DIGITALISATION WORLD

MODERN ENTERPRISE IT - FROM THE EDGE TO THE CORE TO THE CLOUD

ISSUE 2 2022

DIGITALISATIONWORLD.COM

Creating simpler, smarter and more efficient clouds

StorPool
DISTRIBUTED STORAGE

AIOps | 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

AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION

EcoStruxure™
Innovation At Every Level

Deploy your data centre FASTER with less risk using EcoStruxure™ Data Centre solutions.

EcoStruxure™ for Data Centre delivers efficiency, performance, and predictability.

- Rules-based designs accelerate the deployment of your micro, row, pod, or modular data centres
- Lifecycle services drive continuous performance
- Cloud-based management and services help maintain uptime and manage alarms

Discover how to optimise performance with our EcoStruxure Data Centre solution.

se.com/datacentre

Life Is On | Schneider Electric

Editor's view

By Phil Alsop

Technology out of control?

FOLKS THAT SAY 'I told you so' tend to be resented. So, I'll try not to dwell on the fact that, just as the Communist empire was crumbling, I was telling anyone and everyone who cared to listen (so not very many!) that it would be dangerous to assume that all the West's political troubles were at an end.

I did not predict the rise of Middle Eastern extremism, nor the current Ukraine atrocity, but a quick study of the history books was enough to suggest that, no matter how benign the world, and Europe in particular, might seem, there's always a conflict of one sort or another just around the corner. We might become more technologically savvy over the years, and like to think we have become more civilised along the way, but our ability to upset one another, or to pick a fight with someone, somewhere, shows no sign of slowing down. And the lessons of history continue to fall on deaf ears.

Undeterred, I'll make another prediction for the years ahead. While technology brings with it immeasurable benefits in so many ways, it also has the ongoing potential to wreck what we like to call 'civilisation'. And not just because of the obvious risk associated with cyber warfare and more widespread cybercrime – although these are major causes of concern. No, although the rates may vary from country to country, there seems little doubt that, in their pursuit of ever higher rates of profitability, many organisations, if not all, are content to replace humans with automation in so many ways, storing up a potentially major cause of social disruption. However you disguise it, the idea behind automation is to replace humans with machines. And, despite the suggestion that these 'displaced' workers can find employment elsewhere, the reality is that relatively few machines could replace many, many millions of humans. And there are not going to be millions of millions of new jobs for these people to move to.

A recent shopping trip, where, in visiting three different stores, there was no human interaction – I was required to

checkout my purchases without any shop staff involvement – flagged up this cold future. And I won't bother you with the details of some recent utility company customer service interactions, where it would appear that robots are there not to help but deliberately hinder, humans having been ditched along time ago.

The question for individuals, companies and governments across the globe would seem to be: What kind of a future do we want? Environmentally, we seem to have decided that, however dire the warnings, we'll kick the can, maybe not off the road and into the long grass, but somewhere down the tarmac.

I fear that, society-wise, we will similarly let things drift, until the (too late) realisation that millions of folks don't have any work or income, and they are not very happy about the situation. Technology and ethics are maybe not the most obvious of bedfellows, but they need to be, and urgently!

DIGITALISATION WORLD

16

CREATING SIMPLER, SMARTER AND MORE EFFICIENT CLOUDS

StorPool's development team have evolved the storage platform and help expand its features and capabilities so that it can deliver above and beyond what is possible with other primary storage products in terms of reliability, agility, speed, and cost-effectiveness

The data centre trade association

DCA News

DIGITAL BUSINESS

CYBERSECURITY

NETWORKS

NEWS

Angel BUSINESS COMMUNICATIONS feature

DW DIGITALISATION WORLD

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

Editor
Philip Alsop +44 (0)7786 084559 philip.alsop@angelbc.com
Sales Manager
Shezhad Munshi +44 (0)1923690215 shehzad.munshi@angelbc.com
Sales Executive
Jessica Harrison +44 (0)2476 718970 jessica.harrison@angelbc.com
Director of Logistics
Sharon Cowley +44 (0)1923 690200 sharon.cowley@angelbc.com
Design & Production Manager
Mitch Gaynor +44 (0)1923 690214 mitch.gaynor@angelbc.com
Publisher
Jackie Cannon +44 (0)1923 690215 jackie.cannon@angelbc.com

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

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

Digital transformation momentum increases

Digitopia has found that the digital maturity average has improved from 2.7 in 2020 to 2.8 in 2021 across all industries and geographies, according to its Digital Maturity Index (DMI). The same survey found that organisations are reasonably aware of their digital needs, falling in the 'organised' and 'integrated' phases where steps are being taken to improve capabilities in leveraging data and enhancing operations.

DIGITOPIA has found that the digital maturity average has improved from 2.7 in 2020 to 2.8 in 2021 across all industries and geographies, according to its Digital Maturity Index (DMI). The same survey found that organisations are reasonably aware of their digital needs, falling in the 'organised' and 'integrated' phases where steps are being taken to improve capabilities in leveraging data and enhancing operations.

Digitopia's DMI, enables businesses to accurately measure and benchmark their digital progress. It remains industry agnostic, and blends high-end consulting services with advanced software and analytics. Digital transformation is hard, especially during turbulent times where competition, regulatory pressure, challenges arising from climate change and supply chain disruptions heavily impact decision-making. The data shows that while the digital capabilities of many businesses are trending upwards, there is much left to be done for organisations to become 'optimised' or truly digital in their operations. Areas that require ongoing effort across all industries include systems integration, advanced analytics, business agility, and other advanced systems.

