




DIGITALISATION WORLD

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

ISSUE VII 2021

digitalisationworld.com



How blockchain and AI are helping the current COVID-19 vaccine rollout



AI Ops | Apps + DevOps | Artificial Intelligence | Big Data + Analytics
Cloud + MS | DC Facilities + Colo Digital Business | IT Management + Service
Networks + Telecoms | Open Source | Security + Compliance | Storage + Servers

Jacky
*VP Power Solutions
EMEA / France*

Kathy
*Sr. Operations Manager
China*

Jitendra
*DGM Sales
India*

Meet your
GLOBAL POWER PARTNER

*Generators, power solutions and 24/7 support.
Dedicated to data centers.*



Kohler-sdmo.com/EN/application-data-centers

KOHLER®
IN POWER. SINCE 1920.

Editor's View

By Phil Alsop



Cybersecurity – time for a new approach?

IN ASSEMBLING the articles for this issue of Digitalisation World I was struck by the sheer variety of topics being covered under the umbrella heading of cybersecurity. In no particular order, these include: infrastructure-as-a-code security, cloud native security, data protection (security + storage!), DDoS, zero trust, XDR and DevSecOps. Hopefully, this list is representative of some of the main security challenges facing end users right now, but it wouldn't claim to be an exhaustive one (a security feature without mention of ransomware, a publishing first?!).

No, the technologies and issues surrounding cybersecurity are on a scale like no other in the IT space right now. And for good reason. Security and the trust it gives to employees and customers alike is essential in our digital age, where the minute you connect your computer to the outside world, you seem to be entering the Cyber Wild West. So, security deserves to be a, if not the, major IT topic. But I'm beginning to wonder if the size and scale of the problem means that it just might be time for a set of industry standards to be introduced, whereby the many, many security topics are defined, classified and presented as

a coherent whole, as opposed to today's somewhat messy landscape, where there are so many cybersecurity phrases, acronyms and expressions thrown around which, I'm thinking, leave many end users plain confused.

In other words, someone, or, more likely, some body, needs to produce a Security Lifecycle Model (SLM), which is a true representation of the much touted end-to-end security approach and which, importantly, seeks to explain where each technology and approach sits in relation to all of the others, including the many crossover areas. Maybe the thought of carrying out such a complex project is the reason that it hasn't been attempted to date. Then again, maybe I've been looking in the wrong place and a kind reader will point me in the direction of such an SLM!

In conclusion, I would suggest that, until end users have an independently produced and respected SLM, they will struggle to understand just exactly what solutions they do and don't need to implement when it comes to cybersecurity. Worse still, they will be vulnerable to all those security vendors 'bearing gifts'...



Ccontents

ISSUE VII 2021

52 COVER STORY

How blockchain and AI are helping the current COVID-19 vaccine rollout

As promising as the current COVID-19 vaccines are in the fight against the pandemic, the biggest challenge is still how to distribute these vaccines all across the globe



WORLD NEWS

- 06 90% enterprises yet to achieve digital-first goals
- 07 Hybrid challenges
- 07 FLAP markets surpass 2,000MW
- 08 Digital darkness across Europe
- 09 Security and silos hold back automation initiatives
- 10 Covid - the ultimate digital test?
- 11 Average phishing costs soar to \$14.8m

THE ANALYST

- 12 AI spend to reach almost \$342 billion this year
- 14 Over a third of organisations worldwide experience ransomware attack or breach
- 16 Strong growth for the managed edge services market

CYBERSECURITY

- 20 Delivering an effective cybersecurity strategy
- 22 Common misconceptions around cloud-native security
- 24 A question of priorities

- 26 Navigating shark-infested waters
- 28 From cloud to the edge: How Zero trust security makes the everywhere workplace possible
- 30 Why openness means better cyber security
- 32 How to develop and maintain an effective DevSecOps culture
- 36 A three-pronged approach to government security
- 38 How is QKD combatting the increased sophistication of today's cyber-attacks?
- 40 How mass remote work has changed DDoS



AUTOMATION

- 42 Machine Learning success starts with 10 steps
- 44 Five practical ways contact centres can use AI to create value

BLOCKCHAIN

- 48 Blockchain vs Bitcoin: Everything you need to know
- 54 Don't wait for blockchain, it's more accessible than you think
- 56 How to navigate intellectual property risk in blockchain projects

TRAVEL

- 58 Business as usual? Why the aviation industry cannot revert to its pre-pandemic ways
- 60 How data is changing the way hotels streamline operations

DATA ANALYTICS

- 62 Delivering deep-link analysis

HYPERAUTOMATION

- 64 AI and Automation – Is your business ready for hyperautomation?
- 66 Hyperautomation, enabling the next digital age
- 68 How is the cloud encouraging hyperautomation, and why should I care?

SAAS

- 70 Providing reliable, long term SaaS services: The importance of scalability



The data centre trade association

DCA News

72 DCA Data Centre – Data Centre Design Concepts

By Steve Hone, CEO

72 Is the Industry on the Edge of a Great Opportunity

By Stephen Whatling, Chairman at Business Critical Solutions, BCS

74 Design and Build

By Lawrence Hooker, Operations Manager, Sector Lead for Mission Critical at Michael J Lonsdale

76 Getting that little bit more

By Zac Potts, Associate Director (Data Centre Design), Sudlows

77 Top Design Considerations for the most efficient data centre lighting solution

by Zumtobel



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

Account Manager

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

Director of Logistics

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

Design & Production Manager

Mitch Gaynor +44 (0)1923 690214 mitch.gaynor@angelbc.com

Publisher

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

Circulation & Subscriptions

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

Directors

Stephen Whitehurst: Chairman
Scott Adams: Chief Technical Officer
Sukhi Bhadal: Chief Executive Officer

Published by:

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



Digitalisation World is published 10 times a year on a controlled circulation basis in Europe, Middle East and Africa only. Subscription rates on request. All information herein is believed to be correct at time of going to press. The publisher does not accept responsibility for any errors and omissions. The views expressed in this publication are not necessarily those of the publisher. Every effort has been made to obtain copyright permission for the material contained in this publication. Angel Business Communications Ltd will be happy to acknowledge any copyright oversights in a subsequent issue of the publication. Angel Business Communications Ltd. © Copyright 2021. All rights reserved. Contents may not be reproduced in whole or part without the written consent of the publishers. The paper used within this magazine is produced by chain of custody certified manufacturers, guaranteeing sustainable sourcing. ISSN 2396-9016 (Online)

90% of enterprises yet to achieve digital-first goals

45% ENTERPRISES attribute productivity loss during the crisis to connectivity. Tata Communications unveils “Leading in a Digital-First World; Enabling Success with the Right Mindset, Ecosystem and Trust” Report which finds 90% of enterprises are yet to achieve their digital-first goals with 49% admitting that cyber security is the top most priority for their business. It also brings to light, 45% of enterprises lost productivity during the crisis due to problems of connectivity and 41% enterprises attribute the shift to digital-first operating models for maintaining market share during the course of the pandemic. The survey was conducted among business leaders across 750 enterprises in 11 countries and classifies them into three distinct categories as per their digital maturity stage.

● Digital Trailblazers:

Only 10% enterprises have the most advanced digital operating models, connectivity platforms and strategies ensuring secure and trusted operations. 63% of them attribute revenue growth to their digital-first strategy.

● Digital Migrants:

52% of enterprises have limited digitalisation in their business, but still need to improve in several areas of digital capability.

● Digital Aspirants:

38% of enterprises are at a nascent stage of digitalising their business and have been unable to achieve growth due to lack of digital maturity.

“A digital-first operating model is a must for enterprises in the new world order. As economies open, trust and security are core to the competitiveness and agility of enterprises seeking growth. The scale of digitalisation will be the new barometer of success for enterprises irrespective of its size or industry,” said A.S Lakshminarayanan, Managing Director and CEO, Tata Communications. The ‘Leading in a Digital-First World’ Report very clearly identifies gaps and addressal for enterprises in their digital transformation journeys to be in three areas:

● Commit to a digital-first operating model:

44% were not successful in delivering a digital-first operating model for

their ecosystem. To address this, real benefits of digital transformation requires organisations to go far beyond shifting some business processes online. They need a coherent digital operating model that over time reimagines every core channel, process and service offering to maximise the digital opportunity.

● Create quality user experiences with a hyperconnected ecosystem:

91% enterprises admit that they are not able to provide high-quality digital experiences for their customers, employees and business partners. They concur to having only a patchwork of different digital strategies and processes across their organisations. To move up the value chain, a digital-first strategy focusing on agility, control and security is critical. Enterprises must move away from legacy processes and embrace ‘being hyperconnected’ and delivering high-quality, secure and frictionless collaboration for all stakeholders across the entire ecosystem.

● Central to a digital-first business is security and trust:

49% enterprises affirm cyber security to be the most important aspect of their digital strategy to continually improve and 34% enterprises rate themselves poorly at delivering an agile operating model.

This is a stumbling block on their ability to innovate and adapt faster than their competition. As cyber threats and regulatory demands gain centre stage in the new world enterprises must continue to win trust, businesses must stay vigilant and invest proactively to safeguard all stakeholders. As the ‘Leading in a Digital-First World’ Report states, the current shift to digital-first operating models is a defining moment in the evolution of businesses and rethinking the new world.

A digital-first strategy enables secure, connected and digital experiences. The sooner organisations start to accelerate their digital transformation journeys up the digital maturity curve, the more likely they are to empower themselves for the new digital era.



Hybrid challenges

84% of IT teams expect increased budget to facilitate new ways of working, yet only 34% are prioritising hybrid work support. As organisations continue to adapt to and embrace new ways of working, IT teams are facing unexpected challenges.

According to a new survey from Snow Software, 92% of IT leaders report their organisations were moving or had already moved to a hybrid work model. Yet only 34% said enabling the shift to hybrid work was their department's primary focus over the next 12 months. The data suggests IT leaders may be underestimating the unique challenges of hybrid work, especially as their teams are already facing issues such as rising costs and insufficient security. The study surveyed more than 400 IT leaders from organisations with over 500 employees to determine the current state of hybrid work and hybrid technologies.

"Despite the significant transition that organisations have faced over the past year, it seems that the future of hybrid work is putting IT leaders in a position where they will once again be required to quickly shift gears and adapt to a new reality," said Alastair Pooley, Chief Information Officer at Snow.

"While IT teams are planning and budgeting to enable their businesses, many don't have the full picture of what their organisations will need when it comes to supporting a truly hybrid workforce. What we've learned over the past 18 months is that understanding how current technology investments are being utilised and what areas need more support is critical for teams to manage the pivot to a hybrid work environment when they are ready and able."

Key findings include:

- Majority of IT leaders are embracing hybrid work but already facing a new array of challenges. When asked about their feelings towards the larger trend of organisations moving to

remote work, 57% of IT leaders said they were excited and 44% indicated they believe it was a move in the right direction. However, the shift has not been easy, even in the early stages.

IT leaders report controlling and optimising IT costs (18%), reining in shadow IT (16%) and managing cybersecurity threats (13%) as the most challenging aspects of supporting or transitioning to hybrid work. CIOs and C-level executives in particular are concerned about shadow IT, with 26% noting it as the biggest challenge posed by hybrid work.

- IT priorities are now focused on growth initiatives. After a year spent enabling change for their workforce, just 34% of IT leaders said supporting hybrid work would be their top priority over the next 12 months. Instead, respondents are turning their focus to larger corporate initiatives. IT leaders report that their top priorities will be enabling competitive differentiation (57%), reducing or optimising IT costs (55%) and managing digital transformation initiatives (54%). Additionally, 48% of respondents said accelerating cloud adoption and migration was a priority, suggesting this will continue to be an important area of focus despite the rapid shifts that occurred in 2020.
- Following increased IT investments in 2020, IT leaders will spend even more in 2021. One area where hybrid work is having a big impact is IT budgets. When asked if they expect additional funding to support new ways of working, 84% of IT leaders said yes. Another 13% said they expected budget to stay flat while just 2% face budget cuts and 1% are unsure. When asked what they would spend additional budget on, 37% said additional IT staff, followed by 18% investing in SaaS applications and 17% investing in cloud infrastructure.



- Hybrid employees expected to become a bigger burden on IT. IT leaders do expect hybrid work models will change employees' technology needs, with 34% saying it will increase their use of IT resources. Despite spending less time in the office, only 10% think hybrid work will decrease employee use of IT resources. Another 18% believe it will increase department-led technology purchases, which can contribute to shadow IT if the right policies, processes and staff are not in place.
- SaaS applications take centre stage and require greater visibility and management. Unsurprisingly 70% of leaders reported that their investment in SaaS has increased over the past 12 months. Just 2% reported that it decreased and 28% said it stayed the same. IT continues to face issues with visibility and overall management of SaaS applications, which could make the transition and enablement of hybrid work more difficult. Nearly half said that controlling SaaS sprawl was their biggest challenge, while 26% said it was discovering unmanaged applications. When asked about the most impactful SaaS applications at their organisation over the past year, 32% of IT leaders said Microsoft 365 followed by Google Workspace (20%), Zoom (19%) and Salesforce (11%).



Digital darkness across Europe

RESEARCH from Digitopia finds that only 6% of businesses have visibility of their own digital transformation progress.

Digitopia has found that 90% of businesses do not measure digital transformation strategy and are unaware of the progress that they have made throughout their journey. The same survey, which assessed businesses across the UK and Europe, also found that 65% of respondents blame this lack of awareness on being too busy with digital transformation itself to monitor its progress.

The COVID-19 pandemic made one thing very clear - businesses need to continually adapt or risk being left behind. As a result, organisations all over the world embarked on a digital transformation journey that would not only benefit businesses in short term lockdowns, but also create long term sustainability. At first, it was simple: better facilitate remote and hybrid working, leveraging the cloud to create a completely flexible working environment. However, with recovery from the

pandemic well underway, the next steps in a company's digital transformation strategy can quickly become unclear.

According to Digitopia's latest research, this is already the case for the vast majority. The study, which analysed the responses from 700 executives - ranging across C-Suite, VP and Director roles - in 400 different companies, found that only 4% of organisations are aware of their digital transformation progression and accurately measure it.

Lack of visibility over digital transformation progression isn't exclusive to one industry, either. The research assessed the position of businesses across several sectors, specifically: retail, consumer goods, automotive and manufacturing, insurance, banking and finance.

Of these organisations that do not track their digital transformation progress, 'busy with digital transformation' was cited as the most common reason for

failing to measure digital maturity, with 'no shared vision' being the second most popular response at 47%.

The rest are as followed:

- Lack of skills and competencies (39%)
- No sense of urgency (33%)
- Misalignment in leadership (27%)
- Disagreement on importance (13%)

"These findings have surprised us following a year where so many organisations have turned to digital transformation to continue operating," said Halil Aksu, CEO and co-founder of Digitopia. "You manage what you measure, and it's concerning that so few businesses are paying attention to such an important aspect of modern business. Digital transformation is more than just technology, and only by measuring, benchmarking and assessing every aspect of the journey can an organisation know where it is succeeding, and where it needs improvement. Only then can these businesses see a maximum return on investment and deliver sustainable, long term business success."

FLAP markets surpass 2,000MW

THE MARKET SAW 51MW come online in Q2. CBRE expects to see 442MW of new supply come online this year, with 130MW expected to come online during Q3, just short of the 133MW that came online during Q1.

The FLAP (Frankfurt, London, Amsterdam and Paris) data centre markets – the four largest in Europe - have collectively surpassed 2,000MW of supply for the first time.

This follows a quiet Q2, where only 51MW of new supply came online, but a much larger Q1, when 135MW of supply came online. There is still 256MW of supply scheduled to come online during H2, which will lead to a record year for new supply with 442MW coming online. This is more than double the 202MW seen in the last record year of 2017. In terms of take-up, the quarter saw just more than half the take-up of Q1, when 92MW came online (a record quarter for take-up).

CBRE expects the second half of the year will see more than 229MW of customer supply come online, leading to a record year for take-up (the last record for take-up was set in 2020 at 201MW). According to the report, most new supply is being driven by hyperscale cloud deals. A number of providers, in particular those in the retail colocation space, have said they are also seeing increasing interest from enterprise and other customer groups not associated with cloud.

Many enterprises are turning to colocation as they move data centres out of traditional office environments or turn to colocation to gain access to cloud services and connectivity options.

In some markets, opportunities for such customers are becoming increasingly difficult to find with locations such as Frankfurt and Paris experiencing supply constraints. It is unsurprising that these markets will see local records broken for new supply during 2021 (Frankfurt with 167MW and Paris with 87MW). Take-up in these markets will also be at record levels – with Frankfurt expected to see 125MW for the year and Paris 85MW.

CBRE EMEA Data Centre Research Director, Penny-Madsen Jones commented:

"We are hearing more about new sites coming on specifically to meet enterprise requirements at the same time as a large number of hyperscale-focused sites are being launched. The industry realises the importance of having a healthy ecosystem of cloud providers and cloud end users in a market to maintain the importance of the data centre hub. The balance of supply and demand, as a result, is going to remain incredibly important for these markets moving forward. While we have seen some customers explore new market options outside of FLAP as a result of these challenges, many still have requirement to be inside markets they may be serving."

Security and silos hold back automation initiatives

IT AND BUSINESS collaboration proves key to overcoming security and integration challenges; Almost 9 out of 10 organizations agree that IT and business alignment has improved in the last 12 months driving faster innovation, together.

MuleSoft reports that 70% of automation initiatives are being hindered by security concerns and data silos, as organizations increasingly look to automation to improve efficiency and productivity. However, MuleSoft's IT and Business Alignment Barometer also revealed opportunities for companies to overcome these challenges and enable faster innovation across their organizations. IT and business teams working closely together can shrink or even eliminate organization silos, significantly reducing time to market. The report shows that almost 9 in 10 (87%) say IT and business alignment has improved over the last 12 months leading to a number of benefits, including improved collaboration (64%), operational efficiency (58%), and better customer experience (54%).

Based on a global study of 2,400 IT decision makers (ITDMs) and business decision makers (BDMs), the MuleSoft IT and Business Alignment Barometer also highlights organizations' business priorities and challenges over the next 12 months:

Digital imperatives increase automation adoption

In an all-digital, work-from-anywhere

world, it's never been more important to sense and respond to changing market dynamics – and the needs of customers and employees – with speed, agility, and efficiency. Automation has become a rising focus for many organizations to drive convenience, speed, and cost reductions. Organizations report that:

Operational efficiency is top of mind for businesses: Improving operational efficiency (54%), creating better connected customer experiences (50%), improving productivity (49%), becoming more agile for change (48%), and becoming more data-driven (45%) are organizations' top five business priorities.

There's automation everywhere: 95% of organizations have implemented or are in the process of implementing automation initiatives, such as streamlined employee onboarding processes, to improve productivity. 93% see automation as a means to create better connected customer experiences and to improve operational efficiency.

Security concerns slowing down the pace of innovation: The majority (87%) of IT and business leaders say that security and governance concerns are slowing down the pace of innovation. Disparate systems cause security headaches: Almost three quarters (73%) of organizations say the integration of disparate systems has increased their concerns around data security and governance – 31% say it had 'significantly' increased concerns.



Organizations still wary of empowering non-technical users: Most organizations recognize the need to empower business teams to help take the operational strain off IT. However, the majority remain wary about the security implications; 87% admitted security concerns were holding them back at least to some degree from empowering non-technical users to integrate data sources.

Collaborative innovation model for IT and business drives agility

To overcome integration challenges and become more agile, IT and business teams need to work together to co-create value and keep pace with the speed of digitalization. IT teams can focus on producing secure and governed reusable assets, and empower business teams to integrate and self-serve these IT-approved assets to deliver innovation faster.

AI and Natural Language Processing

Faster and more efficient trading

Connecting opportunities

© Copyright 2021 IPC Systems, Inc. All rights reserved. The IPC, IQNAX, Uring, Blue Wave and Compass names and logos are trademarks of IPC Systems, Inc. All other trademarks are property of their respective owner. Specifications and programs are subject to change without notice.

www.ipc.com

Covid - the ultimate digital test?

RACKSPACE TECHNOLOGY has published the results of a global survey revealing that 2020 drove a large-scale push for application modernization. As organizations scrambled to support fully distributed workforces and securely integrate new cloud-native data platforms and collaboration apps into already complex ecosystems, many cranked their existing application modernization efforts into overdrive.

According to the survey, The State of Application Modernization, 71% of respondents say at least one out of four applications are undergoing active modernization, and 24% say more than half of all their applications are underdoing modernization. Most organizations have already paid a price for dragging their feet, over half of respondents say delaying application modernization has resulted in failures to meet compliance requirements (56%) and/or to scale critical services when required (51%).

"The results paint a clear and consistent picture," said Jeff DeVerter, Chief Technology Evangelist at Rackspace Technology. "Organizations of all sizes and across all industries have firmly bought into digital transformation and are actively pursuing strategies of continuous application modernization. In fact, many have already experienced direct consequences from moving too slowly – which may explain why nine out of ten organizations say their appreciation for the business value of applications has increased."

The global survey included 1400+ respondents in IT and non-IT business units, from companies with \$300M annual earnings and above, including both decision makers and application users.

The State of Digital Transformation

Most respondents described their digital transformation journey as actively "in-progress" (65%) and "at a similar place to their peers" (57%). Just over half said they have "a system in place to coordinate cross-functional modernization activities," with "digital initiatives extending beyond a single business unit" (53%). Public sector respondents were more likely to describe their digital transformation as "basic" or lagging. On average, organizations now host 38% of all workloads on public cloud, surpassing private cloud (35%) and on-premises data centers or colocation (27%). This breakdown was remarkably consistent across both business size and industry vertical.

Application Modernization Priorities

Government and manufacturing organizations were more likely to focus on modernizing enterprise software, while retail businesses were more likely to prioritize customer-facing applications and digital content management systems.

When asked what prompts modernizing applications, over half of all organizations (54%) singled out improved customer satisfaction, with nearly as many (47%) also citing increased employee efficiency and satisfaction. Motivations for replacing

legacy applications with new solutions followed a similar pattern, with improved customer experience (CX) leading as a common driver (58%), followed by process optimization (52%) and cost optimization (46%).

The two key themes to application modernization success that surfaced repeatedly were the need to navigate complexity and the need to minimize disruptions and risk.

Consequences of Delaying Modernization

Survey results suggest that the perceived risks of lagging behind competitors are another factor driving organizations to transform their legacy systems. Over half said that delaying application modernizations had resulted, at some point, in failing to meet new regulations (56%) and/or to scale up to meet new demands (51%).

When asked about the top barriers inhibiting technological change at their organizations, respondents pointed to the fear of impacting CX (28%), the entrenchment of legacy IT systems (26%), and the need to work within budget constraints (24%). The most frequently flagged consideration for planning an application modernization project was security (34%). "From an IT perspective, 2020 may be remembered as the year that application modernization morphed from a corporate buzzword into becoming a central element of institutional survival," added DeVerter.

BRIDGEWORKS

THE DATA ACCELERATION COMPANY

DCS AWARDS
Best Data Centre ICT Networking Product of the year

SDC AWARDS
SDC Awards Backup/Archive Innovation of the Year category

UK IT INDUSTRY AWARDS
UK IT Industry Award

SME NEWS
Best in Cloud Acceleration Solutions

SME NEWS
Innovation in Software Defined Protocol Acceleration

CORPTODAY
BUSINESS FINANCE LIFESTYLE
Best for Software Defined Protocol Acceleration

BRIDGEWORKS WINS 6 AWARDS 2020

Average phishing costs soar to \$14.8m

BUSINESS EMAIL COMPROMISE (BEC) and ransomware attacks prove most costly phishing threats to large businesses. Proofpoint and Ponemon Institute have released the results of a new study on the Cost of Phishing. The report reveals that the cost of phishing attacks have almost quadrupled over the past six years, with large U.S. companies losing an average of \$14.8 million annually (or \$1,500 per employee), up sharply from 2015's figure of \$3.8 million.

According to the study, which surveyed nearly 600 IT and IT security practitioners, the most expensive threats to businesses include BEC and ransomware attacks. But the costs to organizations extend far beyond the funds transferred to the attackers.

"When people learn that an organization paid millions to resolve a ransomware issue, they assume that fixing it cost the company just the ransom. What we found is that ransoms alone account for less than 20 percent of the cost of a ransomware attack," said Larry Ponemon, Chairman and Founder of Ponemon Institute. "Because phishing attacks increase the likelihood of a data breach and business disruption, most of the costs incurred by companies come from lost productivity and remediation of the issue rather than the actual ransom paid to the attackers."

Credential compromise (credential theft) generally precedes attacks like BEC and ransomware, usually in the form of an employee being "phished" into giving up their login credentials. According to the Anti-Phishing Working Group (APWG), phishing is a crime employing both social engineering and technical subterfuge to steal personal identity data and financial account credentials. The growth of phishing is not gradual – it's growing exponentially, with the APWG estimating that phishing attacks doubled in 2020 alone.

Other key findings from the 2021 Cost of Phishing report include:

- Loss of Productivity is one of phishing's costliest outcomes. In an average sized U.S. corporation of 9,567 people, this translates to 63,343 wasted hours every year. Each employee wastes an average of seven hours annually due to phishing scams, an increase from four hours in 2015.
- Business Email Compromise costs nearly \$6M annually for a large organization. Of that, illicit payments made annually to BEC attackers is \$1.17M.
- Ransomware annually costs large organizations \$5.66 million. Of that, \$790,000 accounts for the paid ransoms themselves.
- Security Awareness Training reduces phishing expenses by more than 50 percent on average.

- Costs for resolving malware infections have more than doubled since 2015. The average total cost to resolve malware attacks is \$807,506 in 2021, an increase from \$338,098 in 2015.
- Credential compromise costs have increased dramatically since 2015. As a result, organizations are spending more to respond to these attacks. The average cost to contain phishing-based credential compromises increased from \$381,920 in 2015 to \$692,531 in 2021. Organizations experienced an average of 5.3 compromises over a 12-month period.
- Business leaders should pay attention to probable maximum loss scenarios. For instance, BEC attacks could incur losses from business disruptions of up to \$157 million if organizations aren't prepared. Malware resulting in data exfiltration could cost businesses up to \$137 million.

