and closer to the fast, low-latency, multi-user experience that it promises – and then we're in really exciting territory.

Ritam Gandhi
Founder and Director, Studio Graphene
www.studiographene.com

What will the corporate innovation landscape look like in 2021?

COVID-19 has changed lives and businesses; seemingly forever. Trends that had just taken shape or gathered momentum were suddenly super-charged, with the pandemic accelerating their progression at a rate that would have previously taken years. For companies specifically, this has taken the form of rapid, increased technological adoption. Whether approached with reluctance or excitement, digital transformations were needed to remain afloat during the ‘new normal’. As social distancing restrictions and lockdowns took hold, firms had to adopt creative solutions to continue accessing their base of customers, consumers and clients.

Having supported founders and corporate innovation teams as they pursue digital transformation projects, here are some key trends that I believe are set to become a mainstay of corporate culture as we enter into the 2020’s in earnest.

The rise of low-code

Low-code programs allow individuals with little-to-no technical knowledge to design and develop apps, websites, and products of various kinds. Technology company founders no longer have to fret about becoming coding masters to create their vision of a product. Instead, the low-code movement has provided the tools needed to easily develop such creations themselves, without the need to seek help from professional developers. With more people founding their own company than ever before, such low-code toolkits are in increasing demand. Indeed, recent figures from Companies House suggest that the pandemic has inspired a wave of entrepreneurship: 397,135 company incorporations were recorded between April and September this year alone.

As COVID-19 has forced us to rely on video communication platforms and online delivery applications for connection and sustenance, demand for tech has never been higher. And when trying to meet this demand, founders cannot pass up what’s on offer from low-code and no-code platforms. By utilising such programmes in the development of business-critical software, more time can be spent modifying the core product offering for the betterment of the user experience.

These tools may not only help founders develop their vision but may actually inspire a new swathe of entrepreneurs. A Studio Graphene study from earlier this year revealed that 35% of UK adults who want to make a tech product have been put off by their own lack of technical skills and knowledge. A ubiquitous low-code platform, though, would drastically lower this barrier to entry – hopefully providing enough incentive for such would-be founders to begin their own endeavours.

An eye on AI

The incredible potential of artificial intelligence (AI) to radically alter how we approach technology is increasingly evident. To the benefit of corporate executives and small business founders alike, AI developers have increasingly been creating and selling ‘off-the-shelf’ AI products that can provide specific solutions for all manner of corporate problems.
By incorporating such ‘off the shelf’ AI into a company’s operations, firms can effectively kick-start their long-term digital transformation. Through AI adoption, organisations can begin automating certain online processes, identifying operational inefficiencies only observable by sophisticated algorithms, or determine the most viable route to cost optimisation.

Given all these advantages, it's not hard to find evidence of companies becoming increasingly interested in AI. A recent Gartner survey actually found that 79% of organisations were already exploring or piloting AI-based projects. Of all of AI's possible applications, however, I am personally most interested in the potential of customer experience personalisation. COVID-inspired business transformations have revealed the immense benefits of a good digital experience, with the strength of online offerings set to determine the victors of this new digital age.

2021, therefore, will likely see a rush of businesses implementing AI into their digital offerings to help improve the user experience. As large sections of society remain working from home, or else under some form of lockdown, the burden lies on app and website developers to act as an effective go-between between businesses and their customers. If sufficiently optimised with AI-driven insights, this should hopefully help improve the experience for all involved.

Innovation zeitgeist

A notable development during the COVID-19 pandemic is that no organisation has been safe from its ill-effects. Thus, all businesses have been forced to tear down any risk-averse mindsets, red tape, or internal derision that blocked digital innovation during previous years.

In November 2019, just before the onset of the pandemic, a Studio Graphene study found that a significant 87% of large UK businesses felt there was too much bureaucracy preventing them from putting ideas into action. Meanwhile, some 37% admitted to having tried and failed to implement a new technology in the past year.

In the twelve months since, typical obstacles to digital innovation have been broken down by COVID-19. Companies have been moving with more flexibility, and risk, than ever before. As entire economies have been shaken to their core by the virus, companies have adopted a 'sink or swim' approach - and desperately held on to technological innovation as a means to stay afloat.

But even after the pandemic, I don't believe this shift in perspective will change. As business leaders recognise the advantages constant innovation has over adherence to the status quo, more and more innovation will be pursued in a bid to improve a company's offerings – and gain an edge on the competition. Ultimately, I'm looking forward to witnessing how this shall play out, and what ambitious technological developments we can look forward to in 2021.

Ritam Gandhi, is the Founder and Director of Studio Graphene – a London-based company that specialises in the development of blank canvas tech products including apps, websites, AR, IoT and more. The company has completed over 100 projects since first being started in 2014, working with both new entrepreneurs and product development teams

> Given all these advantages, it's not hard to find evidence of companies becoming increasingly interested in AI. A recent Gartner survey actually found that 79% of organisations were already exploring or piloting AI-based projects