According to Digitopia's latest research, as the average score shifts upwards, so do stakeholder expectations for all organisations to provide a more digitally-accessible service. For many organisations, improving their score by a whole level within the DMI (for example, from organised to integrated) takes years of planning and implementation.

The study, which analysed the responses from more than 1000 executives - ranging across C-Suite, VP and Director roles - in over 100 different companies and 10 industries, found that technology maintains the highest priority of importance with a score of 2.91 compared to the customer dimension sitting at 2.77. This is evidence that customer focus is not the driving factor for organisations going through a digital transformation journey. However, customer experience and customer-centricity saw an average improvement of 0.15 points from its 2020 report, the largest of any individual dimension.

Across the six digital maturity dimensions assessed within the DMI, innovation is falling behind as the least developed aspect of business transformation. COVID-19 has had lasting effects on organisations, but without implementing innovation they will not be able to maximise benefits from developing an ecosystem that brings in new and impactful ideas from outside the business.

Digital maturity differs between sectors, but financial services, including banking and insurance, is ahead as one of the digital pioneers with a score of 3.1. Closely followed by automotive (2.9), insurance (2.9), manufacturing (2.8), C&G (2.7), retail (2.6) and services (2.5).

"These findings show that organisations are beginning to understand the importance of digital transformation and measuring this journey." said Halil Aksu, CEO and co-founder of Digitopia. "You manage what you measure, and it's encouraging that businesses are progressing their digital maturity. 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."

Businesses are failing to leverage mobile technology

Digitopia has found that the digital maturity average has improved from 2.7 in 2020 to 2.8 in 2021 across all industries and geographies, according to its Digital Maturity Index (DMI). The same survey found that organisations are reasonably aware of their digital needs, falling in the 'organised' and 'integrated' phases where steps are being taken to improve capabilities in leveraging data and enhancing operations.

SOTI GLOBAL REPORT finds almost half (45%) of enterprises are failing to leverage mobile technology to adjust to the challenges of a post-pandemic economy. In a new marketplace that is more fluid, more digital, more dynamic and marked by a rise in consumer demands, almost half (45%) of global enterprises are failing to leverage mobile technology to adjust to the challenges of a post-pandemic economy new global research from SOTI has found.

Despite over three quarters (79%) of enterprise leaders agreeing their C-Suite realises the importance of mobile technology more now than before the start of the COVID-19 pandemic, over three quarters (76%) believe there is more their organization can do to improve its ability to be agile and adapt to new scenarios.

While SOTI's A Defining Year: State of Mobility 2021 Report found that 81% estimate up to a half of their organization's day-to-day operations are dependent on mobile technology, the report also revealed that in many cases, businesses may be missing the mark in getting the best possible returns from the money they're putting into mobile technology. Almost a third (31%) of enterprises said they failed to see a positive ROI from last year's investment in mobile technology.

SOTI's global research has sought to understand the impact of mobile technology over the last year as well as how organisations can position themselves at the forefront of the post-pandemic mobile revolution. 1,400 business leaders were interviewed from enterprises in eight countries across three continents, including the UK.

These figures suggest that while investing in mobile technology has helped businesses to weather the storm, ensuring a healthy return on the investments comes with additional considerations.

For example, almost a third (31%) of business leaders said that security is the biggest challenge they face with mobile technology, followed by integration with other systems (20%). In addition, more than half (56%) of respondents admitted that they find it hard to manage their organisation's expanding portfolio of mobile devices.

If these challenges are addressed, then businesses achieve the agility they need to respond to future crises and will find it easier to respond in real-time to the market's changing demands. Mobile technology has the potential to provide flexibility and intelligence across the whole enterprise, however it needs to be integrated into core workflows and managed and secured via one platform.

"Our research confirms that mobile technology has become crucial to forging a new path in a volatile economy and that at the same time enterprises are finding it difficult to make the most of their investments. Simply adopting new technology isn't enough to gain the greatest competitive advantage," comments Sarah Edge, Director of Sales, UK and Ireland at SOTI. "To maximise their returns, enterprises need the right mix of mobile technologies and the right integration strategy."

Attention is beginning to turn towards this challenge with around four in ten (41%) organisations considering increased expenditure in either mobile technology security, technology that will allow for better mobile device and system integration (40%), or in cloud-based systems (40%). The mobile revolution will eventually slowdown in terms of the volume of new devices adopted, but enterprises will need to find effective ways to ensure their mobile infrastructure is working to its maximum potential.

"There is still a great deal of potential locked up in organisations' mobile technology and enterprise leaders have high expectations and aspirations for the near future. The most successful mobile solutions consider all the key factors influencing performance – from mobile device and application capabilities to network performance and ultimately the user experience." says Edge.

Data scientists reveal digital roadblocks

SAS research also identifies strategies to capitalise on this pivotal moment and empower data scientists and organisations.

DIGITAL TRANSFORMATION has accelerated significantly due to the COVID-19 pandemic, but the extra demands on data scientists have revealed significant barriers to effective working and high levels of job dissatisfaction in some areas. For example, around four in 10 are dissatisfied with their company's use of analytics and model deployment, while more than 20 barriers to effective working emerged, according to a survey of data scientists commissioned by analytics leader SAS.