"Because threat actors now target employees instead of networks, credential compromise has exploded in recent years, leaving the door wide-open for much more devastating attacks like BEC and ransomware," said Ryan Kalember, executive vice president of cybersecurity strategy, Proofpoint. "Until organizations deploy a people-centric approach to cybersecurity that includes security awareness training and integrated threat protection to stop and remediate threats, phishing attacks will continue."





AI spend to reach almost \$342 billion this year

Worldwide revenues for the artificial intelligence (AI) market, including software, hardware, and services, is estimated to grow 15.2% year over year in 2021 to \$341.8 billion, according to the latest release of the International Data Corporation (IDC) Worldwide Semiannual Artificial Intelligence Tracker.

THE MARKET is forecast to accelerate further in 2022 with 18.8% growth and remain on track to break the \$500 billion mark by 2024. Among the three technology categories, AI Software occupied 88% of the overall AI market. However, in terms of growth, AI Hardware is estimated to grow the fastest in the next several years. From 2023 onwards, AI Services is forecast to become the fastest growing category.

Within the AI Software category, AI Applications has the lion's share at nearly 50% of revenues. In terms of growth, AI Platforms is the strongest with a five-year compound annual growth rate (CAGR) of 33.2%. The slowest will be AI System Infrastructure Software with a five-year CAGR of 14.4% while accounting for roughly 35% of all AI Software revenues. Within the AI Applications market, AI ERM is expected to grow

slightly stronger than AI CRM over the next five years. Meanwhile, AI Lifecycle Software is forecast to grow the fastest among the markets within AI Platforms.

"Disruption is unsettling, but it can also serve as a catalyst for innovation and transformation. 2020 was the year that accelerated digital transformation and strengthened the value of enterprise AI," said Ritu Jyoti, group vice president for AI and Automation Research at IDC. "We have now entered the domain of AI-augmented work and decision across all the functional areas of a business. Responsible creation and use of AI solutions that can sense, predict, respond, and adapt at speed is an important business imperative." The AI Services market was estimated at \$19.4 billion in 2020, representing the fastest growth relative to hardware and software. For 2021, it is

forecast to grow at 19.3%. Over the next five years, it is expected to enjoy the best CAGR at 21%. This technology category breaks down into two segments: IT Services and Business Services. IT Services is the larger of the two, accounting for nearly 80% of all AI Services revenues. From a growth perspective, the two markets are similar with five-year CAGRs of 21%. Overall, AI Services is expected to be a \$50 billion market by 2025.

“AI has emerged as an essential component of the future enterprise, fueling demand for services partners to help organizations clear the many hurdles standing between pilot projects and enterprise AI,” said Jennifer Hamel, research manager, Analytics and Intelligent Automation Services. “Client demand for expertise in developing production-grade AI solutions and establishing the right organization, platform, governance, business process, and talent strategies to ensure sustainable AI adoption at scale drives expansion across both IT services and business services segments.”

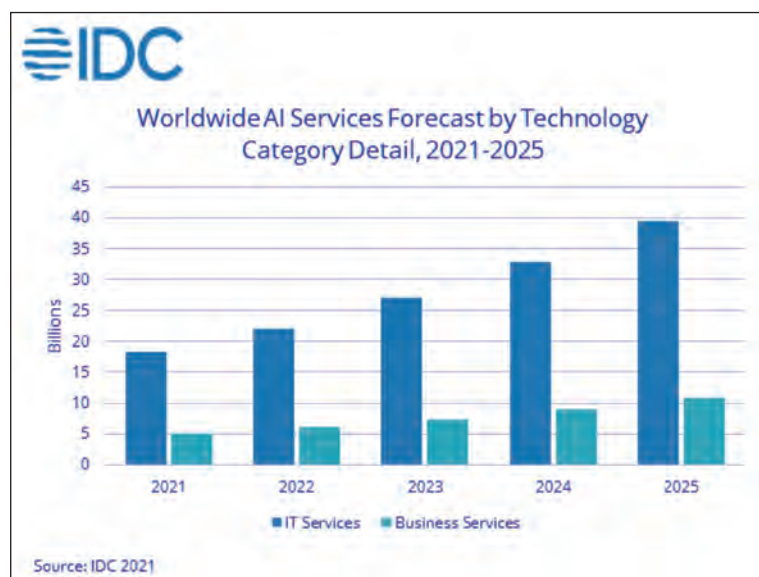
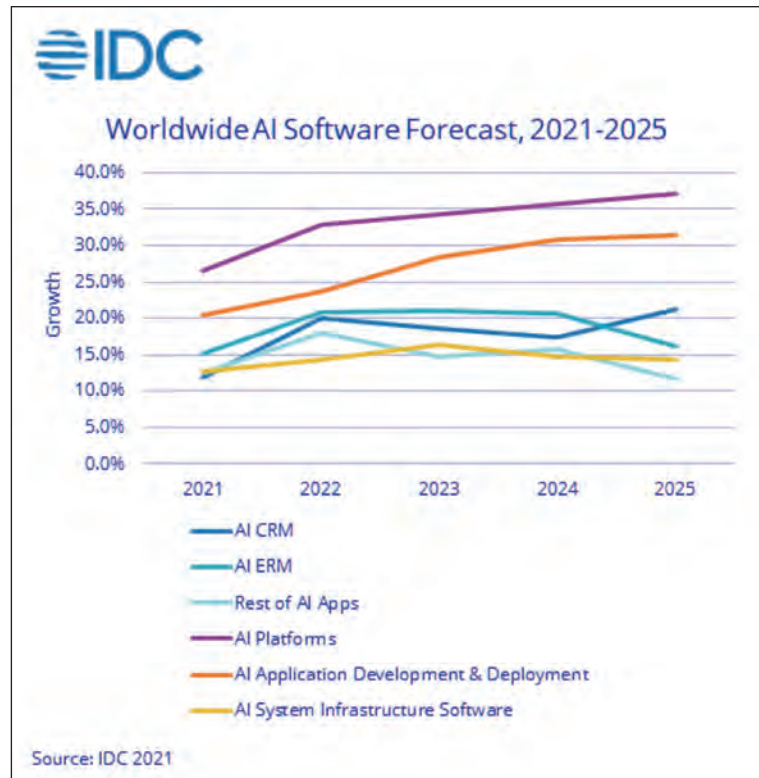
Almost 190 companies were included in the AI Services market in this release of the AI Tracker. Under IT Services for AI, the Top 3 companies in 2020 were IBM, Accenture, and Tata Consultancy Services. Each of the three companies achieved over \$1 billion in revenues and combined for a total of 26% market share. Beyond them, another eight companies generated more than \$500 million each.

The Top 3 companies in Business Services for AI in 2020 were Ernst & Young, Accenture, and Deloitte, accounting for a combined share of 46%. Outside of these top 3, there were another nine companies that broke the \$100 million mark during 2020. Overall, the competitive landscape in both services markets for AI remains highly fragmented where many players from across the services value chain continue to invest in technology assets, innovation resources, and expertise in applying AI to solve industry- and domain-specific problems for clients.

AI Hardware is the smallest category with 5% share of the overall AI market. Nonetheless, it is forecast to grow the fastest in 2021 at 29.6% year over year. It is also expected to hold the best growth spot in 2022.

Over the next five years, its CAGR is estimated at 19.4%. This technology category breaks down into two markets: Server and Storage. Server has the larger share at approximately 82% while Storage is forecast to have better growth with a five-year CAGR of 22.1%.

“The market for AI servers and storage was less impacted than anticipated by the COVID-19 pandemic and is now rapidly picking up steam again, especially at the edge,” said Peter Rutten, research director, Infrastructure Systems, Platforms and Technologies at IDC. “The infrastructure of choice is coalescing around



massively parallel compute using co-processors and server clusters with fast interconnects and networks.” In AI Server market, there were a total of six companies that generated over \$500 million each in 2020; they are (in alphabetical order) Dell, HPE, Huawei, IBM, Inspur, and Lenovo. Together, they held 62% of overall market share.

Meanwhile, in the AI Storage market, there were also six companies that achieved over \$100 million each in 2020; they are (in alphabetical order) Dell, HPE, Hitachi, Huawei, IBM, and NetApp. These six companies had a combined market share of 68%.



Over a third of organisations worldwide experience ransomware attack or breach

A new International Data Corporation (IDC) survey has found that more than one third of organizations worldwide have experienced a ransomware attack or breach that blocked access to systems or data in the previous 12 months. And for those that fell victim to ransomware, it is not uncommon to have experienced multiple ransomware events.

“Ransomware has become the enemy of the day; the threat that was first feared on Pennsylvania Avenue and subsequently detested on Wall Street is now the topic of conversation on Main Street,” said Frank Dickson, program vice president, Cybersecurity Products at IDC. “As the greed of cybermiscreants has been fed, ransomware has evolved in sophistication, moving laterally, elevating privileges, actively evading detection, exfiltrating data, and leveraging multifaceted extortion. Welcome to digital transformation’s dark side!”

Key findings from the survey include the following:

- The incident rate was notably lower for companies

based in the United States (7%) compared to the worldwide rate (37%).

- The Manufacturing and Finance industries reported the highest ransomware incident rates while the Transportation, Communication, and Utilities/Media industries reported the lowest rates.
- Only 13% of organizations reported experiencing a ransomware attack/breach and not paying a ransom.
- While the average ransom payment was almost a quarter million dollars, a few large ransom payments (more than \$1 million) skewed the average.



Source: IDC
Worldwide
Security
Spending Guide
— Forecast
2021, July (v2
2021)

Greater awareness of ransomware incidents has prompted organizations to undertake a variety of actions in response. These include reviewing and certifying security and data protection/recovery practices with partners and suppliers; periodically stress-testing cyber response procedures; and increased sharing of threat intelligence with other organizations and/or government agencies. Greater incident awareness has similarly prompted requests from boards of directors to review security practices and ransomware response procedures.

Analysis of the survey results also showed that organizations that are further along in their digital transformation (DX) efforts were less likely to have experienced a ransomware event. These are organizations that have committed to a long-term DX investment plan with a multi-year approach tied to enterprise strategy.

Europe IT security spending to jump 8.3%

European IT security spending remains robust despite the impacts of the COVID-19 pandemic and is expected grow 8.3% year on year in 2021, according to International Data Corporation (IDC). IDC's new Worldwide Security Spending Guide indicates that European IT security spending will rise to a total value of \$37.2 billion in 2021. It is forecast to have a five-year (2020–2025) compound annual growth rate (CAGR) of 8.2%, surpassing \$50 billion in value in 2025. IT security software will have the strongest year-on-year growth of any category, according to the guide. However, IT security services will remain the biggest spending category.

Spending growth is expected to intensify through 2025. IDC's recent European Industry Acceleration survey found that European organizations continue to regard cybersecurity as their top priority. According to the survey, more Central and Eastern Europe (CEE) respondents rank cybersecurity as the top priority than Western Europe (WE) respondents – 26% versus 22.5%, respectively.

"We can expect increased IT security spending by organizations in Central and Eastern Europe, particularly in the public sector and telecommunications, as they work to close the gap with their peers in Western Europe," says Senior Analyst Vladimir Zivadinovic, IDC European Customer Insights & Analysis. With expenditures of more than \$7 billion, manufacturing is projected to have the highest level of IT security spending of any sector in 2021. As manufacturing becomes more automated, organizations are increasingly targeted by malicious actors, raising the risk of data loss, and damage to physical assets.

The banking and government sectors are projected to be the second and third top spenders on IT security in 2021, each with expenditures of around \$5 billion. Both sectors are increasingly digitalizing to adapt to the COVID-19 "new normal." As industries that work with high volumes of sensitive data, having effective IT safeguards is a priority.

The government sector is expected to lead in terms of growth in IT security spending in 2021, followed by telecommunications & media and transportation. Each of these sectors is expected to boost spending by more than 9% year on year.



Strong growth for the managed edge services market

Managed edge services promises to be a high-growth market as enterprises look to low-latency edge services to address process efficiencies, support new consumer applications, comply with data sovereignty, and deal with security threats.

ACCORDING TO A NEW FORECAST from International Data Corporation (IDC), worldwide revenues for managed edge services will reach \$445.3 million in 2021, an increase of 43.5% over 2020. Over the 2021-2025 forecast period, the compound annual growth rate (CAGR) for managed edge services is expected to be 55.1%.

Given the nascent demand for managed edge services, a wide range of service providers and technology vendors are looking at this market as the next big revenue opportunity. IDC believes public cloud providers, or hyperscalers, will be key enablers of edge services through the partnerships they are establishing with 5G service providers. Some service providers are considering edge services as the catalyst for the fourth industrial revolution while CDN providers are already shifting their investments toward edge applications.

“Managed edge services represent a significant

monetization opportunity for service providers to capitalize on their investment in edge compute,” says Ghassan Abdo, research vice president, Worldwide Telecom, Virtualization, and CDN, IDC. “At the same time, service providers are keenly aware of the potential impact of the edge on their current market position and are watching closely for unforeseen competition from adjacent markets and new disruptors. Technology vendors including network equipment providers (NEPs) and software, datacenter, and networking vendors are vying to shape this market and play a significant role in delivering innovative edge services.”

Based on extensive discussions with service providers and technology vendors, IDC has identified three primary deployment models for managed edge services.

On-premises deployment: This represents managed edge use cases where the edge compute infrastructure is deployed at the enterprises’

premises, also referred to as private deployment. This deployment model is intended to address the need for extra low latency and is applicable to industrial use cases, healthcare, and AR/VR applications.

Service provider edge deployment: This represents managed edge services provided by edge compute deployed at the provider edge, both fixed and mobile. IDC expects this deployment model to spur development of a wide range of vertical use cases.

CDN edge deployment: This represents managed edge services provided by edge compute deployed at the CDN POPs or edge locations. These use cases will enhance content delivery with personalized, high-fidelity, and interactive rich media customer experience.

IDC projects the on-premises edge to be the fastest growing segment with a five-year CAGR of 74.5%. The service provider edge will be the second-fastest growing segment with a CAGR of 59.2%, which will enable it to become the largest market segment by 2022. The CDN edge segment is expected to have a five-year CAGR of 41.9%.

Big Data and analytics spending to reach \$215.7 billion

Worldwide spending on big data and business analytics (BDA) solutions is forecast to reach \$215.7 billion this year, an increase of 10.1% over 2020, according to a new update to the Worldwide Big Data and Analytics Spending Guide from International Data Corporation (IDC). The forecast also shows that BDA spending will gain strength over the next five years as the global economy recovers from the COVID-19 pandemic. The compound annual growth rate (CAGR) for global BDA spending over the 2021-2025 forecast period will be 12.8%.

“As executives seek solutions to enable better, faster decisions, we’re seeing relatively healthy BDA spending across all industries. Leveraging data for insights into everything from internal business operations to the customer journey is top of mind and of strategic importance,” said Jessica Goepfert, program vice president, Customer Insights and Analysis. “Firms in the professional services industry, for instance, are utilizing Big Data and analytics to support their 360-degree customer and client management efforts, as well as advanced project

management initiatives. Banks are using BDA solutions to improve customer onboarding while simultaneously automating business operations and detecting and preventing fraud. Even slower moving industries like construction have started to fuel investments in extended supply chain planning and interconnected and collaborative workspaces.”

The industries currently making the largest investments in big data and analytics solutions are banking, discrete manufacturing, and professional services. Combined, these three industries will account for one third of all BDA spending in 2021. The next three industries – process manufacturing, telecommunications, and federal/central government – will together deliver nearly \$47 billion in spending this year. While the telecommunications industry will see the fastest growth in BDA spending over the five-year forecast, all but one of the 19 industries covered in the Spending Guide are expected to deliver double-digit growth.

Over half of all BDA spending in 2021 will go toward services with IT services accounting for more than \$85 billion of the total and business services making up the remainder. The second largest segment of BDA spending this year will be software, which will see investments totaling \$82 billion. Almost half of this total will go to three types of applications – End-User Query, Reporting, and Analysis Tools, Relational Data Warehouses, and Nonrelational Analytic Data Stores – with the remainder spread across the 13 remaining software categories. Software will also be the fastest growing segment of BDA spending with a five-year CAGR of 15.1%.

“Unlike many other areas of the IT services market, big data and analytics services continued to grow in 2020 as organizations relied on data insights and intelligent automation solutions to survive the COVID-19 pandemic,” said Jennifer Hamel, research manager, Analytics and Intelligent Automation Services. “The next phase of digital resiliency will spur increased investment in services to address both lingering and new challenges related to enterprise intelligence initiatives.”

On a geographic basis, the United States is the largest market with more than \$110 billion in BDA spending this year. Japan and China are the next

On a geographic basis, the United States is the largest market with more than \$110 billion in BDA spending this year. Japan and China are the next two largest markets with BDA spending forecast to reach \$12.4 billion and \$11.9 billion, respectively. The United Kingdom is the only other country expected to surpass \$10 billion in BDA spending this year.

two largest markets with BDA spending forecast to reach \$12.4 billion and \$11.9 billion, respectively. The United Kingdom is the only other country expected to surpass \$10 billion in BDA spending this year. Argentina is forecast to see the fastest growth in BDA spending over the forecast period with a five-year CAGR of 21.2%. China's CAGR of 20.1% will enable it to become the second largest market by the end of the forecast.

IaaS and PaaS to hit \$400 billion revenue in 2025

International Data Corporation (IDC) recently published a new forecast for the Worldwide Public Cloud Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) markets, which includes revenue segmentation across IDC's 18 enterprise workload categories.

The combined Public Cloud IaaS and PaaS market is forecast to have revenues of \$400 billion in 2025 with a compound annual growth rate (CAGR) of 28.8% during the 2021-2025 forecast period. Application development and testing, structured data management, and structured data analytics will be the largest workload segments by revenue share.

Unstructured data analytics/data management and media streaming are forecast to be the fastest growing segments with CAGRs of 41.9% and 41.2%, respectively. Other business applications, file and print, and content applications will grow slower than the overall market average while still delivering double-digit growth throughout the forecast period.

"Enterprise spending on public cloud infrastructure continues to grow faster than traditional IT infrastructure segments," said Andrew Smith, research manager Cloud Infrastructure Services. "We expect all workload segments to grow in the double digits

– some slightly faster than others – as enterprises emerge from 2020 and continue to prioritize workload migration and modernization using public cloud infrastructure."

Cloud IaaS and PaaS is a critical, enabling component for the future of digital infrastructure. The future of digital infrastructure is highly dependent on the ability of complex, connected cloud infrastructure to self-regulate and dynamically optimize itself in response to real-time changes in resource demand, application performance, and end-user experience.

By 2022, IDC anticipates that almost half of an enterprise's products and services will be digital or digitally delivered, increasing the business' reliance on infrastructure (compute, storage, networking) to support more than traditional business applications. Timely access to innovative infrastructure resources – both shared and dedicated – will be imperative to sustain the adaptive, resilient, secure, and compliant digital business models of the future.

Additional trends driving workload growth within this market include:

- Public cloud services remain an essential part of enterprise recovery strategy as IT organizations reevaluate budgets, build infrastructure focused on business resilience, and work toward operating efficiently and managing risk in a post-COVID-19 world.
- Enterprises are shifting from workload migration to workload modernization on public cloud. In 2020, we saw IaaS buyers increasingly prioritize application modernization efforts, viewing modernization as an integral component of the move toward agile application delivery and cloud operations.
- Relentless enterprise data growth continues to push many workloads to the public cloud, as enterprises look to effectively manage data growth, as well as their IT budget. In many cases, cloud infrastructure and application platforms help meet this need by enabling agile and consistent scaling of capacity that can be utilized on demand.

Solid growth for GRC solutions

Worldwide revenues for governance, risk, and compliance (GRC) software experienced healthy growth in 2020, growing 8.2% year over year, despite concerns of a market downturn resulting from the COVID-19 pandemic. At the same time, the pandemic highlighted the need for better coordinated GRC solutions, which is driving further investment. A new forecast from International Data Corporation (IDC) shows global GRC revenues growing from \$11.3 billion in 2020 to nearly \$15.2 billion in 2025.

While the GRC market has experienced a drastic transformation over the past several years, the COVID-19 pandemic elevated the focus on risk areas and threats to business continuity. In addition, the



regulatory environment has both expanded and become more stringent, particularly around privacy, placing greater pressure on enterprises and their compliance capabilities. And corporate boards are facing new directives on environmental and social responsibility from investors and consumers that is forcing them to redefine how enterprises approach governance.

Given the demand for solutions, IDC expects all categories of GRC to increase in revenue over the forecast period. The fastest growth will be in the business continuity and ESG/CSR categories, followed by compliance and risk management. Evolving categories, such as privacy, third-party risk management (TPRM), and environmental, health, and safety (EHS) are also expected to experience solid growth.

“The GRC market is positioned for significant growth as companies seek ways to automate and manage the complexities of expanding governance, risk, and compliance mandates. Understanding how businesses are consuming these solutions and their preferences for packaging and deploying services will help solution providers tailor offerings to meet market demand,” said Amy Cravens, research manager, Governance, Risk, and Compliance at IDC. To better understand the current state of the enterprise

GRC market, IDC recently surveyed more than 200 GRC users in the United States. The survey found that nearly two thirds of organizations currently use multiple GRC solutions with some companies deploying five or more. And enterprises with a higher number of GRC solutions tend to have a lower rate of integration across these solutions. This indicates that enterprises with the highest spending on GRC may not be implementing GRC in an efficient manner and leveraging that investment across the organization.

Other key findings from the survey include the following:

- IT & Security Risk Management is currently the most widely implemented GRC solution, followed by Data Privacy Tools and Management and Corporate Social Responsibility Management.
- Most companies plan to increase their GRC spending over the next three years with IT & Security Risk Management the top area for planned investment.
- Most companies are striving to integrate their GRC solutions more fully but remain divided on the question of custom versus out-of-the-box solutions. Siloed solutions are generally unpopular.
- While nearly one third of respondents require GRC solutions to be deployed on premise, one half expect use of cloud-based solutions to increase over the next three years.



DW ONLINE ROUNDTABLE

BASED around a hot industry topic for your company, this 60-minute recorded, moderated zoom roundtable would be a platform for debate and discussion.

MODERATED by an editor, this online event would include 3 speakers, with questions prepared and shared in advance.

THIS ONLINE EVENT would be publicised for 4 weeks pre and 4 weeks post through all our mediums and become a valuable educational asset for your company

Contact: Jackie.cannon@angelbc.com

DW **DIGITALISATION WORLD**

Delivering an effective cybersecurity strategy

Cybersecurity continues to be a major challenge for companies, with as many as four in ten businesses (39%) reporting cyber security breaches or attacks in the last 12 months.

BY RICHARD SLATER, HEAD OF MANAGED SERVICES AT **AMIDO**



WHILST MANY HAVE STRUGGLED with security issues for decades, the COVID-19 pandemic has compounded such problems. The shift to remote working has made company devices and critical business activity vulnerable to unsecure home networks which exist outside of the scope of traditional security operations teams. This has resulted in many IT teams struggling to safeguard their data and adjust their security practices over the last year.

Whilst many saw the pandemic as a catalytic moment for digital transformation, there's no reason why the same can't be said for cybersecurity. However if companies are going to revolutionise their security practices, they must rethink the way security is

communicated across the business. Here are three vital components that make up an effective cybersecurity strategy in 2021.

Sync cybersecurity with strategic goals

A successful cybersecurity strategy should be in sync with a company's strategic goals and must avoid hindering business performance or productivity. Historically, cybersecurity measures have made it harder for employees to carry out their day-to-day operations, with restrictions in place that strangle operational effectiveness. However, if cybersecurity measures restrict workflow this will lead to frustration among employees and limit the amount of staff adhering to necessary security procedures and even

CYBERSECURITY PLAN



driving them to circumvent security controls. Cybersecurity must also act as an enabler to the overriding strategic aims of the business, rather than setting the agenda itself. Rather than focusing on security first, start outlining the digital objectives of the company and then layer these with security measures that safeguard company data and information. In other words, companies should start with what they wish to achieve and then the security measures will become clear afterwards.

Furthermore, serious problems can arise when information security teams aren't included in the design of solutions. Without continued communication and collaboration, information security teams can be blindsided with potential security risks that they have no choice but to isolate and secure. This creates the reputation that the information security team is the 'big bad wolf', rejecting digital initiatives and arbitrarily enforcing roadblocks that hinder progress. In reality, if information security is integrated into the design and planning stages of digital initiatives throughout, this can foster a better working relationship so that when initiatives are launched they already have the security features required to get the green light.

If this level of collaboration is maintained, then over time digital teams will also become more aware of how to make initiatives secure from the outset. This process requires a cultural reset by which an entire company recognises that information security objectives are shared with the business objectives of the wider organisation, and are required to protect against regulatory, financial and reputational risks inherent to operating technology.

Sharpen up training

Cross-collaboration and harmonising security procedures with digital initiatives and strategic objectives is just the first step. Upholding a high standard of cybersecurity relies heavily on the successful communication of such procedures. Not every employee needs to be an expert in cybersecurity best practices, but the better prepared each and every staff member is, the less likely they'll risk exposing company data to cyber criminals and hackers. Internal cybersecurity training is the fundamental bridge between a company's team of security experts and the wider workforce. It's therefore crucial not to get it wrong. Security training is more effective if it is short, concise, interactive and fun. A succinct 25 minute training session every quarter is going to be much more impactful than a long, five hour session every year.

It's also important to avoid 'blanket' security training and embrace tailored sessions specific to certain job roles. This is best achieved by adopting various tiers of security training that offer individuals the information they need in order to keep company data safe. In addition, training must be communicated through gentle reminders with tangible incentives.