However, the work of data scientists has grown in importance with many organisations accelerating digital transformation projects by using technology to improve business operations. More than 90% of respondents indicated the importance of their work was the same or greater compared to before the pandemic.

To delve deeper into the state of data science, the report assesses the impact of the pandemic, challenges faced, overall satisfaction with the analytics environment, and more. The research showed the pandemic upended standard business practices, shifting the assumptions and variables in models and predictive algorithms and causing a ripple effect of adaptations in processes, practices, and operating parameters. More than two-thirds of respondents were satisfied with the outcomes from analytical projects. However, 42% of data scientists were dissatisfied with their company's use of analytics and model deployment, suggesting a problem with how analytical insights are used by organisations to inform decision-making. This was backed up by 42% saying data science results were not used by business decision makers, making it one of the main barriers faced.

The survey also highlighted some specific skills gaps. Less than a third of the respondents reported having advanced or expert proficiency in program-heavy skills, such as cloud management and database administration. This is an issue given that use of cloud services is up significantly, with 94% saying they experienced the same or greater use of cloud since COVID-19 struck.

"There have clearly been more demands placed on data scientists as the pandemic has accelerated digital transformation projects that many organisations were planning anyway," said Dr Iain Brown, Head of Data Science, SAS UK & Ireland. "A major source of frustration is finding a way for organisations to implement the insights from analytics projects and use them in their decision-making, meaning giving data scientists a seat at the boardroom table might be a way forward.

"Linked to this, we found concerns around support for data science teams and a lack of talent, which has been an issue for some time with demand outstripping supply. Organisations must realise that investing in a team of data scientists with complementary skills could reap huge value for the business, so the cost of hiring needs to consider the return on that investment as we move to significantly more digital and AI-driven business processes."

The research also identified gaps in consistent organisational emphasis on AI ethics with 43% of respondents indicating that their organisation does not conduct specific reviews of its analytical processes with respect to bias and discrimination and only 26% of respondents reporting that unfair bias is used as a measure of model success in their organisation.

When it comes to the challenges identified to ensure fair and unbiased decision-making, Dr Sally Eaves, an industry expert, said: "Data scientists can lend their expertise to craft working guidelines for data access, usage security, and broader issues, such as sustainability and data ethics and bias.

The research revealed positive outcomes from the global disruption of the pandemic. Nearly three-quarters (73%) said they are just as productive or more productive since the pandemic, while a similar proportion (77%) revealed they had the same or greater collaboration with colleagues. This suggests many of the challenges highlighted were in existence, possibly to a greater degree, before the pandemic.

Other challenges experienced were the amount of time spent on data preparation versus model creation. Respondents are spending more of their time (58%) than they would prefer gathering, exploring, managing, and cleaning data.

C-suite needs to become more digitally aware and 'invest, innovate and automate'

Nutanix has published the findings of the recently commissioned IDC CXO Survey, outlining that while companies are building better digital habits and systems, a shift is needed from digital culture to value realisation.

SURVEYING LEADERS across EMEA, the IDC InfoBrief, sponsored by Nutanix, From Digital Culture to Value Realisation showed that 84% of IT leads in EMEA are under pressure to deliver on digital transformation (DX) strategies, and 90% of organisations in EMEA recognise that having a digital-first approach is now a must-have.

"With the pandemic accelerating the rate at which companies have invested in and deployed digital solutions, IDC predicts that in 2022 more than half of the global economy will be based on or influenced by digital solutions," said Sammy Zoghlami, SVP EMEA at Nutanix. "Digital-first not only requires a system rethink, but it also requires a corporate mindset where all C-suite executives see their digital technologies as the catalyst for business growth. The survey clearly states that organisations must consider potential challenges and costs when running multiple cloud instances, highlighting the ongoing need for better multi-cloud management and streamlined deployment to avoid cloud sprawl."

The survey shows that translating digital investments into new revenue streams is a top priority for EMEA organisations, as is data and innovation. Yet respondents believe the onus can no longer rest solely on the shoulders of the IT department and need to be embraced by the C-suite as globally we come to terms with what a digital culture, digital infrastructure and digital-first means to an organisation.

Key findings from the survey revealed:

Turning investments into revenue - Over 64% of EMEA organisations say they have a digital strategy in place. Still, only 3% say they have an enterprise-wide digital strategy that has led to new revenue streams. There is, however,

a disconnect between business, of which 32% state they are in a proof-of-concept pilot stage for their digital projects and IT, of whom only 5% say their companies are developing digital strategies to support new revenue streams.

From IT to C-suite - Respondents are clear that for a digital strategy to have an impact, it is essential to bid farewell to hierarchical structures and move to more fluid and orchestrated approaches between IT and leadership teams. Out of the respondents questioned, at least 47% say that the sign-off belongs to a CXO different from a tech lead for their DX initiatives.

Shaping digital culture - When asked what measures DX leaders are considering to transform the organisation's culture effectively, the following three were ranked the highest: promoting change in management awareness, redefining the missions and evaluations of existing businesses and new businesses, and promoting behavioural change in individuals by renewing the company's purpose and action guidelines.
Key pillars for shaping digital culture - According to the survey, three key pillars stand out in how C-suites must cooperate to create the digital culture, using the cloud as the enabler for all three digital culture streams. These are value economics, data-driven innovation and the future workplace.