Furthermore, information security teams will put their colleagues in the best possible position by ensuring the most secure approach is also the 'easiest' approach. This will mean everyone selects the 'path of the least resistance' and therefore adhere to security by default. Adopting this structure will act as a safety net alongside the regular training sessions put in place.

Adopt a collaborative approach to shadow IT

Maintaining due diligence when it comes to cybersecurity training will ensure employees remain as vigilant as possible to the threats of cybercrime, such as phishing and ransomware attacks. Yet there will inevitably always be a risk, often in the form of shadow IT. This has been a recurring problem for companies in recent years, however it's certainly now of greater concern because the risk of exposure through shadow IT has risen several notches due to the rise of remote working over the last year.

It is now much harder for IT teams to track which software staff are utilising when the entire company is operating from remote, disparate locations. The trick to countering this issue though is to start saying "yes" rather than defaulting to "no". Making a concerted effort to understand why teams have deployed unapproved tech fosters a more collaborative culture, and once you have this understanding you can drive towards the win-win situation to help them in the area that they are trying to help themselves. By being more open and honest, companies are encouraging employees to come to their IT department with requests for help in implementing secure solutions rather than making the initial problem far worse. Most complications around shadow IT come from the perception that IT teams aren't attuned to the needs of the organisation, prioritising collaboration helps to combat this perception and lower the risk of shadow IT. In fact, embracing an open-source approach that breeds a culture of collaboration will serve companies well in their quest for good cybersecurity.

The 'Trust but Verify' model is a great example of cross-collaboration between teams. It means that information security teams train end users and trust them to do the right thing but deploy automation to verify that the work they are doing complies with relevant policies. This empowers end users to remain autonomous and make decisions quickly whilst still knowing there is a verification model that will protect their company from any potential mistakes. Security teams exist as an extension of the business and enable productivity, rather than hinder it. This shift in mindset relies on the successful communication of best practices, effective training and the merging of cybersecurity initiatives with the wider strategic goals at the heart of the business. If companies can implement these measures successfully then 2021 can become a catalytic moment for cybersecurity, just as it was for digital transformation 12 months ago.

Common misconceptions around cloud-native security

The most crucial part of any cloud native journey is learning about cloud native security early on in the process.

BY RANI OSNAT, VP STRATEGY AT **AQUA SECURITY**



ADOPTION RATES for cloud native application architectures are rising quickly within enterprises, and for good reason. Portability, scalability and efficient resource utilisation are commonly cited benefits, but the greatest boon is the significantly reduced deployment times enabled through a cloud native approach. A cloud native approach gives organisations far more flexibility and control over the infrastructure they use, enabling faster workflows and deployment processes. This goes some way to explaining why the number of containers in production has jumped 300% since 2016. However, don't let these numbers fool you. Although cloud native is gaining a

foothold within businesses, there is still a lack of cloud native experience within many development teams, and a lot of common misconceptions, particularly regarding security.

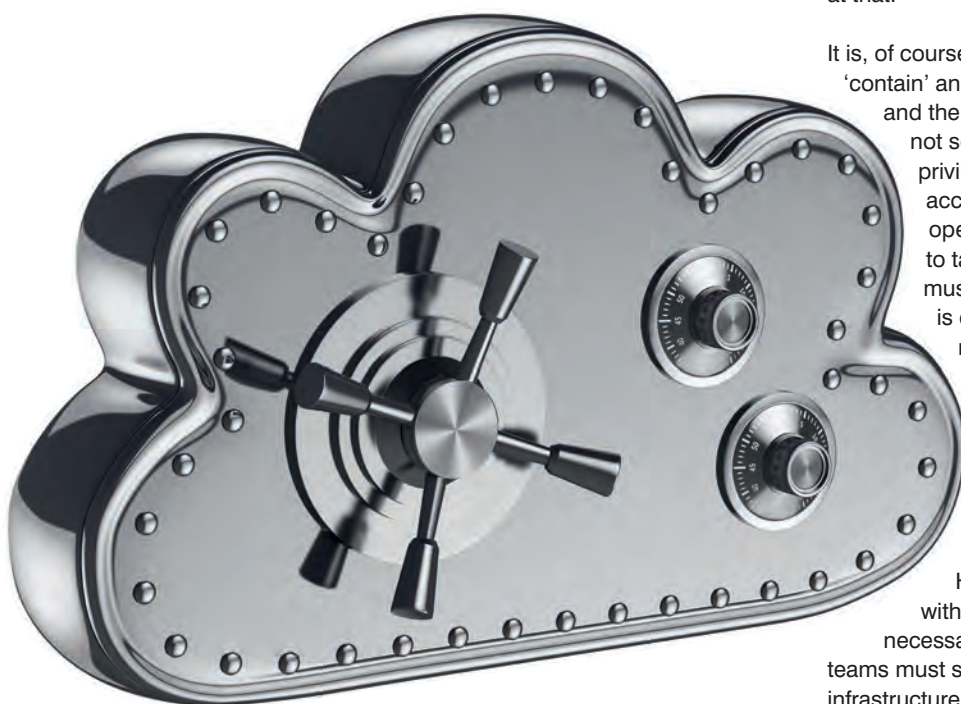
Misconception #1 – We don't need a specific cloud native security strategy

The separation of discrete computing components in containers, alongside concepts like immutability, provide the impression (at least at first glance) that cloud native applications are, by their very nature, secure. This is one of the most common misconceptions we see, and quite a dangerous one at that.

It is, of course, convenient to assume that containers 'contain' and are segregated from other containers and the OS they're running on. But the truth is not so simple. If one runs a container with root privileges, that container could potentially access all the resources on the host, opening up the possibility for an attacker to take over that host. Privileged access must be controlled before the container is deployed and re-checked using cloud native runtime enforcement capabilities.

Embedding cloud native security into cloud native initiatives can make applications and infrastructure more secure, and microservices running in containers or as serverless functions, provide ways to limit exposure.

However, a cloud native deployment without a security strategy does not necessarily enjoy full protection, and security teams must still set policies across the build, cloud infrastructure and running workloads.



Misconception #2 – Secure application code should be the primary focus

Application code should of course be error-free and technologies such as static application security testing (SAST) are of great importance whether you're working with custom code written entirely by your own team, or as is likely the case today, with code assembled from multiple open-source libraries. However, there is much more to securing a cloud native application than just securing the source code. The best, most secure code still won't protect against a scenario where images, which should never change in production, begin executing commands in runtime that were not included in the base image. Nor will it prevent orchestrator misconfigurations or cloud account misconfigurations that can leave entire cloud services open to attack.

Developing secure images is an important element, but a broader focus on securing the overall pipeline from build to deployment, as well as the security posture of the infrastructure it will run on, can be even more critical.

Misconception #3 – Development issues will be fixed in production

One of cloud native's most prominent benefits is immutability, which essentially means that workloads will not and should not change while running in production. In cloud native environments, if a container needs to be updated or configuration changes need to occur, a new version is created within the pipeline to completely replace the previous workload. Making fixes earlier in the pipeline, and then rolling-out new versions through automation results in reduced downtime for patching, which consequently impacts how security teams plan on fixing vulnerabilities.

Confusion arises when security teams are still under the impression that fixes will be made in runtime. When this happens, it puts them at a disadvantage when security issues are 'shifted left' to the DevOps teams, which builds and tests the app in the CI/CD workflow.

Essentially, although the security team must still be involved in protecting against exploits and vulnerabilities in the application itself, how and when they do so needs to change. A stronger partnership with the DevOps team must be forged, and any activity must happen earlier in the pipeline. Fostering this new mindset within both the DevOps and security teams can have huge benefits. With a cloud-native deployment model, the time spent by operations teams deploying patches can be reduced by around 75% (according to a recent Forrester Total Impact study). With fixes made earlier, workloads can simply be re-deployed as new instances. Getting it wrong, however, can lead to security gaps.

One of cloud native's most prominent benefits is immutability, which essentially means that workloads will not and should not change while running in production. In cloud native environments, if a container needs to be updated or configuration changes need to occur, a new version is created within the pipeline to completely replace the previous workload

Conclusion

If teams can get to grips with these common misconceptions, they can begin planning an effective cloud native security strategy. Only through a thorough understanding of the realities of the cloud native journey can teams really begin to plan out the responsibilities, resources, controls, and new interdisciplinary relationships that need to be forged. The most crucial part of any cloud native journey is learning about cloud native security early on in the process. CISOs should be equipping themselves with knowledge and skills around cloud native as a matter of urgency because, if security is done right, it can accelerate adoption, improve efficiency, and make security the main pillar of cloud native.





A question of priorities

Where should cloud-centric organisations focus data protection?

BY ANURAG KAHOL, CTO, **BITGLASS**



FOR MANY ORGANISATIONS, creating an effective data protection strategy to support the adoption of remote work and cloud infrastructure is becoming increasingly urgent. But in working to mitigate risks and build robust processes, IT leaders face a range of challenges, and getting the priorities right is key to overcoming issues as varied as data leakage, compliance, and access control—all while maximising user experience.

So, where should they start? And what are the main data protection challenges that can threaten the integrity, management, and security of distributed data?

Challenge 1: Removing the risk of hidden data loss in encrypted traffic

When workers were in the office and connected directly to the company network, data and applications resided in central data centres, encrypted traffic was limited, and, as a result, on-premises security solutions were sufficient. However, with the move to the cloud, the use of the web, and the widespread adoption of remote working, encrypted traffic has shifted from the exception to the rule. If current data protection solutions don't identify and

control sensitive data in encrypted traffic, they will miss the majority of sessions in which data exposure and misuse is a possibility, leaving the organisation vulnerable to data loss and breaches.

Solution: Stolen data is often disguised and sent uninspected through SSL, and according to a recent Google Transparency report, 95% of traffic is encrypted and therefore not subject to inspection by traditional DLP solutions. This is potentially disastrous, as partial inspection of traffic leaves businesses vulnerable to data loss, meaning sensitive data passing through may be missed.

Consequently, organisations need cloud and web security solutions that can inspect every byte outside the network and beyond the scope of legacy technologies. With this approach, they can ensure that data within encrypted traffic is secure.

Challenge 2: Closing gaps between data protection services

With the move to the cloud, data is distributed across diverse SaaS, IaaS, web, and on-premises environments. Naturally, each of these needs effective data protection. As a result, organisations are adopting cloud access security brokers (CASBs) to secure managed SaaS applications and IaaS platforms, cloud security posture management (CSPM) to scan IaaS instances for costly misconfigurations, secure web gateways (SWGs) to secure the web and unmanaged apps (shadow IT), and zero trust network access (ZTNA) to secure residual on-premises resources as they are accessed remotely. However, this complexity makes data protection uniformity and solution management challenging, and can waste time and money while creating gaps in visibility and control across resources.

Solution: Unified protection, whereby a consistent level of security is provided to all interactions across ecosystems, can be achieved by adopting a comprehensive security platform built in and delivered through the cloud. Today's market-leading technologies can monitor data in transit and at rest within IT resources through capabilities like cloud DLP and ATP. Consistent, easily managed security across all interactions is key.

Challenge 3: Avoiding poor user experience

With workers and the resources they access and use to do their jobs moving off premises, a major element of core infrastructure is now the internet itself. One of its downsides, however, is that this approach limits IT's ability to anticipate, identify, and mitigate issues with their legacy security stack. Additionally, when the majority of services, solutions or applications used by workers are out of the organisation's control, it becomes more difficult to ensure that employees have a good user experience and maintain productivity while data stays safe.

With workers and the resources they access and use to do their jobs moving off premises, a major element of core infrastructure is now the internet itself. One of its downsides, however, is that this approach limits IT's ability to anticipate, identify, and mitigate issues with their legacy security stack

Solution: Many appliance-based security offerings require traffic to be backhauled to a central data center, creating bottlenecks and causing latency, which directly impacts user experience and productivity. A platform that embraces the concept of secure access service edge (SASE) puts data security as close as possible to the user, reducing latency and significantly improving the user experience.

Challenge 4: Eliminating compliance violations across the cloud

Failing to meet and maintain required industry regulations can result in significant fines and even loss of business. With data distributed across SaaS, IaaS, the web, and a myriad of devices with remote access to enterprise networks, visibility and remediation for compliance purposes are reduced, potentially putting your company at risk.

Solution: By obtaining unified visibility and control across the entire IT ecosystem, a range of key compliance standards (PCI DSS, HIPAA, and GDPR, and others) can be met, minimising the risk of compliance violations in today's complex environments. This is done through, once again, through integrated platforms that boast a variety of functionality (DLP, IAM, CSPM, and others) which can ensure that specific regulatory requirements are addressed.

By including these important considerations in data protection strategy planning and execution, organisations can embrace digital transformation with confidence. In doing so, they can close gaps between data protection services, minimise risk, achieve compliance, and deliver a consistently strong user experience.

Navigating shark-infested waters

Why businesses need a bigger boat for tackling IaC security

BY ROBERT HAYNES, SCA & OPEN SOURCE EVANGELIST, **CHECKMARX**



LAST YEAR brought with it a digital escalation of epic proportions for organisations across the globe. As a result, many turned to the cloud to maintain business continuity, ensure the security of their information, and afford their teams the flexibility they suddenly required.

But, with this transition came new challenges for software developers, one of the biggest of which revolved around the proliferation of infrastructure as code (IaC).

Just like Chief Martin Brody in the classic movie *Jaws*, it's forced many developers into uncharted waters. They're taking on a complex beast for the first time, often without proper training or tools in place to do so in a secure manner.

And similar to the mounting pressure put upon the rookie seaside cop to quickly restore normality to Amity Island, expectations to build code quickly in this new environment are ever increasing. With IaC prone to issues like misconfigurations or vulnerabilities which may jeopardise a business, what must organisations do to ensure malicious actors (or fierce ocean beasts) don't take a nasty bite out of them?

Tackling the IaC AppSec beast

With the multitude of cloud services and configurations, IaC templates can become extremely complex. This means, just like the sea-dwelling predator of *Jaws*, there's a lot developers and organisations may not fully understand about the infrastructure they create with IaC, especially when



it comes to security. Unfortunately, the security tools used by many today are not designed to understand IaC templates, let alone spot valid but unwise configurations.

This leaves any application developed within these flexible environments susceptible to attackers looking to prey on, and exploit any misstep made by developers. As Chief Brody found, fending off such menace isn't simple, especially with the speed of development across today's security landscape.

When it comes to application security more generally, it's important to note that when adopting IaC, an organisation's infrastructure is part of a set configuration of files which need to be scanned as part of the overall code. This is often a tough ask for any security testing solution, and presents one of the biggest obstacles to AppSec – making the connection between code, infrastructure, and configurations.

In an effort to combat these challenges and keep the aforementioned actors at bay, it's vital for businesses to concentrate on cloud-native, and specifically IaC for the purposes of this article, security training for developers. To build a robust security culture however, it takes more than just 'once in a while' training, with workers needing ongoing coaching that's interactive and engaging to truly make a difference.

As well as this, organisations should look at allocating additional spend towards software and application security to support the demand of a remote workforce – especially with the rise of the hybrid working model – as well as the more complex software ecosystems they've had to implement this past year.

And just when you thought it was safe...

When it comes to AppSec in the cloud, developing and releasing applications quickly, while maintaining security, is a mindset that, while often talked about, just isn't being executed effectively. This is corroborated by our recent developer survey which found that one in six (15%) aren't performing

any security testing when building cloud-native applications.

Cloud deployment needs to happen fast with as many drops as possible. With this, the current philosophy at many organisations – to get software straight into production and roll back if a bug is found – doesn't work for security.

Yes, it might mean features can be pushed more quickly, but it's not possible to push code and roll back to fix vulnerabilities without presenting an open goal to cybercriminals looking to infiltrate your system.

This mindset is starting to change, and the demand for cloud-based security is increasing the use of IaC. However, this on its own isn't enough. Just because an organisation is starting to adopt such a mindset doesn't mean it's safe to get back in the water. In fact, the tools used for application security which integrate into the tool chain must work far more rapidly, scale to cloud environments and present actionable findings – in a format developers understand – for them to be able to make quick fixes.

Reeling in the benefits

IaC establishes a methodology with tools and technology for infrastructure configuration and provisioning through code. Offering advantages such as automation and cost-reduction, it's a no brainer for many organisations. Despite this it is prone to issues including, security vulnerabilities which could jeopardise not just the applications being built, but an entire business.

To see the true advantages of IaC and ensure security vulnerabilities are kept at bay, businesses need to implement the aforementioned developer security training, ensure increased budget spend on AppSec, and completely overhaul their mindsets when it comes to fixing vulnerabilities.

Only by doing this can they ensure their IaC security practices are strong enough to prevent even the fiercest of adversaries from pulling them under.



XPEDITE INTEGRATES THE IT INFRASTRUCTURE WITH FACILITIES MANAGEMENT IN ONE PLATFORM

THE ONLY DCIM SOFTWARE PLATFORM THAT CAN ENABLE INFORMED DECISION MAKING BY AUTOMATING CAPACITY MANAGEMENT; MIGRATION; ASSET MANAGEMENT AND WORK ORDER PROVISIONING.

DITCH THE INFERIOR

Xpedite

www.rittech.com

[Find Out More](#)

From cloud to the edge:

How Zero trust security makes the everywhere workplace possible

Zero trust security clearly offers the most efficient and cost-effective way to secure the everywhere workplace, which is the future of work.

**BY NAYAKI NAYYAR, EXECUTIVE VICE PRESIDENT AND CHIEF PRODUCT OFFICER,
IVANTI**



THE COVID-19 pandemic has permanently changed the workplace of the future. In fact, a recent Gartner survey found that 90% of respondents plan to allow employees to work remotely at least part of the time, even after the COVID-19 vaccine is widely adopted.

In this new “everywhere workplace,” IT networks, applications, and data are being accessed from everywhere, with employees using various devices to access corporate data and services as they work from any location. While productivity has skyrocketed, this remote work landscape has also expanded the enterprise attack surface and created new security challenges for organizations.

Adding to the challenges posed by the everywhere workplace is the fact that employees are not prioritizing security, even though cybersecurity threats targeting remote workers have reached catastrophic new heights. Ivanti’s 2021 Secure Consumer Cyber Report found that one in four consumers admit to using their work email or password to log in to consumer websites and applications such as food delivery apps and online shopping sites, putting themselves and enterprises at risk.

So, how can IT departments secure their digital assets and defend against the onslaught of attacks aimed at remote workers?

Zero trust security to the rescue

The everywhere workplace demands everywhere security. Say hello to zero trust security!

At its simplest, zero trust security enables organizations to continually verify each asset and transaction before permitting any access to the network. Verification includes, but is not limited to, strong authentication of users, posture checks for devices, and micro-segmentation of networks. Zero trust also takes the whole context of the user's environment into consideration, not just unconnected pieces of data, before granting access. For instance, is the employee trying to access sensitive customer data from a corporate-owned device on a secure enterprise network, or from a personal smartphone using free Wi-Fi at the airport?

With a zero trust model in place, companies can effectively defend against the leading causes of data breaches, such as stolen credentials, password reuse, and user impersonation. In addition, when deployed correctly, zero trust can protect user and data privacy, which is an increasing concern for both users and organizations today.

Automation is key to zero trust effectiveness

Automation that takes context into consideration is a key component of an effective zero trust authentication strategy. Automation tools typically include fundamental zero trust security features such as continuous device posture assessment, role-based user access control, and location awareness. By ensuring the user and device are in good health, companies also ensure that valid requests will be granted quickly and efficiently to reduce the operational cost and pain of zero trust.

With deep learning, supervised and unsupervised learning capabilities, enterprises can proactively and predictively detect configuration drift issues, performance issues, application crash issues, security vulnerabilities, etc. on devices and remediate them before the end user experiences any disruption. For example, Ivanti Neurons lets IT query all edge devices with sensor-based technology and natural language processing to get real-time intelligence



across the enterprise in seconds. It provides quick operational awareness, real-time inventory, and security configurations across all devices on the edge.

A self-healing future

With best-in-class contextual automation and zero trust technologies, enterprises can proactively and predictably detect issues, and then self-heal and self-secure devices.

Customers of Ivanti Neurons experience over 50% reductions in support call times, eliminating duplicate work between IT operations and security teams, and reducing the number of vulnerable devices by up to 50%. Customers of Ivanti Neurons also reduce unplanned outages up to 63%, reduce time to deploy security updates by 88%, and resolve up to 80% of endpoint issues before users report them.

Looking ahead, zero trust security clearly offers the most efficient and cost-effective way to secure the everywhere workplace, which is the future of work. Companies should urgently accelerate their zero trust journey and leverage latest technologies to mature their implementations. In addition to significantly reducing the risk of breaches, an effective zero trust strategy can deliver secure, contextual, and personalized user experiences in this next normal.

Automation that takes context into consideration is a key component of an effective zero trust authentication strategy. Automation tools typically include fundamental zero trust security features such as continuous device posture assessment, role-based user access control, and location awareness

Why openness means better cyber security

The Open XDR movement is gaining traction.

BY BRIAN FOSTER, VICE PRESIDENT OF PRODUCT MANAGEMENT AT RELIAQUEST



WHEN WE THINK OF SECURITY, many will conjure up a mental image of steel doors with impressive locks, armed guards or banks of CCTV camera feeds viewed from a darkened control room – the visualisation is of keeping criminals out and away from our valuable property – and in the case of IT, protecting critical systems, and data.

Cyber security is also resplendent with similarly protective language as nothing sounds scarier than a wall of fire (Firewall), secure perimeter or a cyber kill chain! The latest iteration gaining momentum in cyber security is Extended Detection and Response (XDR) which, depending on which security vendor you ask, “... collects and automatically correlates data across multiple security layers.”

Yet the term XDR which is going through its own hype cycle has been co-opted by many cyber security vendors as a way of convincing customers to buy all their security products from a single supplier. The simplistic logic is often – buy all the bits you need from us, and we can make sure it all works together. For a large enterprise with a dozen different security products – probably from at least half-a dozen different suppliers,



the prospect of having to rip and replace systems is unappealing.

Cyber security is a massive industry. Worldwide spending on information security and risk management technology and services is forecast to grow 12.4% to reach \$150.4 billion in 2021, according to the latest forecast from Gartner, Inc. A staggering sum but still dwarfed by damage caused by global cybercrime that is predicted to reach \$6 trillion annually by 2021 according to Cybersecurity Ventures, an analyst firm.

Legacy approach

The hundreds of vendors selling cyber security products and services have traditionally focused on individual product silos. Specialists in malware protection, firewalls, content inspection, intrusion detection – the list is endless. However, over the last decade, many of these well-known brands have moved sideways – to sell more products. In the last few years, a period of consolidation has seen several brands merge to now offer the entire spectrum of cyber security products across diverse portfolios. The aim is ultimately to increase the average spend per customer and – at least in theory – to ensure everything works together.

Yet, just like white goods in a typical kitchen, few organisations buy an entire cyber security stack of technology and services from a single vendor. According to AttackIQ and the Ponemon Institute, large organizations use an average of 47 different cybersecurity tools across their networks. While research firm ESG estimates that enterprises source their tools from an average of 10 different vendors.

However, herein lies a major issue. In a market chasing after \$150bn a year in potential revenue, there is little incentive for cyber security vendors that sell extended portfolios to work seamlessly with rival vendors. This is a broad statement and there

are some notable exceptions in areas such as SIEM

where the core purpose is to pull together disparate systems. There are also a few vendors that have gone above and beyond in getting their systems to play nice with third party tools – but these are the exception rather than the rule.

Open XDR

For many, XDR could be a different proposition as its goal is to correlate data across multiple security layers. Yet examining the vendor propositions in detail these integrations tend to focus on products within the vendors own stack. Instead, a few pioneers are pushing for an Open XDR approach that aims to not just have a handful of supported third party cyber security products, but tens and ultimately hundreds of integration points.

The companies pushing for this Open approach, ReliaQuest included, generally do not have an anti-virus, firewall, VPN, NAC, or MDM solution to sell – and as such are primarily focusing on adding integration based on what potential customers are already using. The goal is to raise visibility across the entire cyber security landscape to gain a single source of insight and response.

The Open XDR movement is gaining traction and is primarily focused around a few key areas. The fastest growing is cloud security where these systems can peer into multiple clouds, tools, and locations to create a single platform for unified visibility, detection, and response.

Another area is security automation to streamline the investigation process triggered by an alert and allow infosec teams to use accurate data from multiple systems to spot real attacks rather than false alarms.

The last major area is continuous analysis and reporting to validate – and ultimately improve security posture. Open XDR is also gravitating towards being delivered ‘as-a-service’ model which also streamlines deployment and allows organisations to adapt as the threat landscape evolves or the business need changes. Increasingly, many of these capabilities are supplemented by machine learning techniques – and as the Open XDR landscape grows, more third-party tools and data sources are integrated - which in turn makes the overall systems more intelligent and capable of detecting and responding to threats. Essentially a virtuous circle.

Standard evolution

Yet there are some inhibitors. After lack of awareness around Open XDR – the main issue is a lack of open standards for allowing different security tools to interoperate. Part of the problem is that many vendors that have larger “end-to-end” style portfolios have little to gain by working with rivals. In addition, these standards are not mandated within any regulatory frameworks – so there is no pull from customers to ensure interoperability compliance.

There are a couple of notable bright spots. MITRE, a not-for-profit organization that helps maintain the widely used Common Vulnerabilities and Exposures (CVE®) list is pioneering efforts through its Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) knowledge base to model cyber adversary behaviour, reflecting the various phases of an adversary’s attack lifecycle and the platforms they are known to target. MITRE is also working on two new initiatives for sharing cyber threat information. The first is Trusted Automated eXchange of Indicator Information (TAXII™) and this is supported by the Structured Threat Information eXpression (STIX™), both sponsored by the Department of Homeland Security.