The numbers to support this show that 50% of EMEA organisations think that additional investments in managed infrastructure will help deliver better digital value, and 30% say they are co-creating new products with customers and partners. In terms of the workplace, 35% of organisations think that ensuring equal access to information and digital tools to all staff regardless of location will challenge the future workplace.

Managing cloud sprawl remains a crucial challenge for businesses starting their digital journey. As a result, finance departments are stepping up to put measures in place to curb expenditure and manage cloud usage. In support of this, 77% have redesigned purchasing processes to enable pay-as-you-use and consumption models, 58% have rationalised business and developer expenditure in external cloud resources, and over 55% have actively reduced costs on legacy on-premises systems.

Home working increases 'digital anxiety'

Two-thirds of remote workers reported worrying about their online security and privacy, even if nothing is wrong.

WORKING FROM HOME has spiked since the onset of the Covid-19 pandemic in March of 2020. This effort to reduce health risks may have limited the spread of the virus, but according to a new analysis by cyber security provider F-Secure, it may also have helped increase digital anxiety for those working remotely.

In a recent survey, 67% of internet users who work from home reported they increasingly worry about their online security and privacy even if nothing is wrong, compared to 58% of other users.

Senior Lecturer in Cyberpsychology at Nottingham Trent University Dr. Lee Hadlington, who's research interests include employees' adherence to workplace cyber security practices, said it makes sense that people's sudden shift to telecommuting increased their anxieties about online threats.

"It is not surprising that individuals have started to worry more about cyber security, particularly when working from home. Many individuals were thrust into the 'new normal' of home working with very little preparation, training, or equipment. Let's not forget, for most individuals in a workplace environment, cyber security is generally a second thought, and is usually something that is seen as the responsibility of someone else in the company. This, coupled with the fact that many home workers have less than perfect home working environments (e.g. desks in busy parts of the house, limited/poor internet connection, limited working knowledge of internet-based technology), means that these cyber security fears could be symptomatic of a combination of factors," he said.

While worries about online security and privacy were prevalent among all survey respondents, remote workers reported elevated concerns about a myriad of issues, including:

- 65% of those who work from home said the internet is becoming a more dangerous place, compared to 54% of other respondents.
- 63% of remote workers said concerns about data privacy have changed how they use the internet, compared to 48% of other respondents.
- 71% of remote workers said they worry that new internet connected devices – such as wearables and connected home appliances—could lead to a violation of their privacy, compared to 64% of non-remote workers.
- 70% of remote workers felt increasingly uncomfortable connecting to public WiFi due to security risks compared to 63% of other respondents.

"Working from home could also have meant that individuals may have had more time to focus on other aspects of their working life and spent more time engaging in self-reflection and aspects of self-improvement; this could have included a re-assessment of cyber risks in their daily lives. The pandemic also meant people were isolated, with many turned to the one thing they did have access to – the Internet. Of course, spending more time engaged in one activity could lead to an increase in perceptions of risk, particularly when people are being subjected to negative news stories about cyber security related issues," Dr. Hadlington explained.

According to F-Secure Security Consultant Tom Gaffney, managing security while working remotely takes technical security measures that protect data and devices, but also steps to keep people's personal and professional lives separate.

AI/ML technologies are increasingly mission-critical

Rackspace Technology has published a new research report that finds that while Artificial Intellegence and Machine Learning (AI/ML) are on nearly every organization's radar much work remains to be done to tap their full potential.

RACKSPACE TECHNOLOGY polled 1,870 global IT leaders, across industries, including manufacturing, financial services, retail, government, and healthcare to understand the dynamics of AI/ML uptake. While 62% of respondents said that AI/ML is a high priority for their organization, and 70% of all respondents reported positive impacts of on brand awareness and reputation, as well as revenue generation and expense reduction, 36% agreed that measuring and proving the technologies' business value remains a challenge.

"As AI/ML budgets continue to increase, we are seeing projects proliferate across more areas of the organization, and it's clear that the AI/ML is advancing in its importance and visibility," said Jeff DeVerter, Chief Technology Evangelist, Rackspace Technology. "At the same time, the research makes clear that many organizations still struggle with getting stakeholder buy-in, addressing issues of data quality, and finding the skills, resources and talent to take advantage of the AI/ML's full potential."

According to the report – AI/ML is a Top Priority for Businesses, but are They Realizing Its Value? – AI/ML ranks among the top two most important strategic technologies for organizations, alongside cybersecurity. 72% of respondents say they are employing AI/ML as part of their business strategy, IT strategy or both, while 69% of respondents are allocating between 6% and 10% of their budget to AI/ML projects. This compares to a reported spend (as a percentage of overall budget) of between 1% and 10% in last year's survey. AI/ML are being used by organizations in an increasingly wide variety of contexts, including improving the speed and efficiency of processes (52%), personalizing content and understanding customers (44%), increasing revenue, gaining competitive edge and predicting performance (42%), and understanding marketing effectiveness (36%).

In an indication of the increasing maturity of the technologies, 66% of respondents said their AI/ML projects have gone past the experimentation stage and are now either in the "optimizing/innovating" or "formalizing" states of implementation. Most organizations are also citing a wider range of use cases, including computer vision applications, automated content moderation, customer relationship management, and biomedical applications.

With regard to AI/ML adoption, 33% of respondents cite difficulties aligning AI/ML strategies to the business – a year-over-year increase of 10%. In addition, the cost of implementation rose from 26% to 33%, while 31% of respondents of nascent AI/ML technologies as a barrier, representing an increase of 13%. "The fact that many organizations are having trouble aligning AI/ML strategies to the business and navigating the plethora of new tools available indicates that projects are often falling victim to poor strategy," added DeVerter. "Garnering support from the right stakeholders, coming to consensus on deliverables, understanding the resources necessary to get there, and setting clear milestones are critical components to keeping projects on track and seeing the desired return on investment."

From a talent perspective, more than half of respondents said they have necessary AI/ML skills within their organization. At the same time, more than half of all respondents say that bolstering internal skills/hired talent and improving both internal and external training are on their agenda. Comparing departments, 69% of respondents say IT staff grasp AI/ML benefits while 43% say that operations, R&D, customer service, senior management and boards understand the technologies. Sales, HR and marketing departments are considered by respondents to be the least AI/ML-savvy.

83% of successful ransomware attacks feature double or triple extortion tactics

New Venafi research shows that ransomware attackers are regularly exfiltrating data, circumventing 'restore from backup' safety measures.

VENAFI has published the findings of a global survey of IT decision-makers looking into the use of double and triple extortion as part of ransomware attacks. The data reveals that 83% of successful ransomware attacks now include alternative extortion methods, such as using the stolen data to extort customers (38%), exposing data on the dark web (35%), and informing customers that their data has been stolen (32%).

Just 17% of successful attacks solely asked for a ransom in return for a decryption key, meaning that many new forms of extortion are now more common than traditional methods. As data is now being exfiltrated, having a back-up of data – while still essential for recovery from an attack – is no longer effective for containing a breach.

The data also shows that cybercriminals are following through with these extortions, often even after a ransom has been paid:

- Almost a fifth (18%) of victims paid the ransom but still had their data exposed on the dark web

This is more than the 16% that refused to pay the ransom and had their data exposed

- Almost one-in-ten companies (8%) refused to pay the ransom, and the attackers tried to extort their customers

Over a third (35%) of victims paid the ransom but were still unable to retrieve their data

"Ransomware attacks have become much more dangerous. They have evolved beyond basic security defenses and business continuity techniques like next-gen antivirus and backups," said Kevin Bocek, vice president of business development and threat intelligence at Venafi. "Organizations are unprepared to defend against ransomware that exfiltrates data, so they pay the ransom, but this only motivates attackers to seek more. The bad news is that attackers are following through on extortion threats, even after the ransom has been paid! This means CISOs are under much more pressure because a successful attack is much more likely to create a full-scale service disruption that affects customers."

When asked about the evolution of extortion in ransomware attacks, 71% of those polled believe that double and triple extortion has grown in popularity over the last 12 months, and 65% agree that these new threats make it much harder to say no to ransom demands.

This is creating problems for the industry. 72% of IT decision-makers agree that ransomware attacks are evolving faster than the security controls needed to protect against them, and 74% agree that ransomware should now be considered a matter of national security. As a result, 76% of companies are planning on spending more in 2022 on ransomware-specific controls due to the threat of double and triple extortion.

Wider than internal measures, two-thirds (67%) of IT decision-makers agree that public reporting of ransomware attacks will help to slow down its growth. A further 77% agree that governments should do more to help private companies to defend themselves from ransomware.

"Threat actors are constantly evolving their attacks to make them more potent, and it's time for the cybersecurity industry to respond in kind," explained Bocek. "Ransomware often evades detection simply because it runs without a trusted machine identity. Using machine identity management to reduce the use of unsigned scripts, increase code signing and restricting the execution of malicious macros are vital to a well-rounded ransomware protection."

EXAGRID®

Tiered Backup Storage

The Future of Backup Storage:

Tiered Backup Storage

Scales to 2.7PB without forklift upgrades or performance degrades with ExaGrid scale-out architecture.

3X
faster backups than dedupe appliances

20X
faster restores than dedupe appliances

Backup window that is **fixed length as data grows**

5YR
Price Protection Plan

New Retention Time-Lock for Ransomare Recovery

Set up with a
Proof of Concept
to experience the difference.

TEST IT TODAY ➤

exagrid.com

IDC forecasts major AI spend increase

Worldwide revenues for the artificial intelligence (AI) market, including software, hardware, and services, is forecast to grow 19.6% year over year in 2022 to $432.8 billion, according to the latest release of the International Data Corporation (IDC) Worldwide Semiannual Artificial Intelligence Tracker. The market is expected to break the $500 billion mark in 2023.

"AI HAS EMERGED as the next major wave of innovation. AI solutions are currently focused on business process problems and range from human augmentation to process improvement to planning and forecasting, empowering superior decisioning and outcomes. Advancements in language, voice and vision technologies, and multi-modal AI solutions are revolutionizing human efficiencies," said Ritu Jyoti, group vice president, Worldwide Artificial Intelligence (AI) and Automation Research at IDC. "Overall, AI plus human ingenuity is the differentiator for enterprises to scale and thrive in the era of compressed digital transformation."