TAXII defines a set of protocols for securely exchanging cyber threat information for real-time detection, prevention, and mitigation of cyber threats. STIX provides a common format for cyber threat information, including cyber observables, indicators of compromise, incidents, TTPs (techniques, tactics, and procedures), and campaigns. Another bright spot in the interoperability landscape is the Organization for the Advancement of Structured Information Standards (OASIS) that has created the Open Cybersecurity Alliance (OCA). The OCA brings together interested stakeholders to look at a solution for two big issues. The first is the development of an interoperable messaging format for cybersecurity tools, while the other will develop standardized data models and libraries to classify threats in a way that can be analysed by any cybersecurity tool.

All these projects are still at an early stage, but for enterprises that can see the potential merit in Extended Detection and Response – the key question to ask is whether its Open and able to support the cyber security platforms already in use? Or is it potentially forcing you down the road of having to rip and replace your cyber security infrastructure for the benefit of the vendors’ future sales.

How to develop and maintain an effective DevSecOps culture

Every increment in understanding and collaboration around the stack, delivery, governance and empowerment is a positive step forward in realising DevSecOps and safer applications.

BY PATRICK DEBOIS, DIRECTOR OF MARKET STRATEGY, **SNYK**



WITH THE CREATION OF DevOps, just over a decade ago, the intention was to break down the silos between development teams and operations. These silos created divisions and friction points that increased frustration, reduced productivity and prevented a holistic view of the delivery process. The focus was on uniting the different world views people had so both delivery speed and the quality of the product would improve.

Now, with DevSecOps, there's a similar desire to help the people doing the work, to reduce silos, delays and friction, but this time ensuring the product and all its ingredients are secure.

Through bringing roles together - development, operations and security - the team becomes more united, capable and knowledgeable, and thus better qualified to make decisions autonomously. The



place of management, which might previously have been situated between teams, operating from the centre, and perhaps adding extra friction, becomes more directed towards supporting this broader team and facilitating further collaboration. A successful DevSecOps culture means everyone has equal stake in all three objectives and uses their own expertise to support the others. Accountability, empathy, and enablement become crucial characteristics of successful teams.

Of course, this is not a change that can be introduced overnight, and the gestation period for DevSecOps will vary between companies. The nature and maturity of a company's collaboration culture is largely set by the CEO and will contain a mixture of control to create safety, measurement and KPIs to improve, as well as employee empowerment to foster autonomy.

Moving towards DevSecOps will benefit from continuing to improve the functionality of each of these layers. And each company will need to decide where to draw the line between team responsibilities and central management.

Similarly, different company cultures will gravitate towards different models of collaboration. In some, DevSecOps might be regarded as almost a separate project team, bringing together individuals from different teams on a temporary or part-time basis, or as a service layer added to the existing departments. At others, whole teams will work together, side-by-side, on a continual basis.

Some of these models (those that encourage more collaboration and ownership) are likely to be more effective - but the nature of the particular company culture will determine what can be done successfully.

Trust is crucial

However the initial formation is created, growing trust between Security and DevOps is going to be a major point for development. Creating real trust relies upon four, equally important elements: competence, reliability, sincerity and care.

You might view a colleague as competent to conduct a security scan, for example, but if they won't respond to your questions (reliability), or aren't concerned about the impact (care), it will reduce trust. And trust is a two-way street: You can't realistically ask for trust without also being trustworthy, and thus demonstrating these four characteristics. All of this takes time, and it's worth spelling out these ingredients of trust for all parties involved.

Four pillars of DevSecOps

Beyond these organisational and cultural considerations, DevSecOps typically has four main focus areas in which the development teams' responsibilities and considerations will extend far beyond their traditional remit.

THE STACK: The tooling that supports a DevSecOps pipeline is generally the beginning point for most organisational transformations: if your underlying technology doesn't accommodate the changes required, the attempt will fail. Developers want to ensure the application is secure and can be operated securely. Historically, this revolved around the code, but, as the organisation evolves towards DevSecOps, can extend to code dependencies, infrastructure, and external services. Then, pushing further, considerations will extend into user identity and key management frameworks, into logging and exception handling information, and even broader business considerations such as licences and data management.

DELIVERY: The technical process supporting development, security, and operations teams with cohesion and uniformity. Now, teams should ensure how the application is delivered is secure too. This again takes teams beyond code and into the application environment, how it's tested, how it's deployed, how patches are deployed and further.

Teams will need technology and tooling that can seamlessly integrate into the development pipeline. Integrated tools that require little effort are more likely to be adopted by developers, so adopting automation that supports the multi-functional needs of a DevSecOps model is key. Organisations need to look at their technology and automate when necessary and capable, streamline where possible, and eliminate where it's not practical or it is redundant. Minimising the various technologies through which the pipeline travels is an underrated but effective way to optimize software delivery.

Achieving DevSecOps requires technologies in place to enable employees to execute these processes as well as automate them. This, ultimately, reduces the organisation's attack surface and enables effective management of the technical security debt.

Achieving DevSecOps requires technologies in place to enable employees to execute these processes as well as automate them. This, ultimately, reduces the organisation's attack surface and enables effective management of the technical security debt

Delivery in a DevSecOps culture, should improve collaboration as well as achieving more secure development processes as a whole.

Governance: It's essential for a DevSecOps team to discuss how the processes for managing security can be improved.

Organisational processes in DevSecOps break down traditional barriers of authoritarian policies and workflows. To support the model of shared-responsibility, equity of purpose needs to be established between disciplines.

Gating models must be reviewed and removed where possible when shifting to DevSecOps. Traditional security strategies involved key milestones when progress could be halted until an acceptable result was achieved, creating lengthy feedback loops that slowed delivery and ultimately reinforced silo-based thinking. Mutual accountability must be embraced, as a replacement to gating, supported by subsequent process changes.

A significant feature of governance in the DevSecOps culture is to establish a comprehensive metrics program. The ability of the culture to grow and continually improve needs to be demonstrated to the business. Measuring a baseline of vulnerabilities can begin this process, but keep in mind that collaboration is part of the culture.

Teams should be considering security management, threat and risk management - and again, outwards into affairs around compliance, regulations and supplier management.

While the technologies, delivery methods, and empowerment come together to support each other, governance provides perspective into each. It measures the performance of the other elements and can show where more focus is needed.

Empowerment: the fourth and most critical pillar. Ultimately, developers working in a DevSecOps culture will want to be empowered to make decisions because they want to take ownership over the security of the application. Restructuring DevOps and security teams to establish efficient cooperation between them will ensure security becomes a frame of mind rather than a hindrance. Again, this takes time and trust to build through stages, each of which will be ongoing.

Stages to empower a DevSecOps team

The first of these stages will be a collaboration over conversations. This can partially be facilitated by technology, but also requires human interaction. They will raise issues face-to-face, volunteer ideas and get problems fixed by working together.

The second stage for developers involves building a learning culture around security (and vice-versa for security personnel, of course). We'll always need domain experts on particular matters in development, security and operations, but to take their collaboration to the next level, participants from each domain need to develop an active curiosity and learning attitude towards each other's areas of expertise.

They'll be able to bring up new issues, for example, that belong in their counterpart's domain, bring their own perspective and start a conversation to understand how to address issues.

The third and fourth stages are accountability and ownership. That developers feel accountable for security, and lastly that they feel ownership of the domain to as great an extent as anyone else involved.

These are advanced stages and might take considerable time to mature. So organisations cannot rush this. Since a culture change, like the DevSecOps journey, is a long-term investment, it's important that the value of initiatives can be demonstrated along the way. A DevSecOps journey should not be focused on a final outcome, but rather continuous improvement and maturation of the culture within the organisation.

Every increment in understanding and collaboration around the stack, delivery, governance and empowerment is a positive step forward in realising DevSecOps and safer applications.





Experience Pure FlashBlade Now

Test drive modern storage



A three-pronged approach to government security

The increase of ransomware attacks over recent years has cast a spotlight on the need for governments to adopt a risk-based approach to cybersecurity.

BY ADAM VINCENT, CO-FOUNDER AND CEO AT **THREATCONNECT**



SHORTLY AFTER the SolarWinds hack of the software supply chain was disclosed, The United States Cybersecurity and Infrastructure Security Agency (CISA) announced its Systemic Cyber Risk Reduction Venture.

This focused on the relationship between threat, vulnerability, and consequence – in an effort to develop actionable metrics and quantify cybersecurity risks across US critical infrastructure. Not long after this, the UK's National Cyber Security Centre (NCSC) offered guidance to security teams and IT companies on how to assess if an organisation was at risk and the actions needed to mitigate threats.

Assistant Director for the National Risk Management Centre in the US. "These technical capabilities must be coupled with robust risk-management practices – knowing your major risks, understanding the size of your attack surface, assessing the criticality of your digital infrastructure and then using this awareness to harden systems and add resilience in a targeted and prioritised manner."

The Systemic Cyber Risk Reduction Venture takes a three-pronged approach to evaluate cyber risk at a national level: building the underlying architecture for cyber risk analysis to critical

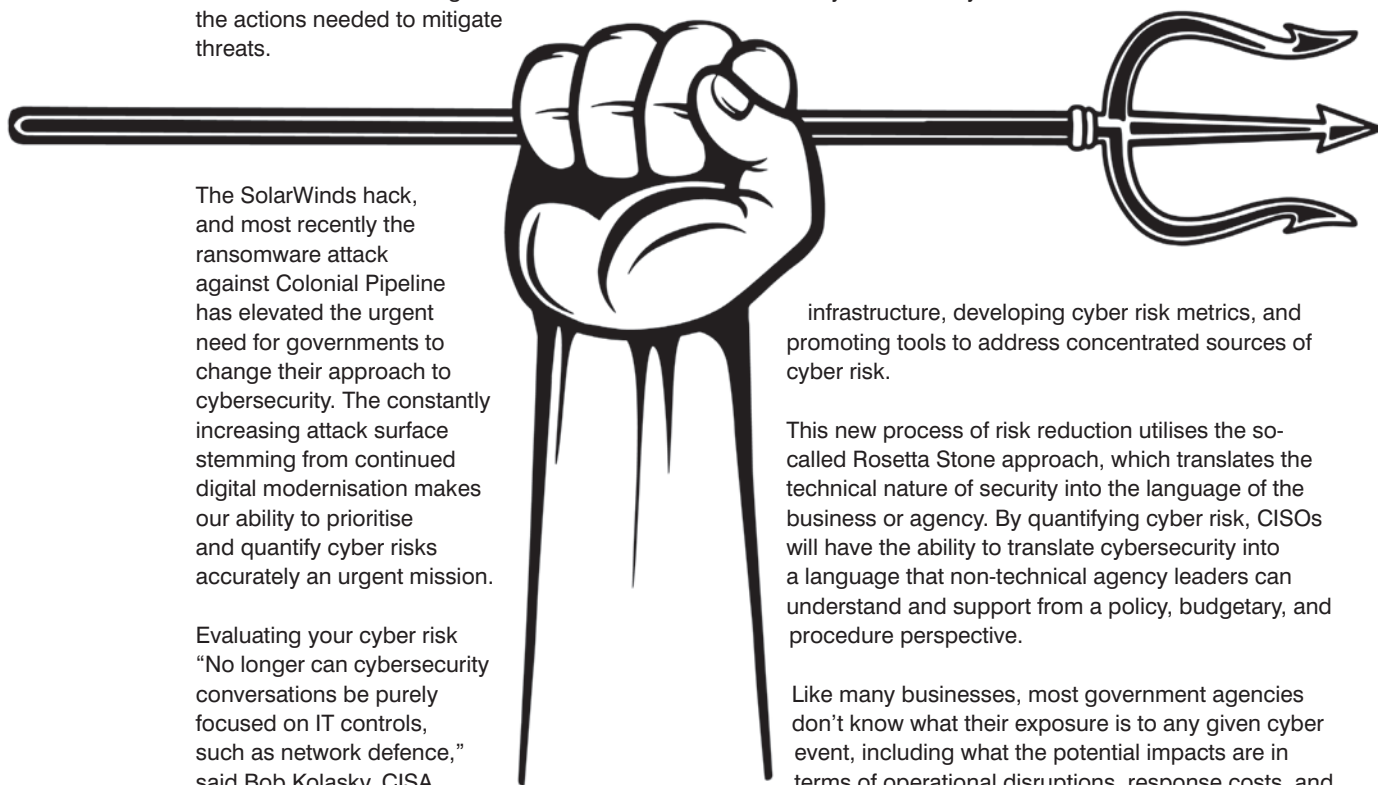
The SolarWinds hack, and most recently the ransomware attack against Colonial Pipeline has elevated the urgent need for governments to change their approach to cybersecurity. The constantly increasing attack surface stemming from continued digital modernisation makes our ability to prioritise and quantify cyber risks accurately an urgent mission.

Evaluating your cyber risk
"No longer can cybersecurity conversations be purely focused on IT controls, such as network defence," said Bob Kolasky, CISA

infrastructure, developing cyber risk metrics, and promoting tools to address concentrated sources of cyber risk.

This new process of risk reduction utilises the so-called Rosetta Stone approach, which translates the technical nature of security into the language of the business or agency. By quantifying cyber risk, CISOs will have the ability to translate cybersecurity into a language that non-technical agency leaders can understand and support from a policy, budgetary, and procedure perspective.

Like many businesses, most government agencies don't know what their exposure is to any given cyber event, including what the potential impacts are in terms of operational disruptions, response costs, and



secondary loss. This typically results in a lack of focus on the risks that matter most to the organisation.

The future is cyber risk quantification

Developing cyber risk metrics attaches a monetary value to risk. These can then be used by organisations to determine what matters most, whether the appropriate controls are in place and can estimate the potential financial loss if an attack was to be successful. The level of security investment that is necessary can then be determined to meet the organisation's risk tolerance. This acts as a starting point for private sector companies, particularly those owning or operating critical infrastructure, to improve future decision making.

Cyber risk quantification removes the risk of human error – no longer relying on human calculation – through automation and supporting it with real-time cyber threat intelligence. Attackers do not take time off, and neither does your agency and its IT infrastructure. Automation becomes a decision support system that operates in real-time opposed to being dependent on individuals waiting for lengthy interviews, training, and manual reviews.

The Systemic Cyber Risk Reduction Venture acts as a starting point for improving government and critical infrastructure cybersecurity, and the UK



should take note and further develop their policies. Government agencies must prioritise mitigation efforts and understand immediate cyber risks so that critical energy applications, functions and data are protected. The time to introduce automated cyber risk quantification, supported by real-time threat intelligence and orchestration capabilities is now.



DIGITALISATION WORLD

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

New product and process development is the foundation for the growth of the DW industry.

If you want to highlight the recent important breakthroughs that your company has made, please submit an abstract to philip.alsop@angelbc.com

It is imperative that Digitalisation World Magazine remains a timely resource for this industry, so we are especially interested in highlighting very recent work.



How is QKD combatting the increased sophistication of today's cyber-attacks?



As global economies digitalise at speed, our collective success depends on the trust of secure and reliable encryption systems,

a dependence as vast as it is easy to underestimate.

BY DR. ANDREW SHIELDS, HEAD OF QUANTUM TECHNOLOGY AT TOSHIBA EUROPE

OVER THE PAST YEAR, the digital world has come to define our everyday life, and encryption systems such as RSA public key encryption (PKE) are essential to the internet, ecommerce, and the secure transfer and storage of vast quantities of sensitive business and personal data. However, the underlying security of this infrastructure is often taken for granted.

This security is now increasingly under threat by the progressive sophistication of cybercriminals determined to steal private data for intelligence and financial gains. Alongside this, there is also the looming prospect that their operations might be further enabled by emerging technology of quantum computing. The combination of nuanced

cybercriminals, paired with the latest technological capabilities, arrives at a particularly critical time when we are observing mass home working, and the volume of data moving across networks is being accelerated by the expansion of mobile traffic, as well as Internet of Things (IoT) and machine-to-machine (M2M) communication. With this, PKE algorithms will become more vulnerable to compromise, and without secure encryption, the private communication we rely on today will start to erode, damaging digital commerce and entire economies.

The race to develop quantum safe encryption

Without a new system of encryption, data breaches and leaks of sensitive information will become more commonplace. Yet while investment into quantum computers themselves has been vast, the level of funding going into the quantum resistant technology needed to balance the quantum threat hasn't always been as forthcoming.

However, this has started to change with the mainstream arrival of quantum cryptography – implemented through Quantum Key Distribution (QKD) – which offers a route out of this quantum dilemma. Unlike conventional public key encryption, whose security depends on the inability of classical computers to solve complex mathematical problems within a practical timeframe, QKD's security is guaranteed by fundamental and unavoidable physical laws. Combined with quantum resistant algorithms, this means that QKD is not only secure from today's data tapping attacks but all future ones as well. Put simply, the method works by securely distributing encryption keys between two communicating parties, so that any attempted interception generates errors which are impossible to hide.

Multiplexing – the next milestone

But not all QKD solutions are the same, and Toshiba has created what could be seen as the tipping point in the adoption of the technology – multiplexing. Conventional QKD systems have the drawback of requiring separate fibre channels for key distribution and data, which makes them more expensive to implement using dark fibre. But with multiplexing, the quantum and classical data channels can share the same lit fibre on the O-band (quantum signal) and the C-band (data traffic) over a distance up to 70km, and with a key rate in excess of 40kb/s for 10 dB loss. Meanwhile a further development – active stabilisation technology – need also be deployed in order to automatically monitor and compensate for miniscule variations in the fibre's temperature or physical length which might otherwise introduce errors and reduce bit rates.

Making multiplexed QKD practical in unstable real-world networks has required major advances in technology, and the arrival of multiplexed QKD is certainly a ground-breaking development. At a stroke,

Without a new system of encryption, data breaches and leaks of sensitive information will become more commonplace. Yet while investment into quantum computers themselves has been vast, the level of funding going into the quantum resistant technology needed to balance the quantum threat hasn't always been as forthcoming

the technology doubles the network capacity, and halves the cost of deployment, making it commercially competitive.

In terms of real-world application, last year Toshiba and BT announced the UK's first industrial deployment of a QKD quantum-secure network in a 6km link between the National Composites Centre (NCC) and the University of Bristol Centre for Modelling & Simulation (CFMS). This demonstrates how QKD can be deployed to protect sensitive data in a way which meets the emerging security requirements of industry. Having installed Toshiba's QKD system, this can now be done over standard BT fibre optic cable at a rate of thousands of secure keys per second.

QKD isn't the sole technology designed to counter the threat of quantum computers, and another – Post-quantum cryptography (PQC) – is also touted as a viable solution. The idea behind PQC is to develop new algorithms not dependant on the vulnerable integer factorisation used by public key algorithms which could be shown to be resistant to an attack by a quantum computer. Yet standard bodies are still evaluating which of more than two dozen algorithms might be up to the job – a process which will take years, with any positive outcome far from certain. The security of QKD's underlying physics, on the other hand, is unconditional, meaning it offers unprecedented security when it comes to the detection of eavesdropping attacks. The future, though, will see room for both QKD and PQC, as each can be deployed in a complimentary way for different applications.

Ultimately QKD is a ready-now fit for the secure backbone communication used by financial services, advanced industry, and healthcare sectors, where secrecy is at a premium. And better yet, it is future-proofed to serve as an important foundation of a future quantum Internet, which will one day connect powerful quantum computers via secure QKD infrastructure.



How mass remote work has changed DDoS

It's hard to imagine a time when Internet connectivity was such an important commodity in our everyday lives. In the pre-pandemic world we relied on it, but the act of national lockdowns, global travel restrictions and quarantine orders pushed us to lean ever more heavily on that connectivity.

BY ASHLEY STEPHENSON, CTO, FOR CORERO NETWORK SECURITY



WHILE WE ARE REACHING the tentative end of the pandemic in many parts of the world - the things that were put in place over the year-and-change of tumult look like they might turn into longer term behaviours, practices and working standards.

Mass remote work is one of them. In early 2020 companies were forced to send legions of workers

home, placing them outside the safety net of office security controls and into potentially insecure home environments.

Cybercriminals easily exploited these new vulnerabilities in these already strained organisations. Phishing attempts abounded, with hackers trying to exploit the general panic of the global pandemic, as

well as the newfound separation between employer and employee. Between January and April 2020, Interpol reported 907,000 spam messages and 48,000 malicious URLs related to Covid-19. Ransomware gangs also saw their opportunity and attacks spiked in the first two weeks of April.

Given the strained state of enterprise networks, it wouldn't take too much to add the straw that would break the camel's back. Cybercriminal groups didn't miss the opportunity and DDoS boomed. Kaspersky reported that DDoS attacks doubled in the first quarter of 2020 and tripled in the second quarter. Moreover, attackers piled on the pressure with each attack. Corero data shows that there was 70 percent growth in attacks over 10 Gbps. The probability of repeat attacks increased by 68 percent with many organisations being attacked one week and then experiencing follow up attacks the next week. Attackers saw an opportunity to not just exploit this weakened state, but to leverage vulnerabilities in the very thing that was holding remote work together - the VPN.

During 2020, Corero saw a near 400 percent increase in the use of OpenVPN reflections as an attack vector - in which gangs would use the OpenVPN infrastructure of one organisation to launch DDoS attacks on another organisation. The victims of the attack would obviously suffer from the usual effect of a DDoS attack, but those whose OpenVPN infrastructures were being used as a vector also suffered from degradation in service and maybe completely unusable VPNs. Another VPN provider, Powerhouse Management, could be exploited to send amplified DDoS attacks. One anonymous security researcher discovered the vulnerability and published their research on GitHub, showing that the UDP ports of 1500 Powerhouse VPN servers were exposed, and could be used to launch DDoS attacks.

Beyond the pandemic

Remote work looks like it's here to stay. Mass remote work seems to have proved popular with both employees and employers. The giants of Silicon valley announced early on that they would install remote work so sturdily within their workforces that only a portion of workers would have to be at the office at any one time. Facebook CEO Mark Zuckerberg said last year as much as 50 percent of Facebook's employees could be working remotely in the next five to ten years. Spotify announced earlier this year that it would be moving to a "work from anywhere policy" for its 6000 employees. The most open throated vindication of remote work was made by Twitter CEO Jack Dorsey, when in 2020 he sent a letter to all Twitter employees saying that his employees would be able to work from home "forever."

But these are merely a few examples of a broader popularisation of remote work. In April 2021, staffing company Robert Half found 49 percent of all workers said they preferred a hybrid work arrangement in

which they spent a portion of their time working in the office and a portion working remotely. Over a third - 34 percent - of respondents said they might quit their jobs if they were made to return to the office full time. A 2021 Dice survey showed that among tech workers, only 17 percent viewed a full return to the office as desirable, where as 59 percent favoured a flexible or fully remote arrangement.

This kind of fundamental shift away from the known quantity of in-office security to a "work from anywhere" model, brings new risks, considerations and of course, vulnerabilities. Ransomware surged during the pandemic, and according to experts that was largely down to the sudden prevalence of remote work. Many pandemic era ransomware attacks were carried out by attacking the VPNs which employees relied on to work remotely. The breach of Japanese gaming giant Capcom was carried out in precisely this manner.

The same is true for DDoS and VPN, devices which can be easily overloaded with relatively modest attacks. This is a cheap strategy for attackers and a costly outcome for victims. When one VPN is taken down, a whole number of remote workers can lose access to important enterprise systems - thus flinging them into a spiral of downtime and lost productivity. In this new landscape DDoS threats may also find fertile ground. What makes remote work so vulnerable to DDoS is the sensitivity of its dependencies. Mass remote work requires a great deal of connectivity to ensure smooth sailing outside the workplace - and that gives DDoS gangs a new range of targets to exploit.

Remote working is bandwidth heavy and likely contributed massively to the spike in internet use during the pandemic. As such, we have never been quite as reliant on internet service providers and telecommunications. For attackers, this presents a valuable target to exploit, and potentially extract value from. If one were to paralyse remote working, then they would similarly paralyse the business and could potentially hold them to ransom.

The same is true of service providers who hold up the connectivity for hundreds if not thousands of clients. In late 2020, a DDoS gang launched a 400 gbps attack at Norwegian Telecoms provider, Telenor and demanded a 20 Bitcoin ransom to cease the attack. While Telenor did not pay the ransom, it's not hard to see how damaging an outage could have been to their customers, nor how valuable the return of service could be. The sudden introduction of mass remote work into the stable and secure networks of the pre-pandemic era is changing our expectations around IT and security. Like so many innovations, it's been created under great pressure and with such speed that few have had the time to think of the larger security implications. Meanwhile, cybercriminals and DDoS gangs are readily adapting to this new landscape and enterprises need to play catch up.

Machine Learning success starts with these 10 steps

“Machine Learning (ML) can take an organisation’s digital transformation to new heights” — It’s a statement we hear time and time again, but in practice, it doesn’t achieve that warm and fuzzy turn-key transformation feeling the statement asserts.

BY SANTIAGO GIRALDO, DIRECTOR OF PRODUCT MARKETING AT **CLOUDERA**



THE TRUTH is that the promise of ML can be difficult to attain, but it is ultimately there for the taking – for those ready to embrace a new way of thinking. While some deem ML as a pie-in-the-sky assertion that’s too good to be true, others are grabbing it by the horns and witnessing the true value it can bring to a business. In fact, according to Forbes research, the global machine learning market was valued at \$1.58B in 2017 and is expected to reach \$20.83B in 2024.

There’s no denying that in order to see the benefits of ML, businesses have to embark on a new kind of data journey – one that may seem difficult, or even uncomfortable. But once an organisation has full scale ML models in production, the benefits are endless. It can help to increase revenue, decrease costs, and even help teams work smarter and do things faster. It’s also sustainable, if a company is willing to work at it.

The thing is, ML is not always easy to implement. We often see teams running into the most issues when bridging the gap from simply dipping their toes in the ML waters to getting to grips with full scale ML production. Luckily for them, these barriers are easily overcome.

In order to achieve enterprise ML success, there are ten proven steps for an organisation to follow:

Taking a holistic approach

When it comes to embracing ML models in all their glory, leaders have to adopt the right mindset and take a holistic approach. Before it can become a driver for change, ML must first be treated as an integral part of an organisation’s data strategy and be baked in from the very beginning. By integrating ML from the start of a project and running it alongside existing IT environments, processes, applications and workflows, organisations can drive better business results. This is because the ML will be continuously learning and developing from the very beginning, ensuring they are working to the best of their ability from the get go.

Evolve the organisation to embrace ML

For businesses that have already dabbled in ML, they will have noticed that there’s a wall between experimentation and large-scale adoption. This wall is there because an organisation may lack the knowledge and skills needed to weave ML development, production and maintenance into their existing processes, workflows, architecture and culture. That’s why embracing ML requires flexibility in the structure of a company and their approaches to how they manage their data. Data scientists and engineers should work closely with leaders, to lead them on the right path when it comes to managing



data and use these insights to guide business strategy.

Building a multi-disciplined team

A crucial part of successfully implementing ML is recognising that people are just as important as the technology itself. To build a team that can support ML models in their day-to-day functions, collaboration and freedom from organisational restriction are key. A data scientist will want a platform and tools that give them practical access to data, compute resources and libraries, without feeling tied down by red tape or access barriers. Whereas leaders will want to see the ROI from adopting ML from the beginning. Bringing a team together from a range of disciplines ultimately means ML models can answer a range of organisational needs and power better business decisions.

A willingness to experiment, and fail

While there are many benefits that come with ML implementation, from automating processes to solving business issues, at its core, it's about science. Proper science takes experimentation and observation, as well as a willingness to accept the failures alongside the successes. Fortunately, when it comes to ML, even failures can be viewed as victories; once an organisation finds that a specific business problem can't be solved with ML, that knowledge frees up efforts to be focused elsewhere. Every experiment should be learned from, and these learnings should form the basis of data strategies moving forward. Iterating quickly

A common mistake for any company wanting to jump on the ML bandwagon is a rush to create an ML model that's flawless from the start. Instead, they should recognise that getting to grips with ML is a process and let teams experiment rapidly, fail early and often, continuously learn, and try new things. This way, they can ensure ML models are performing in the best way for the organisation, fuelled by the right data and insights to drive the business forward.

Choosing the right technology to optimise the data lifecycle

Another important aspect of creating ML models is having the right technology to optimise the lifecycle. Data engineering and data science teams need the ability to work across and control the entire journey an ML model goes on with a business. This lifecycle can be divided into two phases:

- 1. Holistic ML development and the building of ML models**
- 2. Getting to production, scaling and ongoing operations**

The right platform and tools will empower your teams to work seamlessly across both of these phases – to ensure ML models are built properly, are put into production at the right time and scaled with the organisation.

Maintaining integrity

Looking ahead to when an organisation has successfully deployed a few ML models at scale, they need to know that their work is far from over. This is because the underlying data driving those models shift over time, and the models need to react accordingly. Once an organisation has an effective model in place, keeping it fine-tuned takes ongoing effort to ensure it's working accurately. The aforementioned involves continuous reviews of how ML models are performing, how they are reacting to changes and the impact this will have on the future of the algorithms and the business they serve.

Closing the skills gap

When it comes to choosing the right team of people to work and support ML models, organisations should try to build a team with experience, talents, and capabilities across a wide range of skill sets. Companies should think about including everything from data engineering and data science to DevOps and product development people into these teams. That's because a range of people will bring different perspectives and knowledge levels to all the projects in hand, ensuring the best results. The more diverse the team is, the more its members can learn from one another and grow collectively.

Treating models in production like living software

While ML models must be maintained, they must also be protected. And that means having visibility into model lineage and monitoring who can access and make changes to them. Putting access restrictions in place ensures only those who need or should amend ML models are able to do so. Taking these steps will maintain their integrity and accuracy - two crucial aspects to any successful ML model.

Abiding by ethical obligations

Lastly, businesses have to take into account the ethical considerations when it comes to ML. For starters, organisations must have consent from customers and other stakeholders before applying the necessary data against an ML model. By establishing and adhering to a rigorous set of ethical ML standards early on, companies will save time and a huge headache trying to retrofit practices later down the line.

By following these ten steps, businesses can start their journey to seeing ML success. As ML spend continues to grow, organisations need to invest in their ML modes. IT and business leaders have to ensure the integrity of the models are maintained, access is only granted to those that need it and they have the right team in place to develop and grow models with the organisation. The benefits of ML are there for the taking, but only if enterprises are willing to commit to the process. Implementing ML can seem like a daunting task, but by following these ten steps, it doesn't have to be.



Five practical ways contact centres can use AI to create value

Consumer expectations in relation to ultra-fast interactions, ease of engagement and service quality have grown exponentially, fuelled by the lockdown experience of the past year.

BY MARTIN TAYLOR, CO-FOUNDER AND DEPUTY CEO AT **CONTENT GURU**



MORE ADEPT and confident at using a multitude of digital and online channels, today's consumers want quicker resolutions and frictionless journeys across every channel they use to communicate with companies. Little wonder that 80% of customer engagement professionals in a recent webinar said transforming how they engage with customers directly equates to competitive advantage.

In 2020, contact centres had to pivot at speed to cope with the operational realities created by COVID-19. Alongside adopting agile cloud-powered platforms, many contact centres also turned to AI to maximise their capabilities and address customer issues faster. In the same recent webinar, 30% of customer engagement professionals said they intend to roll-out additional AI technology deployments to transform how they model and predict call volumes, enable new automated self-service channels and evolve the role of

personnel based in their contact centre teams. With AI spending set to reach \$110 billion by 2024, indications are that AI is revamping the contact centre and, in the process, helping to redefine the customer experience itself.

Delivering on the promise

Since it first gained traction in the early 2000s, there's little doubt that AI has been a much-hyped technology that business and IT leaders have found difficult to apply to real-world problems in a value-add way. However, advancements like machine learning and natural language processing (NLP) have put powerful new AI capabilities into the hands of contact centres. This is making it possible to improve customer service and the customer experience through automated interactions, while capturing data insights that make it easier to respond faster and more accurately to evolving customer demands.

Today's chatbots can detect words, recognise a caller's mood and respond accordingly, address easily resolved enquiries, and serve up the information human agents need to handle more complex customer challenges with ease.

Let's take a look at some practical applications of AI in the contact centre today, together with the business value these generate:

1. Redefining the customer experience: automating the triage experience

Today's mobile-device wielding consumers find IVR systems frustrating and time consuming to navigate; make one mistake when selecting from a pre-defined menu and it can take hours to get to the answers you want.

Modern chatbots offer an automated first port of call for customers. Within seconds of speaking their question, they can be channelled to the right agent or offered the option of receiving a text or email link that provides the answers they need – whether that's an update on a delivery, a link to reset a password or schedule a service visit or call.

Using NLP-powered chatbots, contact centres can serve up self-service options that will provide a 'first-time-fix' for between 20% to 40% of callers, who'll benefit from a fast and optimised response to their routine queries.

By integrating reactive AI call deflection and intelligent queuing into their operations, contact centres are able to manage high call volumes effectively without scaling up manpower resources or compromising on customer service.

2. Spotting trends and tailoring services to improve the customer experience

Replacing IVRs with AI-powered chatbots that greet every caller with an open ended 'how can I help you today' question also opens the door to capturing rich insights that shed light on why customers are calling, the challenges they're facing right now, the actions they need to take, and how they ask for help.

Using these insights, contact centres can quickly re-engineer workflows to enhance how they respond to customers. Whether that's re-allocating resources, streamlining routing and escalation paths, or customising the customer experience (CX).

3. Delivering personalised interactions

In today's CX battleground, organisations are having to go beyond the basic product/transaction focus demand of the past. Today's AI technologies can help transform customer satisfaction by pulling data from multiple sources, including details like local weather and previous purchasing behaviour, to offer products and services in real-time that match their specific needs and personal preferences. And, according to

Accenture, up to 91% of consumers are more likely to shop with a brand that tailors their service to provide relevant offers and recommendations.

AI can also boost how contact centres look after high priority premium-status or vulnerable customers by ensuring they always go to the top of the customer service queue and are instantly fast-tracked to specialist live agents.

4. Responding to customer demands 24/7

When customers can't quickly get a resolution to their query, they start shopping around. So much so that 75 percent of customers build brand loyalty if they receive a fast response to their queries. However, in today's hyper competitive environment, expectations for near-constant customer service is growing.

AI can help contact centres address this challenge in an efficient and cost-effective way. Assigning virtual agents can automate the handling of a select sub-set of typical customer use cases to deliver automated out-of-hours services, with options to schedule responses for more complex issues that will require the intervention of an expert human agent.

5. Boosting employee motivation

Call centres have a reputation for high turnover rates which add up to significant costs for the business. AI technologies and chatbots can help reduce the strain on customer service teams in a variety of ways. Today's AI technologies can do much more than just eliminate the huge volume of repetitive basic information request calls or automate many of the mind-numbing data entry tasks and manual processes that typically demotivate contact centre employees.

Serving up all the important contextual information that relates to a customer and their issues, AI helps agents be more effective from the get-go with no need to repeatedly ask a customer to explain what they're trying to accomplish. Plus, today's AI applications are capable of providing insights in the current state of mind of the caller, together with recommended actions and options that will support the agent to resolve complex customer problems.

Looking to the future

Today's contact centres are taking advantage of AI to optimise agent performance, deliver enhanced and more personalised services to customers, and uncover insights that will enable them to stay one step ahead of evolving market and consumer demands.

As the contact centre of the past evolves into the engagement hub of the future, AI will underpin how organisations personalise every customer interaction. It will also become increasingly key to enabling organisations to not just anticipate a customer's needs – but also identify if they are becoming dissatisfied and the best actions to take proactively to win back their loyalty.



The UK's cornerstone Smart Buildings Show returns for its largest event to-date, as the free-to-attend conference and exhibition takes place at ExCeL London on 6-7 October 2021. With more exhibitors and content than ever before.

SMART BUILDINGS SHOW, the UK's cornerstone commercial smart buildings event, has announced its 2021 event has now opened for registration. The free-to-attend conference and exhibition takes place at ExCeL London on 6-7 October 2021, featuring industry-leading speaker sessions and panel debates from some of the sector's most renowned brands, including Microsoft, Bluetooth and Siemens Building Products.

This year's conference will cover a diverse range of subjects and deliver thought leadership, education and key insights into the issues affecting today's smart buildings professional, including building automation systems, facilities management, lighting and control systems, energy efficiency and energy management, software, security and smart metering.

The conference sessions will be spread across four dedicated theatres, including;

- **Connected** - Management which will look at how smart building are managed and how the workplace has changed post-covid
- **Connected** - Control which will look at physical devices in smart buildings
- **Connected** - Spaces & Infrastructure which will focus on smart buildings, wellbeing, networks, connectivity and power
- **Training** - which will offer visitors the chance to enhance their industry credentials via CPD-accredited presentations.

"We are delighted to welcome visitors back to Smart Buildings Show conference and exhibition," said Ian Garmeson, Managing Director, Turret Group.

"This year's show will provide visitors with the first in-person event to focus on smart buildings and their associated critical infrastructure since the start of the pandemic. We believe it will provide a fantastic opportunity to network among fellow industry peers and demonstrate how our sector will play a key role in helping the UK to build back better."

Throughout the two days, Smart Buildings Show 2021 will cover key aspects of creating and managing a smart building including; security, services and support, building energy management and health & safety - allowing delegates to;

- **Learn** from the industries most renowned thought leaders and innovative vendors
- **Gain** insights into the key aspects of creating and managing an intelligent smart building, including building automation systems, artificial intelligence (AI), energy efficiency and lighting and controls.
- **Network** among leading brands to become part of the latest thinking, sharing experiences with other organisations

The conference will host all the latest information on the smart buildings market and will include a number of panel discussions that promise to be the centre of some lively debate.

Mark Tyson, Head of Property Operations at Legal & General Investment Management Real Assets, will be hosting a panel entitled, 'Is there a trade-off between healthy buildings and net zero carbon buildings?' featuring Simon Wyatt, Partner at Cundall. This panel debate will take place on Wednesday 6 October at 1pm.

On Thursday 7 October at 10:45am, join Adrian Scott, Business Development Manager at Priva UK Ltd for his session, 'Local and remote management of healthier buildings with Building Automation Control Systems', as he discusses the proposed requirements for providing a healthy and clean future workspace in the post Covid-19 world.

The full speaker line up, including Microsoft, Verdantix, Arcadis and Quuppa – to name a few, is available on the show website. This year's Headline Sponsor, Bluetooth SIG, is joined by Platinum Sponsors; aico/HomeLink, The DALI Alliance, Sauter Automation and Schneider Electric.

To register for your free ticket, visit smartbuildingsshow.com to unlock all the information you need to make your buildings more economic and functional.

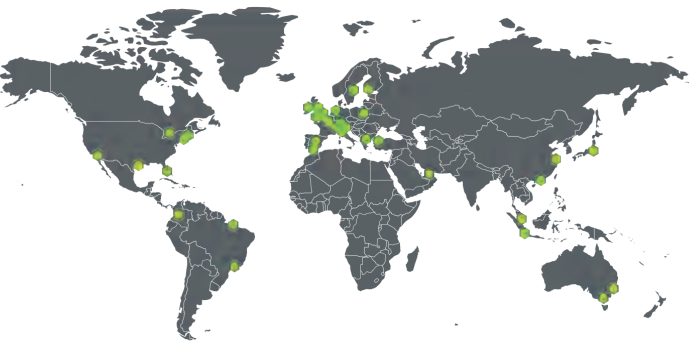
For more information on exhibiting and sponsorship, please contact Claire Hatchett at c.hatchett@turretgroup.com. Keep up with Smart Buildings Show at @smart_build on Twitter and #SBS2021 across all platforms.



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.



What are the Properties of a Blockchain Network?

Blockchains, in general, have three properties:

Traceability - Traceability

is the ability to know where something came from (Provenance) and know where it ended up (Destination). This is a useful property for tracking where money came from, and what it was eventually used for. This is also useful for determining the origin of items.

Immutability - Immutability

means that whatever happens on the blockchain, stays on the blockchain. This is a very useful property for providing trust within a system. If the data cannot be changed, then we have an easier time believing that what the network said happened, actually did happen, and no third party has tampered with the data.

Transparency - Transparency

is provided by several factors. The source code of most blockchains are open source, and can be audited by anyone wishing to understand the network. With respect to Bitcoin, all transactions can be viewed by the public, which increases the ability to audit and trust the activity on the network. These factors contribute to the transparency of the network.

Internet vs. Blockchain

The invention of the internet is a common comparison to the way blockchain and cryptocurrency is entering the mainstream. After the internet was established, anyone from around the world had access to information. The ability to publicize your voice became possible, followed by the ability to keep current with the times. The internet essentially decentralized information, creating somewhere we can easily trade, transfer, and share information.

Blockchain vs Bitcoin: Everything you need to know

If you know anything about Bitcoin, there's a good chance you've also heard about its underlying technology: Blockchain. Blockchain is the technology behind cryptocurrencies like Bitcoin, enabling peer-to-peer digital cash systems where users are in complete control of their account balances and transactions. In this article, we'll explain what blockchain is, how it works, and why it's required to make cryptocurrencies like Bitcoin possible.

BY MRUGAKSHEE PALWE, **CRYPTO VANTAGE**



What the internet did to information, blockchain is doing to money. Various blockchains are creating the internet of money, a global financial ecosystem that allows us to trade, transfer, and share value in a decentralized way. Just like pre-internet, we relied on centralized sources for our information. We currently rely on centralized entities dubbed as banks to provide our financial infrastructure. Blockchain is changing this paradigm at a staggering rate.

No Bitcoin Without Blockchain

Bitcoin was invented on October 31, 2008, and launched January 3, 2009. The attempt to figure out how to securely link together transactions goes back as far as 1997 with foundations rooted in “HashCash”, a pre-bitcoin phenomenon. Without the founders of Bitcoin figuring out how to create a tamper-proof chain of transactions, Bitcoin would not be possible.

So how does it all work?

The Bitcoin blockchain is a series of individual blocks that contain transactions taking place on the network. Computers around the world maintain the same copy of each individual block. These computers form the Bitcoin Network, and maintain the security and authenticity of the blockchain.

The transactions that take place on the network are put into blocks, and linked together cryptographically, and thus the blockchain has been an obvious choice of words to describe the underlying technology to Bitcoin and other cryptocurrencies.

Blockchain cuts out the Middleman

In the original whitepaper where Satoshi Nakamoto introduced Bitcoin, he detailed a “peer-to-peer electronic cash system”. Peer-to-peer means that there is no need for a third party to authenticate transactions on the network.

Cash transactions are a peer-to-peer payment system. There is no third party required to facilitate the transaction between you and a merchant for a purchase or transfer when using cash. The property of cutting out the middleman in online transactions has the potential to disrupt many industries. For example, from making supply chains more efficient to making global financial transactions faster and cheaper.

The Difference Between Blockchain, Cryptocurrency

Cryptocurrency is an application of blockchain. Just like the internet serves many applications (like websites), there is a wide range of cryptocurrencies, each with their own unique purpose serving as applications on their own blockchain. Blockchain is the underlying infrastructure that makes cryptocurrency possible.

Another point worth noting is that not all blockchains have an associated cryptocurrency. While cryptocurrency is the first application of blockchain,

Bitcoin was invented on October 31, 2008, and launched January 3, 2009. The attempt to figure out how to securely link together transactions goes back as far as 1997 with foundations rooted in “HashCash”, a pre-bitcoin phenomenon. Without the founders of Bitcoin figuring out how to create a tamper-proof chain of transactions, Bitcoin would not be possible

industry professionals have found ways to apply the technology in a variety of ways that don't require a cryptocurrency to be tied to the blockchain.

The Many Uses of Blockchain

A new industry is emerging in the technical corners of the planet. In finance, blockchain has many use cases including tokenization, cross border transactions, and censorship-resistant payments.

In other industries, blockchain can be used to form agreements in business relationships to reduce disputes and ambiguity between partners. Smart contracts, which are self-executing coded contracts, have enabled new forms of digital agreements. This becomes very useful as it digitizes the contract and automates its execution.

Applications that are built on top of blockchains are called decentralized applications, or dApps for short. dApps are applications that exist on decentralized networks such as Ethereum. Ethereum can be thought of as an application or token platform, with the capability of hosting dApps. Your dApplication can leverage aspects of blockchain such as the durability of decentralized networks, or the censorship resistance of cryptocurrency, simply by deploying your





idea on top of an existing blockchain. You don't need to worry about the underlying computer infrastructure, as this is provided to you by willing participants all over the world.

Can Blockchain Fail?

Blockchains are just software built by humans, and humans can make mistakes. That being said, the Bitcoin blockchain has been active for more than a decade, without a single successful hack performed on the network. The developers of Bitcoin have decided to make trade-offs with the software, opting for more security and trust, instead of an efficient network that can process a global load of transactions.

Many hacks have taken place on blockchain networks in the last decade. Hackers either exploit the code directly, or gain control of the network through the governance mechanisms. For example, in order to hack the Bitcoin network through governance, you would need to control 51% of the network. This task has been deemed impossible, as the Bitcoin network is so widely distributed that it is nearly impossible to amass that much computational power. However, other blockchain networks are smaller, and thus, much more vulnerable to a 51% attack.

The Difference Between Public and Private Blockchains?

Blockchains can be examined in a number of ways. One of those ways is by looking at who has access to the network. The Bitcoin network, for example, is completely open to anyone and everyone to use, without bias. The Bitcoin network applies no preferential treatment to you based on social status, or geographic location. It is for these reasons that Bitcoin is considered a public network.

A private network is more suited for use cases that require permission for accessing and utilizing the network. A private network is better suited for

enterprise purposes, such as supply chains, and closed financial systems.

What Are the Downsides of Blockchain Technology

The downsides of blockchain need to be talked about in the context of what that particular blockchain is trying to solve. If the blockchain is aiming to be a global payments system, that blockchain needs to be primed to scale to meet demand, while maintaining security for its users. This is a hotly debated topic, but it all boils down to how blockchains are implemented and governed. If we look at Bitcoin, for example, the blockchain uses more electricity than the country of Ireland in a single year to process no more than seven transactions per second. Contrast this to VISA, which processes 65k transactions per second, and Bitcoin doesn't quite meet the standards.

What's worse is that adding more computers to the Bitcoin network doesn't solve the scalability problem. As more computers are added to the network, the network gets stronger security, but remains to process only seven transactions per second. Since the inception of Bitcoin, developers have created new blockchains that are more scalable, but are arguably less secure than the security that the bitcoin network provides.

Why Blockchain and Bitcoin are such a Big Deal

In today's digital age, efficiency and privacy are more important than ever before. The sophistication and level of security surrounding blockchain and Bitcoin is remarkable, providing everyday people more power, control and convenience when it comes to managing their money.

Whether digital money takes over our traditional paper money that is stored in physical banks is yet to be seen, but one thing is for certain: the complex world of Bitcoin and blockchain is on the rise, with absolutely no signs of slowing down.



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



How blockchain and AI are helping the current COVID-19 vaccine rollout

As promising as the current COVID-19 vaccines are in the fight against the pandemic, the biggest challenge is still how to distribute these vaccines all across the globe.

BY MOHAN NAIDU, MANAGING DIRECTOR, [FPT UK](#)



THE GLOBAL SUPPLY CHAIN is inherently complex due to the large number of intermediaries involved, making rapid shipments and deliveries at scale difficult to achieve. The answer, however, may lie in Artificial Intelligence (AI) in tandem with blockchain technology. Blockchain is no longer limited to financial services but has already been applied in industries such as logistics and retail, where it allows real-time shipment tracking and shared access to data. The lessons learned can be utilised to create a global ledger for COVID-19 vaccine distribution - which is currently susceptible to a major logistical problem.

Several pharmaceutical firms globally have developed and launched COVID-19 vaccines with impressive

efficacy rates of up to 95% – and in many countries, the rollout is in full swing. But as promising as these vaccines might be, the biggest challenge is still present: a reliable and efficient solution to distributing these vaccines globally and rapidly. According to the World Economic Forum, it would take 7 to 19 billion vaccine doses distributed worldwide to eradicate the pandemic.

Over the last few years, AI has moved from the realm of science fiction to a tangible technology that dramatically reshapes the healthcare sector. The constant mutating of diseases and viruses presents a great challenge for healthcare providers. But with the help of AI, the diagnosis and treatment processes

would be significantly accelerated. AI has been statistically proven to be more accurate in detecting diseases from medical imaging and therefore reckoned a viable source of diagnostic information for clinicians. However, healthcare facilities need to be aware that technologies such as ML and NLP still require some degree of human oversight.

Keeping a tab on storage fridges

One difficulty is that each vaccine must be stored and distributed under specific conditions, inducing logistical hurdles that can affect these vials' safe and rapid roll-out. Together with IoT-based sensors, blockchain can be applied to fulfil such a daunting task. In fact, two British hospitals have already leveraged digital ledger technology to keep tabs on the storage and supply of these temperature-sensitive vaccines. The two hospitals in Stratford-upon-Avon and Warwick use blockchain technology to monitor the storage fridges and improve record-keeping and data sharing across NHS supply chains. Once the vaccine batch data has been collected on a device, the technology can verify that it hasn't subsequently been altered or tampered with, greatly reducing the risk of errors that comes with manual tracking.

Prioritising the most vulnerable patients

With vaccine demand outstripping supplies, governments worldwide were rushing to determine who should be the first to receive the jabs. While the common approach of prioritising the elderly and frontline healthcare professionals seems reasonable, it ignores a range of risk factors that can drive a higher chance of mortality in COVID-19 patients. Ethnicity, sex, race, and age could all be crucial variables when it comes to the risk of suffering severe COVID-19. But how to decide who should get the potentially life-saving shots first?

Machine learning might be one answer to this dilemma. It could be used to leverage an enormous amount of data on any patients' health history, existing conditions, social and environmental factors, then correlate these with current local infection rates to detect hidden patterns. In South Dakota, the United States, healthcare delivery system Sanford Health use a machine learning model to spot those with the greatest risk of suffering from severe COVID-19 outcomes. AI provided an evolving, real-time picture of which patients got the sickest with COVID-19. Elsewhere, Vietnam's Government relied on AI algorithms to automatically calculate the probability of infections based on their updated records of confirmed cases, their travel history, as well as highly infectious areas.

Blockchain solutions in Pandemic Time

Measuring the spread of the virus With applied decentralized ledger technology, blockchain encourages us to interact with what is happening in real life faster. The information is compiled and synchronized from disparate sources, countries with



high transparency. Medical organizations can do research more effectively, thereby making precise and valuable predictions for the future to deal with diseases like CVOID or pneumonia.

In today's complex healthcare system, our information is in different medical centres with various medical records, which might lead to different diagnostic results or some fraud and abuse cases in health insurance. This usually caused by two main reasons: Medical centres want to keep medical records for their internal purpose, or they can even provide this information to their partners for commercial purposes. The patients sometimes don't share all their pathological information since they have low trust in that medical centre; they are too shy, or they forget their disease histories.

Raising community trust and awareness As patients now have full control of their medical data, they get their rights to decide how their data is shared and used for what purposes. Besides, people can easily update new information through one trusted source of synthetics. All related researches will have to ask for the right to approach the necessary information. Supporting medical supply system Blockchain technology plays a huge role in medical care based on different advantages: Reliable information allows us to calculate precisely the number of medical supplies or trained medical staff needed to prepare for a manufacturing plan. Detect and prevent counterfeit drug manufacture: Closely monitor input materials and the manufacturing process to ensure the genuine. Build platforms to track donations of medical supplies or other forms from all around the world and deliver them to the right people.

Wrapping Up

The globe has reached a critical juncture in technology evolution in which the right tools are available – and they are crucial weapons in the fight against the pandemic. Still, there is more that needs to be done. A mass vaccination effort requires global coordination and cooperation in streamlining the COVID-19 vaccine supply chain and not least, in driving all relevant stakeholders towards a consensus to embrace such a system.