Among the three technology categories, AI Software will see its share of spending decline slightly in 2022 as spending for AI Hardware and Services grows more quickly. This trend will continue into 2023. Overall, AI Services is forecast to deliver the fastest spending growth over the next five years with a compound annual growth rate (CAGR) of 22% while the CAGR for AI Hardware will be 20.5%.

In the AI Software category, AI Applications accounted for 47% of spending in the first half of 2021, followed by AI System Infrastructure Software with around 35% share. In terms of growth, AI Platforms are expected to perform the best with a five-year CAGR of 34.6%. The slowest growing segment will be AI System Infrastructure Software with a five-year CAGR of 14.1%.

Within the AI Applications segment AI ERM is forecast to grow the fastest over the next several years relative to AI CRM and the rest of AI Applications. Among all the named software markets published in the Tracker, AI Lifecycle Software is forecast to see the fastest growth with a five-year CAGR of 38.9%.

In the AI Services category, AI IT Services enjoyed 20.4% year-over-year growth in the first half of 2021 with worldwide spending reaching $18.4 billion. This growth is forecast to improve to 22% in 2022 and remain there through the end of the forecast period. AI Business Services are not far behind in terms of growth with a five-year CAGR of

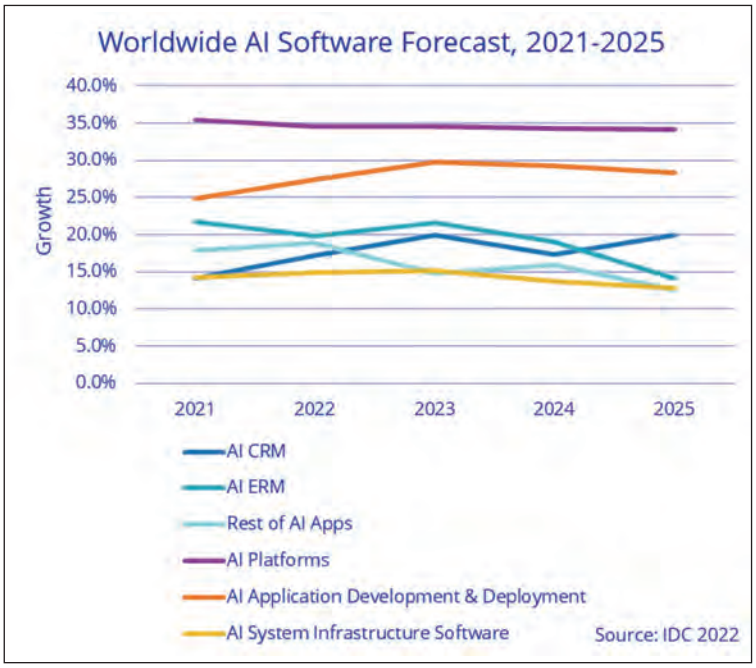
21.9%. By 2025, IDC expects overall AI Services spending to reach $52.6 billion.

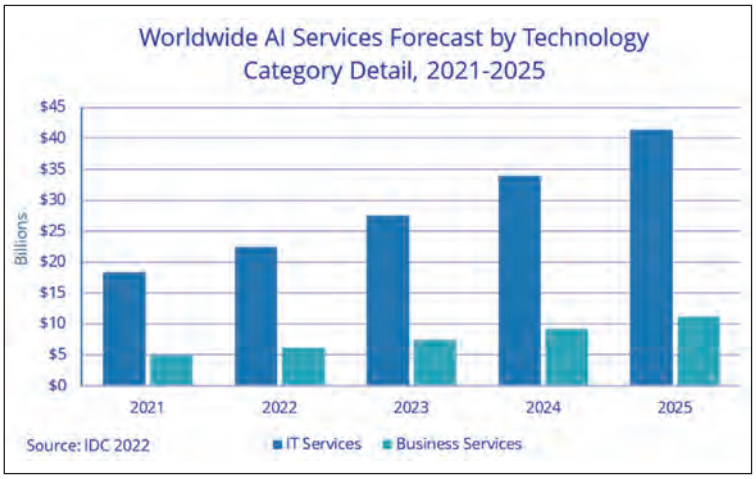
"AI remains a key driver of IT investment, which in turn boosts spending on related services to ensure sustainable adoption at scale," said Jennifer Hamel, research manager, Analytics and Intelligent Automation Services. "Client demand for expertise in developing production-grade AI solutions drives IT services expansion, while the need to establish the right organization, governance, business process, and talent strategies spurs spending on business services."

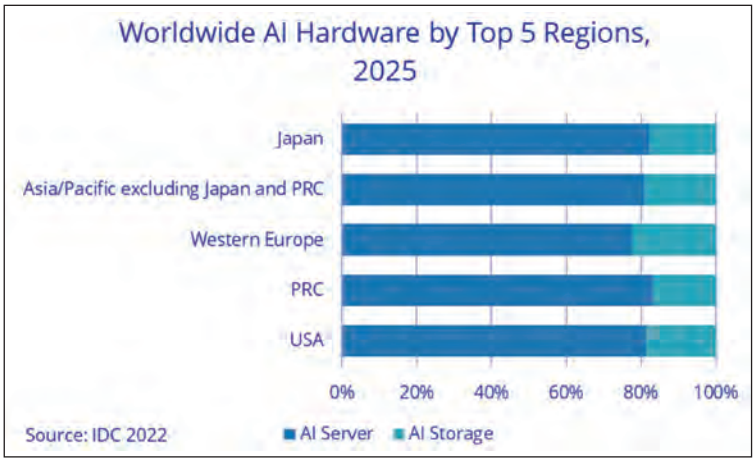
What this should tell organizations is that nickel-and-diming purpose-built hardware for AI is absolutely counterproductive, especially given the fast-growing compute demand from increasing AI model sizes and complexities

Relative to Software and Services, the AI Hardware category grew the most in terms of market share in the first half of 2021 with a jump of 0.5% share. It is forecast to reach 5% market share in 2022 with year-over-year growth of 24.9%. AI Storage saw stronger growth relative to AI Server during the first half of 2021. However, this trend will be reversed in 2022 with AI Server expected to see 26.1% growth compared to 19.7% growth for AI Storage. In terms of spending share, AI Server holds the lion's share of the category at over 80%.

"Of all the spending in the various AI market segments, AI Hardware is by far the smallest," said Peter Rutten, research vice president, Performance Intensive Computing at IDC. "What this should tell organizations is that nickel-and-diming purpose-built hardware for AI is absolutely counterproductive, especially given the fast-growing compute demand from increasing AI model sizes and complexities."







Creating simpler, smarter and more efficient clouds

DW talks to **ALEX IVANOV, PRODUCT LEAD AT STORPOOL STORAGE** and responsible for the product strategy and management at the company. He has a lot of experience working in the storage market and a deep understanding of the storage needs of today's businesses managing large-scale clouds running diverse, mission-critical workloads. His focus for the past two years has been working closely with StorPool's development team to evolve the storage platform and help expand its features and capabilities so that it can deliver above and beyond what is possible with other primary storage products in terms of reliability, agility, speed, and cost-effectiveness.

DW: *A good place to start would be a brief overview of what StorPool storage is and what it does, please?*

StorPool Storage is a storage software provider that develops its own solution for block storage – a software product for distributed data storage in cloud environments. Our solution is used by many companies worldwide that serve millions of users globally. The unique software solution helps large enterprises, SaaS vendors, hosting and cloud providers, and MSP companies deliver fast and reliable applications to their end-users. It is the perfect foundation for companies that manage their own cloud infrastructure and need to optimise it to grow their business, solve their data storage issues, or need fast and reliable access to their data to do their job effectively.

We rank among the top providers of such solutions, often winning deals versus giants like IBM, Dell, HPE, NetApp, Pure Storage, etc. The global IT leaders Atos, Dustin, CloudSigma, Nasdaq Dubai, Kualo, Amito and others are among the companies that take advantage of our reliable and fast storage systems.

DW: *And can you tell us a little bit about the main use cases for your software?*

StorPool Storage systems are ideal for storing and managing the data of primary workloads that demand extreme reliability and low latency - databases, web servers, virtual desktops, real-time analytics solutions, and mission-critical software. StorPool simplifies our partners' cloud infrastructure, removes all the pains they experienced with legacy storage products, and supercharges their revenue and profits.

Our customers' specific benefits from StorPool Storage vary depending on their use cases, technology stacks, and scale. However, the core capabilities of StorPool are that it is reliable, agile, managed with ease, utterly hands-off, and speedy. StorPool Storage has native plug-ins for Cloud Management Platforms like OpenStack, Kubernetes, OpenNebula, CloudStack, and OnApp. Thanks to

the built-in automation in each plug-in, partners can seamlessly manage their clouds from their CMP's familiar user interfaces. In addition, StorPool supports VMware, Oracle VM, Hyper-V, XenServer, and many other technology stacks.

Under the hood, StorPool builds out shared-storage pools out of DC-grade storage drives directly attached to commercial off-the-shelf servers to create the ultimate primary storage systems. These pools provide standard block device interfaces to the virtualised, containerised, or bare-metal workloads running in a cloud. We also provide a hosted analytics suite that collects hundreds of metrics per second to deliver deep insights into each storage system's performance and availability.

DW: *What are the Disaster Recovery capabilities you provide?*

StorPool's storage architecture ensures no single point of failure. To put it simply, if any part of your storage system malfunctions, the system will continue to work flawlessly. The storage architecture guarantees its continuous work even if multiple hardware components fail. We can boldly declare that we have many customers that never had a single minute of downtime for years – even during scheduled maintenance, storage device replacements, replacements of the entire infrastructure or even a change in location of the whole cloud infrastructure.

StorPool Storage systems support creating tens of thousands of snapshots of the volumes in your primary storage system without performance impacts. In addition, StorPool Storage delivers native multi-site capabilities that enable business continuity and disaster recovery practices out of the box. StorPool supports asynchronous replication of snapshots from one or more primary StorPool Storage systems to a single (many-to-one replication) or multiple (many-to-many replication) secondary StorPool storage systems. Cross-site replication is also possible, whereby two primary sites replicate snapshots to each other.

Asynchronous snapshot replication synchronizes only the data increments to the remote storage system to maximize the network link efficiency and minimize the transfer time, while at the same time guaranteeing all data is available at the remote location.