Don't wait for blockchain, it's more accessible than you think

When blockchain first hit the tech scene about 12 years ago, it was mostly recognised as the technology enabling Bitcoin transactions. Since then, it's taken a while for blockchain to establish itself in the business world, but today we're seeing more enterprises take advantage of it to help build trust and loyalty with their customers and business partners; improve business efficiencies; and boost supply chain transparency.

BY ADELA WIENER - CEO, **AURACHAIN**



WHILE THERE ARE numerous benefits that come with blockchain there are still many CEOs scratching their heads as they try to make sense of what it can really do for their businesses. Here, we explore why it's important; how this transformative technology will change how we conduct any exchange of value with each other in the future; and how the technology is more accessible than you might think.

Blockchains allow for the immutable (unchangeable) record of data and the automatic execution of digital agreements known as smart contracts. Blockchain

applications are becoming increasingly important to help businesses share accurate information quickly, securely, and transparently, stored on ledgers that can only be accessed with permission. Helping to track transactions such as orders, payments and much more, it optimises record keeping, holding information safe from fraud or vulnerabilities and eradicates the need for third party validations.

Where can blockchain bring value?

Blockchain can bring many benefits across numerous industry sectors. For instance, in supply chain, helping

organisations to verify the source of their products and track their movements from factory to warehouse, and onwards, by offering a digital space where all data is held securely. Another supply chain application is the detection of contaminated or counterfeit products. Blockchain applications help to build trust with customers by offering proof that the goods they have purchased are exactly as advertised. In certain industries such as food and automotive, where transparency is important to comply with standards or to meet regulations, the use of blockchain is growing exponentially.

In financial services, blockchain is already providing numerous operational advantages and areas of service differentiation. Applications are being rolled out across the world for hybrid trade finance activities, internal finance functions such as recording payables and receivables transactions, payments, settlements and more. Across each of these areas, blockchain provides numerous advantages, including improved financial control, reduction of risk, heightened transparency, and auditability. More so, it can deliver cost savings by streamlining processes and removing the need to pay third parties to oversee or approve an agreement or transaction. And it also significantly reduces the risk of fraud due to the immutable nature of the information it controls.

Building trust

It is blockchain's ability to deliver accurate and timely data stored as a confidential record, only shared with people within the network, that makes it such an attractive proposition to any business that transacts with its customers digitally. As businesses look to automation to optimise and accelerate many of their other day-to-day processes, they can also optimise customer service processes and take the pain out of disagreements by automating their contracts with blockchain.

Blockchain applications can be integrated with customer data and CRM systems as part of secure processes. Doing so significantly enhances the process of creating customer documents such as legal contracts. Instead of having to rekey data stored on the CRM, the blockchain application allows the business to auto-populate using the data from the CRM platform. Not only does this streamline the process but it removes the risk of human error. Blockchain applications also allow users to easily build rules and set criteria, determining what information is required in different situations - for example, removing an auto-renewal provision from a contract at a certain price threshold. By adding this rule in a blockchain application, businesses remove the need to manually change the provision on the CRM platform. This again removes the risk of error and therefore strengthens the customer relationship. On the subject of customer data, businesses face an ongoing challenge of managing customer data securely, with the pressures of data protection

compliance always in mind. This risk that can be significantly mitigated through blockchain applications. In fact, this is the most important feature of blockchain technology as it enables businesses to create verifiable and secure CRM records. This is especially useful for businesses that source customer data from variety of sources. This includes anything from internal data, online information or subscription databases. With blockchain, all records are encrypted, making them almost impossible to hack. And because each record is linked to the one before and after, hackers would have to alter each individual record in the chain.

The low-code approach allows non-technical users to develop blockchain applications without the need to write complex code

Looking to the future

In the not-too-distant future, we predict that blockchain applications will become increasingly valuable to a variety of sectors including financial services, government, insurance and logistics. They will be an efficient alternative to disputing contracts with lawyers or other bureaucratic systems – saving time and eliminating the financial burden that often accompanies contract disputes.

With so many efficiencies, and trust and transparency benefits on offer, why aren't all businesses using blockchain applications already? As CEOs and their teams start to realise the advantages of blockchain, their biggest hurdle will be finding a team of skilled developers to build a blockchain platform. Tech talent is in high demand right now and these skills can be difficult to come by. However, there is an alternative solution, and one which makes blockchain far more accessible, and that's through low-code. The low-code approach allows non-technical users to develop blockchain applications without the need to write complex code. Of course, expert programmers, cryptographers and computer scientists are still required to create the base upon which blockchain applications can be built. Once this is in place blockchain applications can be successfully developed using low-code platforms.

Thanks to the availability of low-code platforms incorporating blockchain, we believe blockchain will become far more accessible to many more enterprises. It's potential across so many sectors is undeniable, and rather than continue to question what's in it for the business, we anticipate CEOs asking instead, when they can start to reap the benefits.



How to navigate intellectual property risk in blockchain projects

It's been well over a decade since blockchain technology first burst onto the scene. And although that initial use case was supporting the public ledger of pioneering digital currency Bitcoin, the intervening years have seen countless new innovations.

BY CHRISTOPHER SMITH, SENIOR ASSOCIATE AT REDDIE & GROSE LLP, PATENT & TRADE MARK ATTORNEYS



TODAY, blockchain has gone well beyond cryptocurrency to serve as a vehicle for creating trust and driving collaboration between disparate parties. It's used in everything from anti-money laundering tracking to IoT monitoring, and international money transfers to supply chain monitoring.

Yet as tech firms and financial service organisations stake more of their reputation and money on blockchain projects, it pays to acknowledge the intellectual property (IP) implications. Depending on the project, firms may need to understand the nuances of open-source licensing, and take steps to mitigate the legal risks associated with copyright infringement.

More patents, more risk?

The sheer volume of new patent applications filed each year illustrates just how popular blockchain has become. A study from consultancy KISS Patent claims that more blockchain-related patents were published

in the first half of 2020 than in all of 2019, and that 2019 saw three times more blockchain patents published than in 2018. Interestingly it is Fortune 500 companies that appear most active in this space, rather than blockchain-centric start-ups. Alibaba and IBM were the top two publishers as of September 2020, with the Chinese tech giant filing 10 times more patents in the US than Big Blue.

However, filing for a patent doesn't mean it will be granted. This can create uncertainty for companies looking to steer their own innovations clear of potential legal risk – whether for the patent applicant who does not know if their innovation will be protected or for the third party who does not know if a competitor's patent will actually be granted. And the more patent applications there are, the more possible risk. A second element of unpredictability is that the sheer volume of blockchain patent applications being filed means not all have been published. That means if your company wants to bring a blockchain-based

product or service to market now, you'd have to launch "at risk". There may be a patent pending which you technically infringe, but if information about it hasn't been published in the public domain, it's impossible to know.

The good news is that a lot of this uncertainty will certainly dissipate as the technology matures and blockchain implementations become more standardised and interoperable. Already some standards-setting organisations such as the Institute of Electrical and Electronics Engineers (IEEE) have published standards including Framework of Blockchain-based Internet of Things Data Management and Standard for General Process of Cryptocurrency Payment.

More will surely follow. When this happens and essential patents can be determined, it's likely that patent licensing pools will follow. These enable patent rights to be aggregated among multiple holders and made available to licensees for a fee. Even where some elements of blockchain technology aren't standardised, the most important patents will likely be licensed on fair, reasonable and non-discriminatory (FRAND) terms, representing a voluntary licensing commitment that standards organisations often request from the owner of an IP right (such as a patent) that is, or may become, essential to practice a technical standard.

These developments will reduce risk for companies that want to incorporate blockchain tech into their products and services, although royalty payments to patent holders will likely be necessary. The challenges of using open source.

Another risk relates to the use of open-source code. As in other areas of software development, companies are increasingly turning to third-party components as a low-cost way of accelerating time-to-market and competing with larger, better funded rivals. Open-source licences describe what can and can't be done with this code, although whether a breach of terms constitutes copyright infringement or breach of contract may depend on the jurisdiction you operate in.

There are two main categories: permissive and restrictive. As the name suggests, permissive licences, such as the MIT licence Bitcoin has adopted, do not place any restrictions on software reuse—even for commercial purposes. Modifications of the code don't even need to be distributed under the same licence, or at all. On the other hand, while restrictive licences such as the GPL 3.0 allow for free distribution of copies of the software, they also require that any modified versions of the code be licensed under the same terms.

This may cause problems for blockchain companies whose business model relies on selling licences to a



product that incorporates this code. Unless they're able to separate open source from proprietary code, the whole product could be considered a modification of the open-source code and therefore must be made freely available. If, however, the business model is offering services on top of a blockchain or offering blockchain-as-a-service, then using open-source code with restrictive licences may be less high-risk. That's because the underlying software is not considered to be distributed.

What happens next?

When it comes to open source, using permissive licenses is usually the lower risk option, even in the latter scenarios outlined above. However, when it comes to the uncertainty created by mounting volumes of patent application filings, there are a couple of proactive steps that organisations could take.

The first is to file your own patent applications based on in-house innovation. That would put you in a strong position to benefit from cross-licensing or contributions to patent pools as the technology matures. A second, cheaper option, is defensive disclosures describing specific techniques and uses of technology. These provide "prior art" protection against patent applications filed later, ensuring the latter will be rendered invalid.

The bottom line is blockchain is here to stay. If your organisation wants to use the technology to drive business growth and reach new customers, it's increasingly essential to understand the implications of IP law. It may save a lot of time and potential legal cost down the road.

Business as usual?

Why the aviation industry cannot revert to its pre-pandemic ways



After a summer of chaotic scenes in airports and ever-changing travel restrictions, many in the aviation sector are longing for business to return to 'normal' and hankering for the pre-pandemic days. Returning to its old ways, however, is the worst thing that the industry could do.

BY CEO AND CO-FOUNDER AT **AIRPORTR**

THE PAST 18 MONTHS, although extremely challenging, have given rise to a stronger and more resilient industry, one which is at long last futureproofing itself and embracing digital transformation. At a time where airline and airport resources are stretched and consumer confidence in travel is low, now is the time for the industry to double down on that transformation rather than reverting to historic processes and operations.

In choosing a path of digitalisation and innovation, the industry has a prime opportunity to improve its sustainability credentials and make long-term improvements to the passenger experience. If there was ever a time to improve and transform the industry, it's now.



Accelerating innovation and digitisation

In the wake of the industry's worst financial year, the aviation ecosystem has been tasked with how to restart operations with increased agility, depleted resources, and significantly less revenue. One need only look at the reports coming out of the UK's airports

in recent months to realise that a systemic change is needed within the sector for it to find its feet again. Covid-19 outbreaks within the UK Border Force, influxes of passengers following updates to the traffic light system, and last-minute schedule changes are just some of the recent issues that airlines and airports have had to contend with.

The benefits of innovation and digitisation are clear, but the industry has been notoriously slow to adopt new technologies. Focusing instead on cosmetic improvements such as wider seats, catering, and in-flight entertainment, the sector has arguably been too short-sighted in its approach to improving passenger experience. Whilst the appetite to digitise and innovate may have been there, it had been stunted and delayed by the mammoth task of addressing legacy infrastructure and regulations.

Fast-forward to 2021 and digitisation is no longer an exciting project to one-day explore, but rather a critical process to fully embrace. The quandary that many airlines are finding themselves in was made all

the more apparent when Monika Wiederhold, global lead for safe travel at Amadeus, explained that “The current need to hand-verify health documents while maintaining social distance means that some of our airline customers need around 90% of their check-in staff to process just 30% of passengers”. Operating at this level is simply not viable long-term.

These issues have accelerated the uptake of digital technologies and fast-tracked innovation across the industry. As summarised by the IATA in its post-Covid-19 vision for travel, there is a “...need for a flexible approach and resilience. In turn, this brings an urgency to put available technology to use, to provide this flexibility and unlock the full benefits which are achieved with global coordination rather than isolated approaches.”

This acceleration of digital innovation has manifested itself across the whole aviation industry ecosystem. Up until 18 months ago, the use of biometrics in airports, for example, was in its infancy but with the need to digitally verify identities tied to test results or health passports, and contactless methods now critical to inhibiting the transmission of Covid, biometric technology has gone mainstream.

What airlines and airports are understanding, too, is that these short-term solutions have long-term benefits to the passenger experience. The recent biometrics trial at Istanbul Airport, which was initially introduced to encourage passengers to touch as few surfaces as possible on their journey throughout the airport, also led to a 30% reduction in passenger boarding times.

Improving the passenger experience in terminals has been at the forefront of digital initiatives like the pre-ordering of products and services in airports without needing to queue or enter the retailer. Airlines, like those within the Lufthansa Group, have launched self-service baggage tracers, allowing passengers to file a missing bag report in moments by submitting their flight, baggage and passenger details a handful of steps using their smartphone.

Airlines are having to invest more in conversational and self-service technology, to enable them to talk to passengers in a human-like way but with automation. This requirement has been driven by the unprecedented scale of disruption and subsequent interactions they have had to manage with their customers. Additionally, they have had to introduce more automated workflows around recovery – for example when there are cancellations or disruption. Communication in real-time, issuance of vouchers and refunds to customers is now more instantaneous. This has changed the passenger experience for the good. No longer do you simply get a text from the airline to say your flight is cancelled, with no reasoning, and then have to spend hours on the phone to get a refund processed.

A sustainable future is within our reach



What is exciting about this digital revolution in the air transport industry, is that there is still so much more to be explored, however it is happening at a real pace. Concepts which once seemed futuristic and unattainable are now becoming a reality. By making technology the bedrock of operations, airlines, airports, and the various organisations that make up the ecosystem, are unlocking a world of opportunity.

For instance, several airports are planning infrastructure for the future whereby terminals have significantly less check-in points and baggage processing. To enable this streamlined vision of the future airport, we can expect to see more and more airports working towards off-site, advanced processing. Effectively this would enable airports to reduce their real estate and contribute to net zero strategies.

The off-site processing of bags will also help mitigate the emissions associated with air travel. One of the industry's most stringent, tangible, and immediate sustainability targets is to change the way passengers get to the airport, by encouraging public transport usage. This involves changing consumer behaviour and building trust in the reliable alternatives to make it achievable. For instance, most major UK airports are introducing vehicle drop-off fees to deter vehicle usage, however as long as passengers are laden with baggage, the use of public transport will only ever go so far. By leveraging technology, airlines and airports can process passengers separately from their baggage, allowing them to travel light to the airport and seamlessly through the terminals.

Digital technologies are therefore serving not only to make the passenger experience positive and Covid-safe in the short-term but also laying the foundations for the industry to streamline operations, stay agile, and meet its sustainability targets. The reopening of international travel may have had its teething problems, but the future certainly looks bright for air transport.



How data is changing the way hotels streamline operations



The hospitality and travel industry has undeniably been one of the hardest hit by the pandemic. The sector has had to completely re-evaluate the way it delivers its

services to comply with constantly changing rules and government regulations, and to guarantee the safety and loyalty of both its guests and employees.

**JOE BEAUMONT, HEAD OF HOSPITALITY AT
EXPONENTIAL-E**

LEISURE FIRMS ACROSS THE WORLD have turned to technology to radically overhaul their existing processes, giving way to a huge opportunity – leveraging data. The industry has adopted technologies such as IoT to help inform strategic operatives. And the availability of and access to data collected during digital interactions presents firms with the ability to completely transform how they run, manage and improve their offerings, including providing guests with a seamless and personalised experience.

It's all well and good to talk about the potential impact of data, but what does best practice look like in the sector? And how can it help revive hotels big and small around the world?

Data management, the crucial first step

Reputation is arguably one of the most important factors in hospitality. It safeguards customer loyalty and attracts new clientele. And in recent years,

reputation is no longer limited to how clean a hotel room is but expands to how safe guests' data can be. Data breaches have severe consequences for hotels, with Marriott Hotels being fined £18.4 for a data breach that hit millions of their guests. Guests' data is now considered the most valuable asset to a hotel and protecting it is of paramount importance.

From managing databases and servers, and ensuring compliance and security, data management can prove to be time-consuming and challenging, especially for large global hotel chains. It is, however, a strategic imperative. This is especially true when taking into consideration that many hospitality firms have had to cut their staffing levels by half during the pandemic, often resulting reduced number of employees able available to monitor certain aspects of IT operations, such as cybersecurity. By bringing in third-party cyber security expertise, this can often ensure peace of mind as a service, and help leverage and enhance data management strategies, especially when regarding security and compliance.

Creating a digital journey for guests

In the hospitality industry, first impressions are everything. So, guaranteeing a stress-free arrival and booking process for hotel guests has always been front of mind, which is why many hotels have moved to digital-first check-in processes via phones or through downloadable apps. In doing so they've gained the ability to email guests with all the information they need ahead of their trip, and offer them the chance to amend their booking details to align with their preferences, such as their room type, dietary requirements, or arrival needs. This is where the compliant and safe data collection begins to boost the customer experience.

Once guests have safely checked-in, hotels will be able to use these applications to ensure and maintain high-quality service for the duration of the guest's stay. For example, guests will be able to automatically log-in to the hotel Wi-Fi, book restaurants as if liaising directly with the concierge, control the temperature and television in their room, or simply contact reception staff, housekeeping or leisure facilities via instant messaging for other queries. All the guests preferences can be kept for future bookings and reference, for example a room could be set to the preferred temperature prior to the guests arrival. In addition, staff would be able to send personalised messages or offers to guests during their stay, or provide real-time assistance with aspects such as directions to the pool.

How IoT is making holidaying even easier

Alongside these kinds of applications, IoT sensors are already being implemented throughout resorts or hotels to improve guest experiences. However, the benefits span beyond this. Hotels and other hospitality facilities will be able to easily locate equipment such

as luggage racks and cleaning carts via asset-tracking technology. Maintenance staff will also benefit from the ability to review performance data collected by specific devices located around a property, and troubleshoot any repairs required should conditions drop below appropriate levels. When implemented alongside 5G, IoT devices may even support hotel restaurants in improving food tracking and waste disposal. In time, these technologies will make it easier for those working in the leisure industry to improve the quality of guests' stays, track the delivery of services and gather feedback, just as they would pre-COVID, all while removing all physical touchpoints and complying with government health and safety regulations.

The future of data-driven hotels

The real beauty of these digital approaches for hotels is that they will allow them to extend their engagement to guests well beyond the end of their stay. Management teams' requests for feedback from guests will be far more streamlined via modernised applications, and combining this data with information gathered during their stay will help paint a clear picture of the quality of experience guests are receiving.

The most compelling benefit for businesses, however, is likely to come from the technology's direct impact on the bottom-line. The data collected from these technologies, from applications to IoT sensors, can play a vital role in helping management to reduce energy costs and guide sensible planning resourcing decisions, including when it comes to capacity and personnel. When New York's Chatwal Hotel upgraded to a smart lighting system throughout the hotel for example, it reduced its lighting energy consumption by 90%. With these advancements, it's clear that the introduction of data management in response to the pandemic may actually enhance the experience hotels can deliver on significantly. Providing them with a powerful tool for transforming one-off guests into loyal, dedicated customers, boosting both reputation and future revenue will ensure the hospitality industry, like many others, enjoys the benefits of the digital age.



Delivering deep-link analysis

How you can harness the power of graph analytics to achieve a 360 customer view without rebuilding the entire IT system.

BY MARTIN DARLING, VP EMEA, **TIGERGRAPH**



ACHIEVING a 360-degree view of their customer base is the dream for many companies wishing to boost sales, drive operational efficiency and ultimately attract more customers. However, they often find it difficult to ask complex questions about the business because their data is trapped in siloed, legacy relational databases that lack the flexibility and power to perform deep link analysis.

Graph databases solve this fundamental data link problem and introduce a powerful new computational capability – graph analytics. Relational databases struggle with deep-link analysis because of the very nature of the way data is organised in lists. In list format, drawing a link between one record in one table and another record in another table involves a table join, but relational databases become increasingly inefficient as the number of table joins rises above three or four, especially if the tables are large and the number of queries is high.

Graph databases can connect data in multiple relational databases and organise it into a set of vertices representing business objects such as a

customer, payment or order connected by edges that represent the relationships such as this order was placed by this customer. This ability to map the data into pre-connected business entities without disturbing the original datasets effectively turns it into an analytical layer, sitting above the original data. What's more, it can maintain query performance even as it grows to billions of edges and vertices because, unlike a relational database, it doesn't have to load entire tables into memory to perform a query. Only the data that is required for the query need be loaded as it 'hops' from one node to another, so queries of 10 hops or more are no problem for a graph database. In-query processing adds another dimension to graph analytics, enabling queries to be constructed in such a way that it is not necessary to hop in and out of the database to complete a function.

This is a fundamental shift in the way we think about data storage, and it enables the use of a host of computing techniques or algorithms which are incredibly powerful in graph but virtually impossible within a traditional relational database.

Mapping your data

There is nothing inherently wrong with relational databases for many business applications. Developed in the 1970s and 80s, relational databases are well suited for the storage and retrieval of data and simple records management. However, to achieve a 360 customer view across multiple databases and unearth new business intelligence, you need to be able to ask questions about the relationships among different pots of data which involves bringing together disparate data held across marketing, sales, accounting, customer service and other business functions.

Organisations are harnessing graph analytics to create a digital map of their customer data while leaving existing databases undisturbed. The result is a 360 customer view across accounting, sales, customer service, marketing and other domains – but it doesn't end there. Businesses are using graph analytics to:

1. Boost the conversion rate for digital channels



2. Identify new customer segments to target for future growth
3. Reduce the cost of acquiring new customers
4. Shorten the time of the buying journey
5. Access new customer segments

Connect datasets and pipelines

A distributed graph database enables you to connect internal and external datasets and pipelines to extract invaluable business intelligence in real time, as demonstrated by Xandr, the advertising and analytics division of AT&T's WarnerMedia. It works across 15 WarnerMedia channels including Cinemax, CNN, HBO, and TNT, each holding data on millions of customers. The challenge for Xandr was creating a unified picture of all of these customer databases to deliver a seamless experience across the portfolio for both viewers and advertisers.

They created Community, an advertising platform which would be able to disambiguate user data from multiple platforms. The goal was to create unified entities across the multiplicity of data sources and deliver a joined-up advertising experience – even as viewers jumped between their personal devices (mobile, tablet, laptop) and across channels. To achieve this, Xandr built the first and largest identity graph of its kind in the advertising industry using a graph database that scales horizontally to accommodate more than five billion vertices (business entities such as users, devices and identifiers) and seven billion edges (relationships among entities) and ingests a billion updates per day. Graph analytic capabilities, such as entity resolution and centrality algorithms, stitch together identities across the separate databases to create a view of households and devices that is both unified and granular.

Now Xandr not only knows how many times an ad has been seen on a particular device, it can tell how many times that ad has been seen across all the viewer's devices – and target advertising accordingly. And the result is clear: Xandr wins advertisers from the competition by offering higher quality data and more precise targeting.

Target customers with personalised real-time email
In online retailing, product recommendation is a never-ending battle for accuracy and timeliness. Studies show that businesses can attract customers by doing a better job of recommendation than their competitors. Yet, despite this, 74% of marketing leaders report they struggle to deliver customer recommendations to all their customers all the time. It's not surprising then that Gartner says companies are actively looking for new solutions for this perennial problem.

Kickdynamic found the solution in graph databases. It's an email marketing platform that helps more than 200 leading brands boost customer engagement and sales, and it chose to build its recommendation engine on graph rather than a relational database

because of the superior ability to pull CRM data from multiple sources, connect sequences of 10 or more datapoints to extract meaningful business intelligence and deliver all of this at scale and at speed.

The ability to process queries in real time allows it to deliver live pricing based on customer preferences and product availability, capture key 'business moments' and deliver targeted recommendations – before the customer disappears. This resulted in increased engagement, brand loyalty and sales conversions – all thanks to graph analytics streamlining the process of building recommendation emails. "Kickdynamic knows that compelling, individualized experiences are the most effective way to create customer loyalty and drive revenue" confirms Gabriele Corti, Chief Product Officer at Kickdynamic.

In-database machine learning for fraud detection
Retail businesses everywhere struggle with fraud, but financial services company NewDay has found a way to automate a lot of its anti-fraud measures with the help of graph analytics. It has achieved a big jump in detections and prosecutions, turning the tables on criminals by identifying fraud at all stages in the credit card lifecycle including application fraud (trying to obtain credit cards with stolen personal information), transactional fraud and first-party fraud (fraud by existing customers).

With revenues of nearly £1 billion per year, five million consumers and an operation spanning the largest online retailers and best-known credit cards, as well as access to third-party fraud prevention and identity checking databases, NewDay had no shortage of data on which to draw. However, bringing all of this information together in a meaningful way was a time-consuming manual process that required fraud investigators to jump in and out of internal and external databases.

Using graph analytics, NewDay created a system that brought together myriad databases, both internal and external, empowering fraud investigators to speed up the analysis of complex frauds. In addition, sophisticated algorithms enable it to analyse more than 10 million transactions per month and identify suspicious cases while minimising false positives. Consequently, anti-fraud at NewDay is more intelligence-driven, allowing it to block cards and issue new ones more quickly and refer a greater number of cases to the police.

NewDay says that their graph-based system is still in its infancy but has already yielded a 10-15% uplift in the number of fraud cases being detected which the head of fraud prevention, Danny Clark, says is only the beginning.

With graph analytics, organisations can achieve a top-down view of customer data, generating new insights to grow and develop the business.

AI and Automation

Is your business ready for hyperautomation?

As businesses gain through improved ROI, investment in hyperautomation is expected to increase to achieve operational excellence and resilience.

BY BALAKRISHNA D R, SENIOR VICE PRESIDENT, SERVICE OFFERING HEAD - ECS, AI AND AUTOMATION, **INFOSYS**



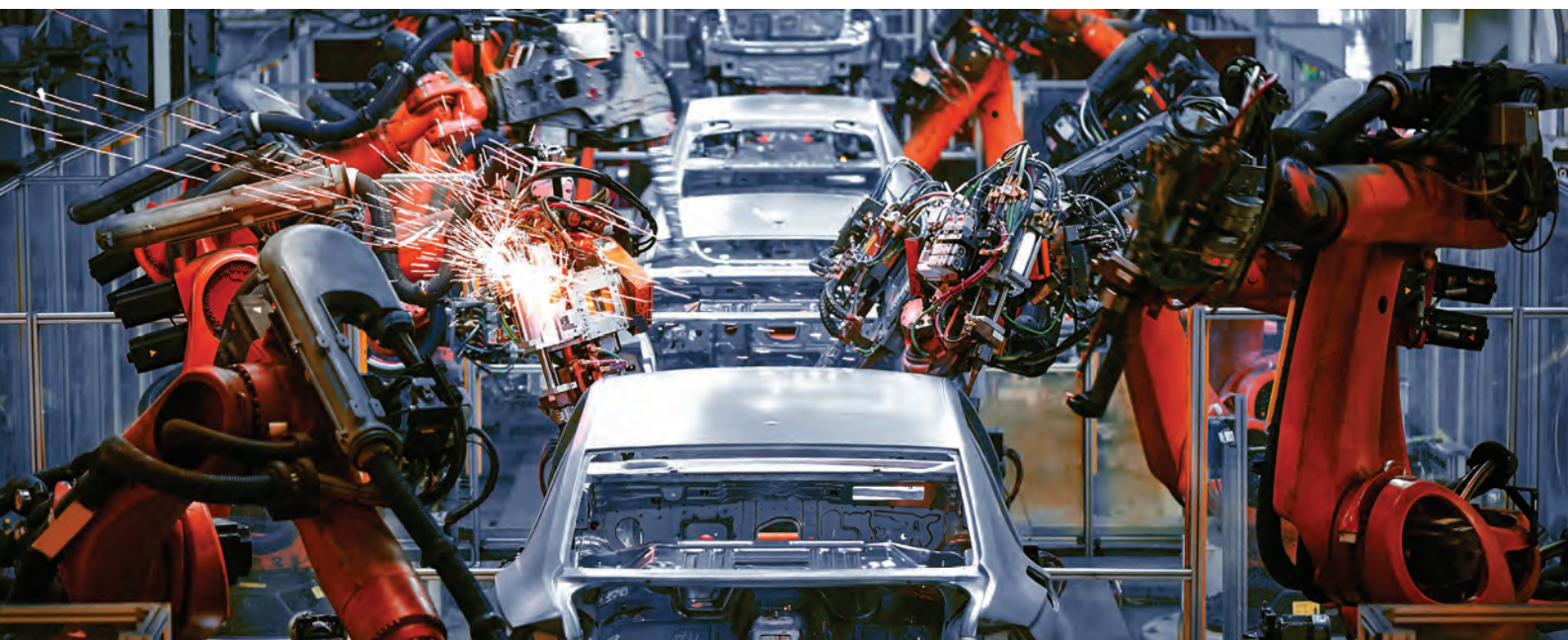
AUTOMATION has found a place in businesses since the beginning of industrialization. Enterprise automation tools have made efficient routine business processes such as accounts payables and order management. Even industry-specific processes like claims management in insurance or loan underwriting in banks today require little human intervention with the help of Robotic Process Automation (RPA). While automation software has traditionally focused on the 'doing' aspect of processes, modern-day automation includes the infusion of AI with RPA resulting in intelligent automation that also augments the human ability to 'think'. Can we extend the value of automation even further?

Hyperautomation is an expansion of automation using sophisticated-AI based automation tools and

software and an ecosystem of platforms and systems that extends automation to every business process in an organization that can possibly be automated. It promises to automate complex operational decision-making. To reap the full benefits of hyperautomation, organisations need to invest in sophisticated technologies and build access to the large amounts of data required to drive automation on a large scale. Are they ready to do that?

Roadblocks to achieving hyperautomation

The road to effective hyperautomation is filled with challenges. Lack of vision can lead to investments in solutions that either do not scale up or integrate well with other tools, resulting in automation occurring in siloes. The automation landscape offers multiple



solutions, and enterprise architects are often left debating on the capabilities they need to invest in. Sometimes, the shelf-life of a solution and vendor stability are overlooked, impacting both support and enhancements required to keep pace with changing needs.

Lack of guidance or know-how to assimilate RPA with other tools is a common hindrance, particularly when employees do not have the necessary skills. Cultural resistance to automation due to fear of job loss is a difficult hurdle to overcome. The AI maturity of all the players in the entire automation chain needs to be the same to maximize benefits. Lastly, unstructured data and security concerns can derail the hyperautomation journey.

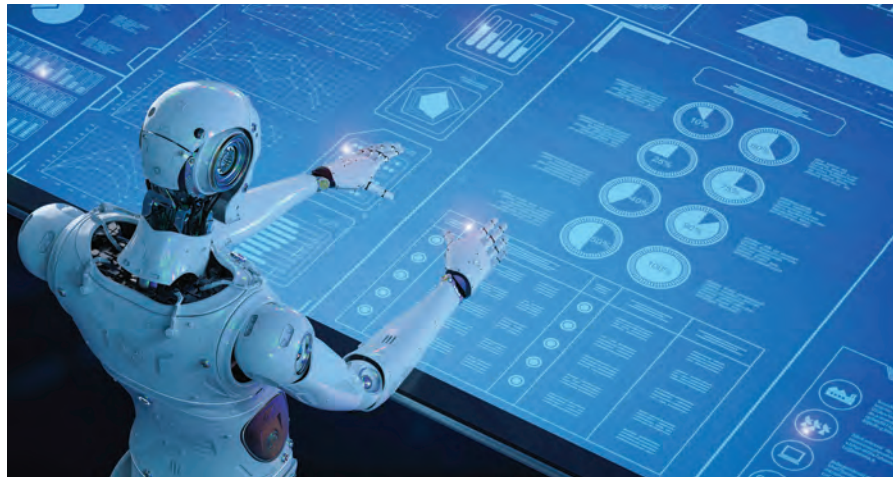
How can organizations ready themselves for hyperautomation?

Enterprises may invest in the most complex AI-based automation solutions, but unless they align to the long-term strategic roadmap to hyperautomation, they will fail to deliver the desired value. Technology innovation leaders should plan for end-to-end automation that is well-aligned to the overall business goals. The roadmap must include complementary technologies that are can be both scaled and well-integrated.

The first step to hyperautomation is to assess the AI maturity of an organization. Based on the maturity, a long-term strategy must be designed to ensure technology-buying decision-making is streamlined to optimize the following key elements – revenue, costs, risks, and quality. The next step is to assess the different technology markets and create an investment plan to effectively deliver tactical and strategic business values.

Is the investment adding to the revenue? Will it enhance processes, increase customer engagement, or introduce new services – are some questions that enterprises must ask themselves. The choice of automation tools must contribute to optimizing costs by reducing errors or expediting and redesigning processes for efficiency.

Every automation must consider the risk of non-compliance with regulatory requirements. Adding AI to the automation mix brings legal, ethical, and compliance responsibilities that need to be taken care of. To ensure trust and prepare for future regulations, organizations should take steps to ensure that AI



implementation is explainable. Automation success will depend on selecting the appropriate data for each use case and ensuring its quality. A strong use case strategy driven by business needs and not as much by technology can set the tone for success early in the hyperautomation journey.

Creating a powerful integration strategy is vital as it allows systems to be managed centrally and communicated throughout the organisation. Enterprises must assimilate and orchestrate the different platforms, tools, and software that it uses for hyperautomation. Digital Operations tools that align closely to the automation roadmap must be selected. All AI applications must be integrated with digital operations tools to augment business processes and deliver long-term business value.

None of the steps taken will lead to success unless an effective change management strategy is devised to counter employees' fears of being made redundant with hyperautomation. Employees must be allowed to upskill and reskill to take on high-order thinking jobs, as the mundane is taken over by hyperautomation. Businesses need to focus on recruiting the right talent and invest in continually up-skilling them.

Conclusion

Post-pandemic, hyperautomation has picked up pace across industries to improve productivity and capacity, to meet fluctuating demands, and improve the quality of services and products delivered to customers and enhance customer experience. As businesses gain through improved ROI, investment in hyperautomation is expected to increase to achieve operational excellence and resilience.

The first step to hyperautomation is to assess the AI maturity of an organization. Based on the maturity, a long-term strategy must be designed to ensure technology-buying decision-making is streamlined to optimize the following key elements – revenue, costs, risks, and quality

HYPERAUTOMATION:

Enabling the next digital age

Hyperautomation is proving to be a serious consideration when it comes to transformative business technology.

BY IOURI PROKHOROV, CEO AT **INTELASTEL**



THE Covid-19 pandemic has forced organisations to change the way they work, driving the rapid uptake of new tech within businesses. Abrupt changes in working practices meant technologies that facilitated complete flexibility, especially for remote connection and collaboration, were catapulted into the forefront as businesses faced ever-changing circumstances.

With adaptable, remote infrastructure now rushed into place, most of the 2021 trends forecast by the research giants were those building on its uncapped potential. One example that could have the biggest impact on digital transformation and the broader virtual landscape is what Gartner dubs as 'hyperautomation'.

Simply speaking, hyperautomation takes the notion of automation, in which a manual process is replaced by a computer or machine, and broadens its application by stringing multiple processes into one complex flow.

According to Gartner, hyperautomation will be worth almost £430 billion by 2022 and has the potential to lower IT operational costs by 30% by 2025. So, it's understandable that it is seen as one of Gartner's top tech trends for 2021 and beyond.

Out with the old, in with the new

While task automation is not a new concept, the arrival of new tools, such as artificial intelligence (AI), machine learning (ML), robotic process automation (RPA) and low code application development platforms, drives a real step-change in its potential. In automation's present form, teams can identify a repetitive task and design a workflow to replicate the job automatically. However, this fragmented approach is too inefficient to be scalable, with workflows typically designed individually and distinctly.

Hyperautomation takes automation to the next level by considering whole business processes and automating entire workflows end-to-end. While hyperautomation was previously hindered by the complexity of analysis required for even the most basic human tasks, advances in ML and computer-aided decision-making now means the need for continual human input for some tasks is increasingly reduced. This holistic approach can automate entire job functions, in most cases improving upon the efficacy, efficiency and accuracy of the human user. In addition, in this integrated approach the entire process is confined to a single dashboard, making it easier for the IT department to manage.

For example, one use case would be in software





development. By adding the application of AI to low code and no code application development platforms like Intelastel, you can create software that aids and augments the application building process and automates trickier composition tasks, as well as flagging and helping fix any new issues, acting as an on-board advisor. This in turn will negate the need for businesses to source software developers every time they need a minor fix or new application.

Imagine solutions that use AI to continuously learn from your and others' usage, to then offer recommendations as to how system improvements can be made based on your work processes. The aim is to reduce complexity and maximise time to value through guided and straightforward system configuration. Intelastel, the no code application development platform, is on a path to deliver this capability.

Workforce reskilling

Automation of laborious and repetitive tasks is something the world's workforce will celebrate. The pandemic has provided a strong incentive for CEOs to invest in automation, as companies come under pressure to implement social distancing, reduce office numbers, and minimise physical contact. To ring in these changes, 'automation architects' will become highly sought after by companies. While 20% of companies with hyperautomation requirements currently employ an information architect, Gartner expects this to reach 90% by 2025.

Business leaders not only have to convince employees that hyperautomation technologies are advantageous to the business but must now begin to retrain or upskill their teams in readiness and ensure that implementation is carried out ethically and in a way that is right for customers and employees. As new automation technologies take over certain menial tasks, there will be an emphasis on process skills like active listening and critical thinking, as well

as cognitive abilities, like creativity and collaborative problem-solving. This marks a move away from traditional technology user training towards using tech in a way that augments and adapts to their current roles.

Reports by Deloitte have found that one in four (23%) of workers have seen a change in ways of working because of the implementation of automation technology, while one in 10 have already had to retrain because their role has been affected.

Culture reboot

According to the same Deloitte report, many business leaders have yet to consider how their employees' roles will be impacted by automation technologies, and the potential need to retrain and reskill their workforces - meaning many could be caught off guard.

Successful hyperautomation isn't just about new tech, it's about readiness among people. Equipping teams with new skills will enable new technologies to be integrated into businesses more effectively. It will also support in changing workers' perceptions of automation technologies as a potential threat to their career, into a vital asset that supports their day-to-day work and truly takes us into the next digital age.

Offering such diverse potential, hyperautomation is proving to be a serious consideration when it comes to transformative business technology. Organisations pursuing these advances must now embark on their own hyperautomation strategy. That starts with considering the most viable use cases for automation and the data and documents involved in those processes, and assigning the right team to manage it including subject matter experts, process owners and IT specialists. Finally, businesses require a comprehensive, birds-eye plan for implementation that accounts for the requirements of the entire process and the project's end goal.

How is the cloud encouraging hyperautomation, and why should I care?

Every business needs to be thinking in hyperautomation terms and investing tools such as DPCs - or risk being left behind.

**BY ALASDAIR HODGE, PRINCIPAL ENGINEER AND SOLUTIONS ARCHITECT,
CLOUDSOFT**



DIGITAL TRANSFORMATION initiatives have naturally encouraged organisations to consume infrastructure resources through APIs (Application Programming Interface) which can save costs, increase productivity and encourage innovation. There is still, of course, a need for traditional paper-based sources in the chain, but by and large IT infrastructure can now be provisioned through an API, which is great news for businesses looking to drive scale and enables what we now know as hyperautomation.

Defining hyperautomation

Although it is a relatively new term, hyperautomation is defined by Gartner as being "an approach that enables organisations to rapidly identify, vet and automate as many processes as possible using technology, such as robotic

process automation (RPA), low-code application platforms (LCAP), artificial intelligence (AI) and virtual assistants". In recent years it has shifted from an option to a condition for survival and, according to the latest forecast by the analyst firm, the global market for technology that enables hyperautomation will reach \$596.6 billion in 2022.

So, what's really behind this trend?

The blend of



hyperautomation and the cloud allows engineers to be more creative and start to build tools to automate wider processes. The public cloud has taken this to the next level, meaning that we are now seeing not only virtual disks, machines and networks being provisioned through APIs, but we are now also able to accelerate complex work – such as virtual big data analysis – as well as performing repetitive yet intuitive tasks like reading invoices, sales reports, contracts and official documents through digital twins. Organisations have been quick to notice the increased agility hyperautomation affords them to drive innovation and bring new products to the market. Meanwhile, the speed and efficiency of the people who have built the tools that make it easier to consume APIs is a key driver behind hyperautomation.

Partnering with hyper cloud specialists

Historically, many big organisations (think banks and insurers) would view IT infrastructure as so crucial to their day-to-day operations that having their own data centre was a necessity to provide them with competitive edge. Those days are long gone, and now most leading providers see the opposite is true: their IT infrastructure is so critical to their day-to-day operations that they must outsource their data centre to drive other benefits across their organisation. This includes the cloud.

This approach is nothing new and logic behind this is undeniable – why should an organisation waste valuable time, creativity and resource employing a team of talented engineers to babysit operating systems and install patches when they could partner with a specialist, freeing up time to drive innovation and improve business processes?

Enter hyper cloud providers. By partnering with a company like AWS (Amazon Web Services), Microsoft Azure or Google Cloud Platform, not only does an organisation have access to leading APIs, but the scale at which they operate is truly global. This provides organisations with even greater opportunity to consume IT infrastructure in different ways, as well as letting businesses tap into the likes of AWS's network to deploy their resources anywhere in the world and reach a global audience for a fraction of the cost.

Security and Resilience

The next concern for businesses is usually the security of their data. There is a common misconception that moving to the public cloud – and the associated move towards hyperautomation – means losing control. To a degree, an organisation will cede a small amount of control, but this sacrifice in favour of the public cloud brings with it huge convenience as well as big gains. Not only does an organisation have full control over where it geographically stores its data – think GDPR – but crucially it can still maintain it in a highly available way by using resilient mechanisms that exist across hyper cloud platforms.

The denial-of-service protection that hyper cloud providers offer, for example, are the best mitigation against threats due to the huge economies of scale they can support. One only needs to look at the many different cyber-attacks in recent years to see how critical this is to a business's reputation and bottom line, so it's easy to see why the public cloud is so attractive to organisations and how this, in turn, drives the march towards hyperautomation.

Using DPCs to coordinate the information orchestra In the wake of the Lloyds TSB IT disaster in 2018, where 1.9 million customers were locked out of their bank accounts for a week, banks and other high-profile institutions moved quickly to shore up their systems. Previously, resilience in the banking world

was focused on ensuring the organisation had enough capital to deal with any fines. However, the TSB fiasco showed the world that the operational resilience of a firm depends on the uptime of the IT system and how critical this is to remain functional.

Of course, large organisations' IT estates have evolved via a hybrid model, with increasing complexity, interconnectedness and interdependence. With such complex architectures to oversee, and the need for RTOs (recovery time objectives) of a few seconds, we must recognise that technologies will fail; it is one of the fundamental flaws of distributed systems. More than ever, what is needed is for workloads and applications to be continually managed. But how can organisations do this effectively?

We work with a large, multinational bank that deals with sensitive information on a daily basis and has a complex network of systems supporting functions such as underwriting or fraud. Because banks and other large financial institutions are taking trading positions, often running into billions of dollars, they must have real time insight into how much risk the bank is exposed to. If any one of these systems goes down for any length of time, then the company is not able to operate – resulting not only in reputational damage, but potentially also regulatory fines.

In line with the ITIL 4 principle of “automate where possible”, the automation of failure detection and recovery is a must. This can only be achieved by tooling that can operate across both on-premises and external environments, managing your hybrid estate and enabling the (hyper)automation of workloads ‘at the right time, using the right technology, in the right location, for the right price’.

Gartner recently announced a new product category that meets this need – the Digital Platform Conductor (DPC) tool. DPCs go beyond solving the resilience problem; they are a solution to the complexity crisis many large organisations are facing. Our tool, AMP, has been deployed across a series of verticals, including banking and defence, and is a crucial tool for dealing with automation at scale – or hyperautomation – and for bringing the public cloud-like benefits of such automation to the entirety of the IT estate.

In today's social media -fuelled news cycles, businesses can't afford for everyday failures to bring down their IT systems. The risks are too great and a firm's system must be available as much as possible because its operational resiliency depends on it and hyperautomation, driven by the automation benefits of public cloud, is the answer. To adapt one of my favourite quotes; “software hasn't just eaten the world, it devoured it and has come back for seconds”. That's why every business needs to be thinking in hyperautomation terms and investing in tools such as DPCs - or risk being left behind.



Providing reliable, long term SaaS services: **The importance of scalability**

A key factor for the success of many companies is creating a business model with the opportunity for significant growth. This is particularly true for SaaS businesses; the market as a whole has seen exponential growth in the last few years and is expected to reach a value of approximately \$220.21 billion as soon as 2022.

BY TERRY STORRAR, MD, [LEASEWEB UK](#)



ALTHOUGH THE EVENTS OF LAST YEAR have not been easy on any industry, SaaS spend, driven by the dramatic increase in remote working, has experienced a strong 12 months. In fact, last April, Microsoft CEO, Satya Nadella, was cited saying his company has seen, “two years’ worth of digital transformation in two months.”

However, there is always the possibility that rapid expansion such as this will bring with it some growing pains. The nature of a booming industry lends itself to accumulating intense competition.

However, with this, companies must be careful to ensure that their infrastructure allows for the

nesseated growth; the last thing a business wants is for success to be hindered by an inability to grow with the demands of customers.

For a lot of SaaS companies working with infrastructure partners, there are numerous factors that can increase a company's ability to grow and handle increasing demands. There are several factors which can help SaaS scale with their customers, most notably the implementation of flexible SLAs, providing the right technology in the right places and offering suitable support which will effectively meet the needs of their customers.

Offering a Variety of Options - Tiered SLAs

Service Level Agreements are an essential building block for any modern cloud-centred businesses. However, SLAs are far from standardised and can differ greatly depending on what SaaS providers are willing to offer. SaaS businesses are well advised to carefully study the terms of each SLA they are offered by infrastructure partners, because growth brings with it changing priorities. What might have been an ideal set of terms at one stage in the development of a business may no longer be fit for purpose once infrastructure requirements expand.

For example, it's useful to have the option of different SLA tiers that are specifically designed to meet their customer's changing needs as they grow. This could provide additional assistance for business critical functions and guarantee faster response times, priority technical help or advanced support that delivers round the clock technical expertise, enabling SaaS businesses to pass on these capabilities to their customer base.

Better SLA tiers can also focus on infrastructure performance to ensure that the latency and uptime of key services, ranging from servers, cloud and colocation to network and hosting can be tiered as needs dictate.

Providing the Right Tech in the Right Places

For SaaS-focused infrastructure providers, it can be hugely beneficial to put in the time and energy to understand the current and future needs of their client, both in terms of business and technology. Not only does this ensure they can offer appropriate technologies based on need, but they can understand more specifically where this infrastructure needs to be located and what the probability will be that demand will grow in the future. This can be hugely important to organisations selling SaaS products, who ideally, don't want to be making frequent changes to their infrastructure strategy or partners.

The challenge is, growth can come quickly and companies need to act fast if they are to embrace new opportunities for success. It's not unprecedented, for

example, for organisations in the media and gaming sectors to require dozens or even hundreds of new servers in various international markets in order to accommodate demand for a new title. Being in a position to specify the scale and location of these infrastructure assets can make a significant difference to service performance, reliability and the overall customer experience.

Being Flexible and Adaptable to Changing Needs

A critical focus for SaaS providers is their support functions. 'Must haves' should include 24/7 support availability, minimum-to-no downtime and maximum flexibility. Every SaaS business has unique needs, priorities and customer requirements, and infrastructure support should be geared to enable growth, not hinder it.

The importance of support has become even more apparent during the past 12 months, as organisations have relied on their SaaS providers more than ever. As services have been scaled to meet increasing demand, everyone in the 'end user - SaaS provider - infrastructure provider' ecosystem has been reminded about the importance of getting effective help when it's needed.

Those in the SaaS business have seen the industry boom in recent years. However, as the market grows and diversifies customers will continue to expect more from their cloud provider and success will be measured by who can meet these expectations. Being flexible, scalable and able to keep up with changing demands of customers is not only the key to cultivating successful, long-term relationships with customers, but is hugely important for the overall success of any SaaS company.



DCA Data Centre: Data Centre Design Concepts

BY DCA CEO STEVE HONE



THE DCA are taking a break from the features related to Special Interest Groups during the summer, to focus this month on various aspects of Data Centre Design and construction. This month articles range from design of Edge DC's to design of DC lighting systems.

The DCA are currently considering introducing a new group that will focus on the challenges facing data centre construction both for investors and those organisations tasked with delivering the service. This will be reliant on the level of interest we receive to setup this working group so please contact The DCA if this would be of interest to you (contact details are below).

The purpose of the group is yet to be fully defined, but its broad objectives will focus on removing barriers, identifying best practice, and increasing consumer awareness.

Although this is not an exhaustive list, the scope of this group could include key areas such as:

- Carbon assessments and embedded carbon energy reuse
- Sustainability and technology reuse
- Development planning and risk assessment
- Design Management
- Prefabrication
- Standardisation
- Speed of Construction/delivery and removal of barriers
- Essential utility supplies water, power, comms
- Energy shortages and grid capacity
- Supply chain contracts and SLAs

- Planning and Building Regulation
- Phased construction and dealing with live halls
- Managing the changing needs of consumers
- Skilled labour shortage
- Investment and DC financing
- Insurance and Legal considerations
- Ever changing regulatory pressures
- New disruptive technologies

Many of the suggestions above also feed into other Special Interest Groups we have set up, cross collaboration between groups is openly encouraged.



The DCA currently facilitates nine Special Interest or Working Groups and DCA members are welcome to join any of the groups and contribute, to find out more here:

<https://dca-global.org/groups>

If you or your organisation are interested in being part of the Data Centre Design and Construction Special Interest Group please contact Steve Hone:

steveh@dca-global.org or call **0845 873 4587**.

Is The Industry on the Edge of a Great Opportunity

BY STEPHEN WHATLING, CHAIRMAN AT BUSINESS CRITICAL SOLUTIONS, BCS



The changing landscape

THE DATACENTRE landscape is fundamentally changing and alongside the hyperscale

development, we are also seeing an increasing market towards edge data centres to support a growing need for greater connectivity and data availability. Whilst the decentralised data centre model has been around in various guises for some time, it fell out of favour for a lot of businesses as they sought to exploit the efficiencies of operating fewer, larger

datacentres. However the phenomenal growth of The Internet of Things (IoT) is driving a resurgence in its popularity. Cisco is predicting that in the five years upto 2022, 1.4Bn internet users will have been added, there will be 10.5Bn more devices and connections and broadband speeds will have increased by over 90%. Only edge networks can provide the high connectivity and low latency required by the IoT to meet users' expectations and demands for instant access to content and services.

The rise of AI

In addition, the rise of AI and immersive technologies such as virtual and

augmented reality (VR/AR) is also a factor that will help drive this move. Whilst not perhaps mainstream yet many sectors are assessing the benefits. For example, in the manufacturing environment, the now ubiquitous robots on many production lines can be improved and their role expanded by AI. A recent report by the Manufacturer (26th February 2019) found that 92% of senior manufacturing leaders believe that the 'smart factory' will help them increase productivity and empower their staff to work smarter but a similar Forrester report also found that only one in eight large manufacturing businesses are using any form of AI. However, these kinds of innovations

require a lot of computing power and an almost immediate response as a single machine that 'pauses for thought' could create a knock effect that causes immeasurable damage to the factory, production line and productivity. Once again edge computing is best placed to support this.

In the case of AI and AR, speed is an important factor. In the edge decision making is held closer to the point of need and as a result the reduction in latency between the device and the processing power enables a much faster response time. Equally importantly the data itself can be better managed in an edge environment. The data is often governed by local legislation and now it can be held in smaller data centres closer to the point of use it becomes easier to meet the legal requirements in the local region.

Data Security

One of the major factors that needs to be considered is data centre security with cyberattacks increasing in both frequency and scale. Problems originating from the physical infrastructure have also been found to be behind outages in recent years. Some experts have suggested that edge computing potentially represents a soft underbelly for cyber security. For some the use of the word 'edge' has allowed users to assume the security of these systems is not as important as local or Cloud systems. However, moving forward clients will be expecting significant investment in security and disaster recovery processes as well as the physical maintenance and security of these localised data centres.

Investment in Telecoms

Another key consideration is that the increasing adoption of edge and cloud-based infrastructure for both social and business use is also placing greater demands on the distribution network in terms of latency, bandwidth and capacity. The increase in data over the next five years will place a lot of pressure on the telecoms network. It is the telecoms industry that will need to continue to invest and upgrade capacity to ensure that the infrastructure supports the growing demand for data flows to and from the edge and the cloud. Our Summer Report, which is available to download from our website, also highlights this issue with three-quarters of respondents agreeing that



the telecoms industry needed to provide this investment. Less than 2% of all those surveyed believed that the current infrastructure would be able to support the current predictions of growth in data. This is likely cause for concern.

The need for Power

Similarly, these new data centres will need power. The thousands of servers across all connected countries will need to be located and designed with energy in mind. It is perhaps worth noting too that countries that can't support the wider network demands will quickly fall behind in the race to realise the value of AI and AR.

The Opportunity

There is no doubt that massive increase in the data that is available from billions of devices and the rise of AI is both an opportunity and a challenge for businesses. Companies that can handle the scale, analyse the data and monetise its true value will have a real advantage. Edge computing will be able to handle more than a traditional network with many more transactions per second over many more locations and architectures but how and when will this infrastructure be delivered?

Conclusion

The fact that half of our respondents believe that edge computing will be the biggest driver of new datacentres tallies with our own convictions. We believe that the edge of the network will continue to be at the epicentre of innovation in the datacentre space and we are seeing a strong increase in the number of clients coming to us for help with the development of their edge strategy and rollouts.

In our view, the recent trend of migrating computing power and workload from

in-house, on-site data centres to remote cloud-based servers and services will reverse a little. The next evolution, led by the need to make more and more decisions with little or no discernible delay, will see a move towards computing power being closer to the source of the user and the data that needs to be processed. More and more connected devices relying on the edge means more and more data centres, probably smaller than the typical Cloud data centre but no less important. With future trade, manufacturing, autonomous vehicles, city traffic systems and many other valuable applications relying on edge computing the security and maintenance of these systems will be paramount. However, there is no doubt that edge computing forms part of the future data centre landscape.

About BCS:

BCS (Business Critical Solutions) is a specialist professional services provider to the international digital infrastructure industry. As the only company in the world that is dedicated to providing a full range of services solely within the business critical and technical real estate environments, we have successfully delivered over 1500 MW of mission critical data centre space in 24 countries. Privately owned, the company acts as a trusted advisor and partner to a wide range of international clients whose data centre estate is critical to their success. Key clients include: leading organisations in the colocation and wholesale data centre sector; global technology companies; landlords and data centre operators; as well as two of the biggest data centre developers in the world.

Design & Build



The following information provides an insight and details as to why more clients are moving away from traditional procurement routes and opting to engage with MEP contractors much earlier than traditionally might have been the case, through a Pre-Construction Services Agreement (PCSA) and two stage tender processes.

BY LAWRENCE HOOKER, OPERATIONS MANAGER – SECTOR LEAD FOR MISSION CRITICAL AT MICHAEL J LONSDALE

THE PCSA and early engagement of the MEP contractors means we can properly familiarise ourselves with the project and really contribute to the design process, advise on buildability, programme, sequencing and construction risk while the project is still in its infancy.

This without doubt integrates the whole project team, results in a high-quality design that doesn't stray from the client's intent and reduces the likelihood of disagreements later on.

Design

Traditionally the consultant would design the project to stage 4 and then produce a tender information pack for the MEP contractors to price. The design would be complete but would include several CDP packages and elements that that would not be fully developed until a MEP contractor is appointed.

This often means that unavoidable changes to the services design, spatial co-ordination, façade and structural penetrations and associated builders-works are realised late in the design process and impact upon procurement and even the commencement of physical works on site.

A similar thing can happen with suppliers of major plant items, which would also benefit the from early project engagement.

Having a MEP contractor on board during the stage 3 design means CDP specialist and the suppliers can be brought in early in the process, this aids the co-ordination, maximises the pre-fabrication possibilities and leads to a better developed scheme earlier than could normally occur through the traditional route.

Design Risk

At MJL we are frequently seeing the MEP packages being let as a Design and Build; currently, around 60% of our work is on a design & build basis. We do still see a lot of projects taken to Stage 4 by the client's consultant and then let under a D&B contract. While this may provide the client with the ability to test the market-place and obtain more detailed competitive quotations for the MEP services, the cost for the design is somewhat duplicated.

Early engagement of the contractor through a PCSA during the stage 3 means that we can really get into the detail of a project and validate the design, understanding the risks and putting strategies in place to reduce them. It also means that we can support the client's designer and assist them with information and ideas that would otherwise not be available to them, through our direct experience and through the involvement of our specialist supply-chain at a stage early enough for their suggestions and proposals to be considered and adopted.

Innovation

Innovation through the traditional procurement route is extremely problematic, even when better solutions are proposed it is often too close to the necessary deadlines for procurement and commencement on site for them to be incorporated into the final design. Through a PCSA period however, innovation can be really explored. When innovation is offered in a true D&B scenario, there is time to review, challenge and investigate all the various options before having to decide and incorporate into the final design.

Health & Safety

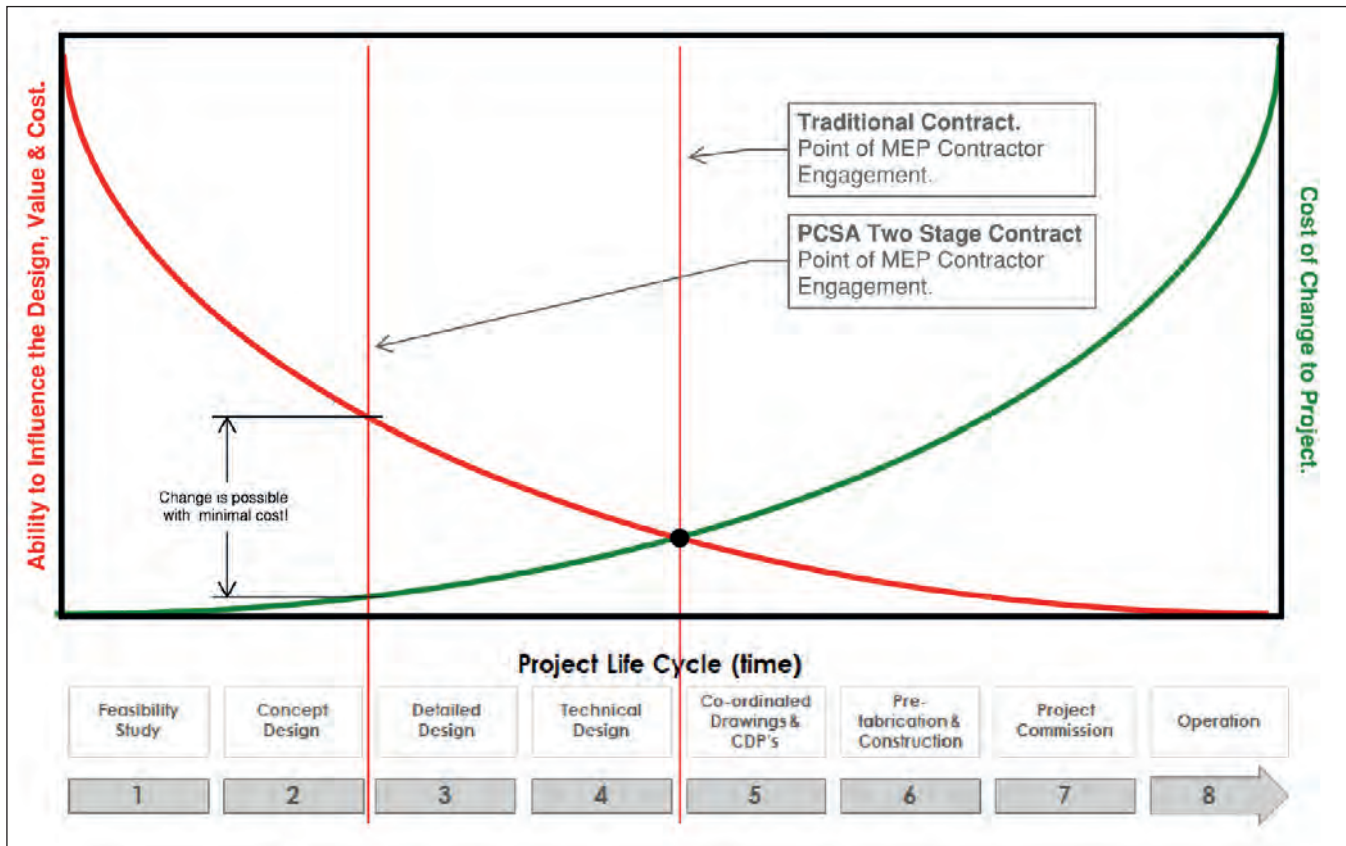
Health & Safety of the construction workers, the future occupants and the maintenance staff who will continue to operate the building is of upmost importance to all stakeholders on the project. By being engaged early we can undertake a full risk analysis of the MEP services design and suggest ways of mitigating risk through construction techniques and services layout while there is opportunity to do so. This also often involves engaging the specialist supply chain so that we can bring in their expertise to the project.

Logistics

The logistics requirements on projects is something that becomes more involved year on year, the construction of buildings has changed and the way we do things has had to change too. What we bring to site now is large, prefabricated modules and assemblies rather than the raw materials and a different set of skills and capabilities is required to undertake this safely. MJL have invested heavily into our in-house Plant Logistics division, that now handle all plant and materials across our 60-plus sites. This integral facility reduces risk and allows us to take a proactive role during the design phase, producing detailed logistics, cranes and plant movement methodologies to ensure what is being designed is optimal from a logistics point of view.

Pre-fabrication

Pre-fabrication is the most efficient method of installing services when it is possible to do so. By early involvement in a D&B contract we can achieve a true appreciation of the construction sequences. This allows us to consolidate and confirm pre-fabrication opportunities which can then be reflected in the services design layouts. By having



the MEP contractor involved early it's possible to maximise the opportunities for off-site pre-fabrication and therefore streamline the installation process, reduce the on-site build programme and reduce the level of site labour man-hours.

Commissioning

One of the most important elements of a project is ensuring the MEP services are setup and commissioned properly. MJL has its own in-house commissioning team that can assist from the outset. Having the commissioning managers who are going to be involved with the delivery of the services involved in the earliest possible reviews of the design as it develops gives certainty over the commission-ability and de-risks project delivery.

This is particularly important when there are partial, phased hand overs of systems, or areas of the project that need releasing early for client fit-out with some services functionality.

BIM & Pointcloud

BIM has without doubt transformed the way we design and build projects, however its deployment is still not well timed to fit in with the overall design

and procurement processes and is far from efficient. Through a traditional procurement route the MEP services consultant would develop a fully co-ordinated BIM model as part of their stage 4 information.

Unfortunately, while this should avoid co-ordination issues it doesn't incorporate certified manufacturers data which only becomes available once full purchase orders are in place. Likewise, the federated project model will consist of the structural engineers models and this also will normally change once the structural frame contractor updates the level of the design detailing.

The reality is that the consultant's models are often parked, and the MEP contractor will model the whole services installations from scratch, resulting in lot of abortive work being done by the consultant and being paid for by the client. If MJL own the co-ordinated model during stage 3 the consultant can concentrate on getting the design and schematics completed while we can develop a stage 4 model. This can then be developed into a construction model and produce the construction issue drawings without having to start again.

On existing buildings, the advantage is even more evident as we would PointCloud survey the structure early in the design process so that we have pinpoint accuracy to base our models on which again would avoid problems later and speed up the design process.

Price

As we are all aware if change can be captured early then the impact on cost and time is minimised. By having MJL involved as the design develops, we can track the cost plan and flag any risks to the cost plan. This enables informed discussion and where acceptable to the client, the design to be altered to either avoid cost growth or provide compensatory savings on other elements of the scheme.

Traditionally, projects get priced at the end of stage 4 and then value engineered to meet the available budget, this is the worst potential outcome for a quality building and the most likely scenario under which the original design intent gets diluted and the client's operational requirements become unachievable. The PCSA process is generally undertaken on an open book basis with the cost consultant, using pre-agreed rates and OHP.

Getting that little bit more



ZAC POTTS, ASSOCIATE DIRECTOR (DATA CENTRE DESIGN) AT SUDLOWS

discusses what getting the best performance from a Data Centre means as this can be interpreted in numerous ways.

WHAT DOES IT MEAN to you to be squeezing every drop of performance out of a data centre? The answer will undoubtedly change depending on the angle you are coming from, but should it?

Designers of the cooling, or power systems, may read this as delivering the highest capacity or most efficient cooling or UPS System. IT teams will have different ideas of “performance” depending on what they do: Compute power, bandwidth, agility or storage capacity perhaps.

Finance, of course, will likely look at the bottom line – a high performance data centre is one which generates a lot of money, or costs very little to support a business which generates a lot of money. Yes?

Fundamentally, performance is about output, so it is critical that we understand what performance means to the data centre in question. Unfortunately, there are very few data centres with a single function - bitcoin mining farms maybe - but the vast majority are inherently

complex with numerous functions, the proportion and distribution of which may even change with time.

Getting the most out of any single facility can mean a variety of things. Is it more racks, more power, or higher density? Is it high performance compute, GPU arrays, or other specialised hardware? “High Performance” can mean many things to different people. Performance is different than efficiency but often the two become closely linked - make it more efficient, and then use the spare capacity you’ve created to deliver more.

Whatever the intended meaning, there are two things critical to delivering high performance; definition, and operation. The definition stage outlines what is needed, and within what limitations. Depending on the application it could be simple or fairly complex, but to be able to squeeze every bit out of a facility or design, it is important to ensure the definition is sound, free from ambiguity or issues, and applies the right constraints in the right places. It is not the supply air temperature to the data centre,

which is important, for example, but the temperature of the equipment being supported. Defining the wrong parameter often results in great effort and expense being invested meeting a specific requirement which is later uncovered to either be outdated or set arbitrarily. Whether a new facility or an existing one, the investment in the definition stage will always pay off as once fully defined, we are then able to maximise the performance of the facility, and because of a good definition we will know what performance means.

For many years, and indeed still today, many high-performing data centres will consist of a number of carefully tuned systems, each looking after part of the system and reacting to changes in demand, be it at the IT or facility level. These control systems work to balance the performance targets and constraints set out in the definition stages, so the importance in getting that right is clear. Advanced design tools like CFD and advanced load placement algorithms offer a way to refine operation but are still based on the same definition and only offer information based on a snapshot in time.

A data centre with a solid definition, well designed with a modern deployment of sensors and controls, would still be a good example, delivering good figures in any number of KPIs chosen to be reported. That said, momentum is growing with the adoption of more complex systems with a wider scope and some level of machine learning. Machine learning can in some cases be overstated. At this time, the level of adoption is limited, and within active deployments, there is a range of successes and failures. The proven potential of machine learning systems cannot be undervalued though, especially when it comes to the final incremental improvements in efficiency and performance. It is in this area where



machine learning offers an impartial, multi-skilled, constantly working, and constantly watching, team member. One who is aware of the goals and can predict how these are best achieved.

The same tools which feed into leading design processes, are being integrated into the ML decision tree of the ML models. At Sudlows for instance, our modelling and simulation team are integrating CFD and hydraulic system models so algorithms can work with both observed historical data, and continually recalculated simulated results of scenarios which, hopefully, we'll never experience – unnerving combinations of poor load placement, system failures, peak days and grid power interruptions.

Limited to just improving the performance of the M&E, a developed ML system will soon become unchallenged, but fortunately the scope is much greater. Systems have expanded to consider long and short-term reliability, offer predictive advice on imminent faults and issues, and, perhaps most importantly, bridge disciplines to advise IT and M&E systems

based on the calculated impact to the other.

There is a huge gap between the majority of the industry and the small few who are implementing such systems at scale and given the adoption of basics such as aisle containment, it might well be a long time before we see such systems in the majority of spaces, but we will eventually. The key to squeezing every last drop of performance out of a facility might one day be a highly refined machine learning system, but first and foremost, in my opinion anyway, it is the project definition. A poor definition of what is required and the constraints within which to operate will hinder the future deployment of machine learning much the same as it will hinder the initial design and manual refinement.

For today, although such advanced controls will always offer an edge, a well-designed facility with a “standard” system can still be optimised for a good level of performance gains through good initial design and constant review, indeed using many of the same tools which feed

into an advanced ML platform.

In many ways a modern facility with its extensive data collection and dynamic operation, is “ML Ready” when the time comes, but in the meantime, it is critical to build up from the basics and invest in the definition and design, or the additional layers of the future will have a very poor foundation upon which to build.

Zac Potts, Associate Director, Sudlows

Zac leads both the award-winning Data Centre Design Team, and the Engineering Simulation Team at Sudlows where he has directed the design, simulation, construction and testing of multiple high specification data centre projects.

Contact Sudlows - zacpotts@sudlows.com
sudlows.com/ hello@sudlows.com
[/ www.sudlows.com](http://www.sudlows.com)

Top design considerations for the most efficient data centre lighting solution

BY ZUMTOBEL UK

LIGHTING may only consume a fraction of the total energy used within a data centre but its impact and cost savings go far beyond the cost of lighting. In addition to saving energy, money and maintenance efforts, a highly efficient LED lighting system can offer data centre operators a simple solution to maximise both safety and the productivity of their staff.

Extremely long life, low carbon emissions and excellent task lighting are just some of the benefits of highly efficient LED lighting. Spending a little extra time during project design stage and partnering with lighting experts will lead to fewer issues in the long-term. Zumtobel Lighting are experts in this sector and have looked at addressing key lighting specification considerations for Data Centre applications:

Ambient air temperature

The ambient air temperature of a facility is often considered one of the most important aspects of data centre design. Hot and cold aisles typically result in fluctuating temperatures and increasing pressure on any hardware found within a data hall. The first step is to determine if the luminaires being considered have been fully tested and have an appropriate ambient temperature rating for the environment.

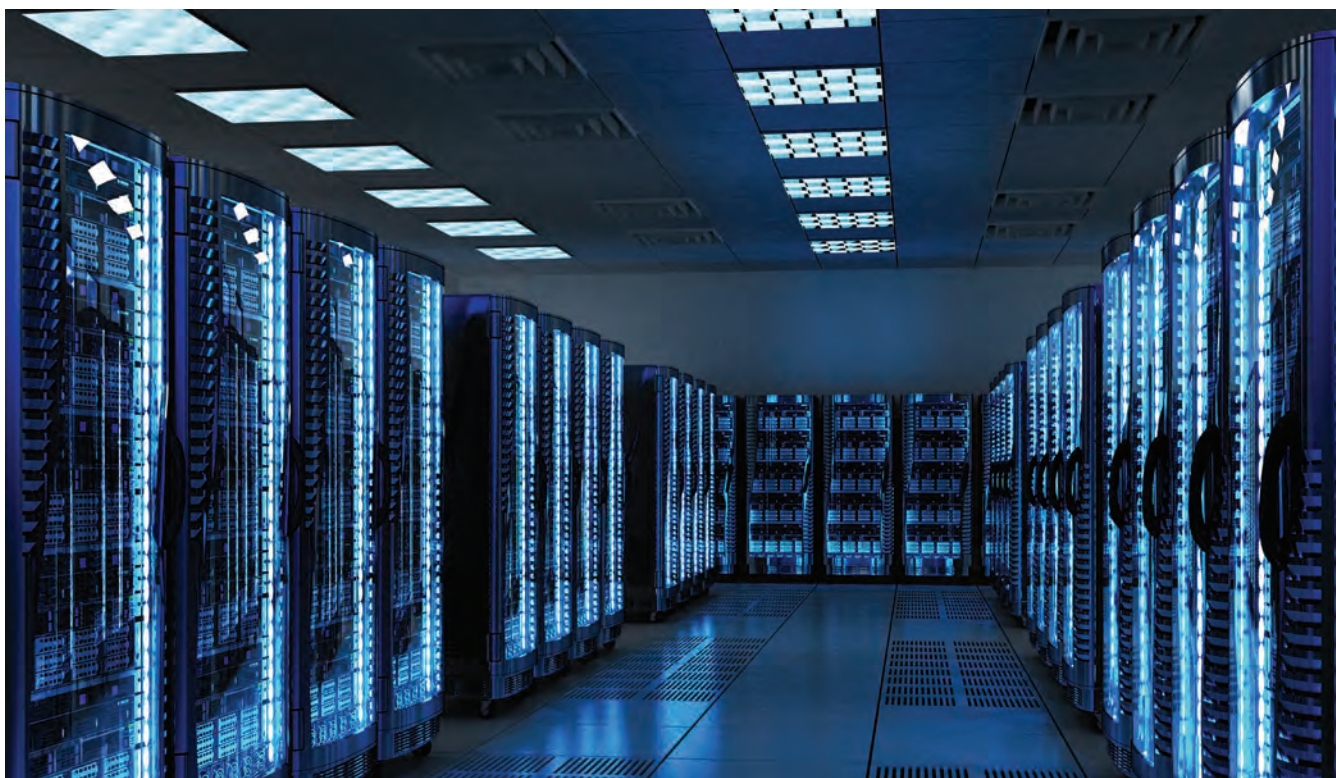
Task lighting

Although data centres do not have the same occupation rate as traditional commercial businesses, technical engineers need to monitor and work in close proximity to the servers. A well-lit working plane is crucial, engineers can accurately record information and clearly see the task at hand. It is vital that the

lighting system is designed to light the face of the servers, similar to a library where you are illuminating the spines of books to 500lux for ease of identification.

The introduction of innovative lighting control can also prove beneficial, additional energy savings of at least a further 10 per cent can be experienced when LED luminaires are integrated with sensors to manage when and where light is used, reducing running time and unwanted heat gain.

Lighting control should be the rule rather than the exception as the right choice of highly efficient lighting coupled with an intelligent lighting control system will enable consistent monitoring of a lighting installation whilst enabling remote reporting of potential faults within the system.



Emergency lighting

Every data centre is laid out differently so there is no one size fits all solution. Emergency lighting systems are a critical part of any commercial building, data centres are not an exception they must have a proven emergency lighting scheme, this is a legal requirement forming part of the wider life safety system. Along with a consistent and reliable power stream, your emergency lighting back-up system needs to provide power to the emergency luminaires for between 1 and 3 hours depending on the geographical location.

High ambient air temperatures can lead to a design preference for central battery systems (which can be located remotely) as over self-contained emergency luminaires, due to heat exposure, can result in reduced battery life expectancy and increased susceptibility to overheating and failure.

External lighting

Data and premises security are at the forefront of a Critical Facility operator's priorities, whilst IT security measures are paramount, unfortunately external lighting is all too often a neglected design focus when fortifying a facilities perimeter defences. External lighting can help support and define the building's entrance, perimeter and produce better

visibility for CCTV identification. In addition to security lighting, the use of architectural lighting within client-facing zones such as a reception area, can support brand identity. The correct choice of products used across external areas will give the facility an identity whilst improving security for the building and its employees surroundings.

Modularity

The Data Centre Industry is growing fast, one of the key challenges facing Developers and Operators is how

to build and scale to meet client demand. Products which offer modular construction allow for greater design flexibility and enable the build to progress piece by piece, increasing MW capacity without compromising on time or value. Prefabricated sections constructed within off-site controlled manufacturing facilities, improve build consistency, decrease on-site install time, and reduce the quantity of large multi-skilled site based install teams when compared to traditional methods of construction, and are also kinder to the environment.

About Zumtobel

We are passionate about designing and producing the highest quality of light. Our work is driven by the knowledge that the right light can create the right environment for people to thrive when tailored to their individual needs. Guided by a unique design approach, we continuously push our boundaries in search for perfection through unique and timeless design. As we develop the next generation of lighting, we build on our family heritage to refine the aesthetics of light and shape the lighting of tomorrow. With a special blend of passion, grace and avant-garde ideas, we turn light in to an experience and remain committed to the goal of improving the quality of life through light. Zumtobel is a brand of the Zumtobel Group AG with its headquarters in Dornbirn, Vorarlberg (Austria).

Zumtobel. The Light.

Zumtobel UK Details

Tel: 01388 420042

Email: info.uk@zumbelgroup.com

Web: <https://z.lighting/en/zumbel>



ROUNDTABLE

WITH ERIK SALO AND ANDY PALMER

10:00 – 11:00 AM (+1 GMT)

REGISTER NOW

digitalisationworld.com/s/seagate

In this exclusive roundtable, tech celeb Erik Salo and Seagate enterprise solutions specialist Andy Palmer discuss the latest intelligent storage solutions to optimize data centers.

They go into depth on Seagate Corvault, Salo's invention, and reveal the key trigger that led to it. Afterwards, they will be addressing questions.



Erik Salo
Sr. Director
Worldwide Systems
Distribution



Andy Palmer
UK Channel Lead
Enterprise Data
Solutions

A New Category of Intelligent Storage

Exos CORVAULT is a high-performance, self-healing block storage system that delivers multi-petabyte capacity, five-nines availability, and hyperscale efficiencies for data center and macro edge environments.