DW: *Do you apply any DevOps practices?*
StorPool applies a Continuous Improvement process that allows us to build, test, release, and deploy new versions of the software at short time intervals, which is also known as continuous integration/ continuous delivery and deployment. We take the latest builds of the software through a round of automated and manual testing on the dev/test clusters maintained by StorPool and the dev/test clusters operated by our customers. After ensuring that the software works as expected, we push each update to the production clusters of our customers.

This approach enables us to push more than 30 updates of StorPool Storage to production every year – an achievement typically associated with the leading IaaS, PaaS, and SaaS vendors. As a result, the primary storage systems of our customers continue to improve rapidly. Many of them have also added secondary storage systems in separate sites that enable backup and disaster recovery scenarios. These practices enable us to respond to software issues or threats to their environment faster than anyone else on the market.

DW: *Let's move on to some recent company news, starting with the release of StorPool Storage v19.4 – what's new?*

StorPool Storage v19.4 offers quite a lot of improvements in our product. We continue to deliver next-generation, customer-centric support, and the latest release offers improved management and monitoring capabilities for the mission-critical StorPool Storage software. The new version StorPool 19.4 offers better agility, reliability, updated hardware and software compatibility, management and monitoring changes and improvements in the business continuity features. We've also updated our OpenNebula addon and added support for OpenNebula version 6.2.

In 2021, we introduced 39 updates to our product that were focused entirely on improving the user experience and future-proofing our storage solution. StorPool Storage continues to be the primary storage platform ideal for cloud infrastructure running diverse, mission-critical workloads. In the next release, we'll keep advancing our product with space optimisation and management features needed to meet the product maturity expectations

of current and potential customers, especially power users with large-scale clouds like IT services providers and SaaS/e-commerce giants.

6. Version 19.4 suggests you've been around for quite some time – it would be great to have an overview as to how your solution has developed during this time, no doubt in response to continuously changing end-user demands?

Over the years, we had the chance to participate in a vast and competitive international market. We had the opportunity and freedom to develop our software product according to users' needs and create a unique solution that has no analogue in the world. StorPool's software is designed to keep our partners' storage systems fast irrespective of utilization rate, if drives or servers break, or while rebalancing the data inside. We always deal with software and hardware issues in the best way possible. Essentially, StorPool always extracts the maximum performance of our partners' hardware to accelerate their user-facing services.

We never stop analysing the market and identifying the challenges and problems that companies managing large volumes of data are experiencing or may experience in the future. We provide a complete storage solution with the flexibility and versatility that modern companies need to provide reliable and fast services to their internal or external customers. To stay competitive, StorPool never stops making changes and planning future updates while solving every single issue even before it arises. We always strive to provide the best storage experience possible to our customers and their users.

DW: *And StorPool has recently announced some impressive Year on Year growth, as well as a 92% Net Promoter Score – good times for the company?*

For the past two years, we've observed significant growth for StorPool. We did not slow down in our development even during the pandemic, and in 2020 we reported 80% growth of the company. We have solidified our place in the storage market for the past year and continued developing our platform. In 2021, we recorded another 30% Year over Year revenue growth and 92% Net Promoter Score. In addition to maintaining the trend of achieving high financial results, we also won the Storage Transformation Project of the Year award at the SDC awards 2021 for our project with one of our customers, the leading IT managed services provider Dustin Group. This award was another recognition for StorPool, for our unique team and our efforts to do things the right way.

DW: *You've also published the Public Cloud Performance Measurement Report 2022 – what does this cover?*

The Public Cloud Performance Measurement Report presents a testing methodology for evaluating the storage performance of any public cloud in the right way. This report showcases the performance of the block storage offerings of well-known public clouds – Amazon AWS, Google Cloud, Microsoft Azure, Linode and OVHcloud and compares them against Katapult, a StorPool-based public cloud. The Katapult system is part of a production public cloud, so results on this service are directly comparable to results from the big five public clouds.

Katapult, a virtual Infrastructure as a Service platform, is developed by Krystal, one of the largest independent UK web hosting companies. The solution we've built with them is a high-performance storage system with an extremely high level of data protection offered from its triple data replication.

DW: *We've saved the best until last(!) – StorPool won the SDC Awards 2021 Storage Transformation Project of the Year, it would be great if you can talk us through the winning project?*

StorPool won the Storage Transformation Project of the Year on the SDC Awards 2021 for the project "Dustin Group replaces VMware and Hyper-V with a New-Age IT Stack powered by StorPool". It was a pleasure to receive this award. Behind this project lays a ton of work and dedication from StorPool and Dustin's teams. The main objective of this project was to build an efficient cloud platform that meets the changing needs of Dustin's customers. Over time the company acquired multiple IT platforms that had become too large, complex, and expensive to manage efficiently. They needed to consolidate their various hardware and software platforms, streamline their operating expenses by eliminating IT management overhead and remove the previous limitations.

Dustin selected StorPool Storage for their primary and secondary block storage needs. OpenNebula was their choice for the cloud management platform, running the KVM hypervisor. The migration to StorPool gave them increased flexibility of their platform and the freedom to address faster the market dynamics and the challenges of tomorrow.

DW: *Any final thoughts or comments?*

As final thoughts, I can say we're not stopping now, that's for sure. In the future, we will conquer many more peaks. We have ambitious goals which will make us grow, become even better, and excel in what we do. We will continue developing our product to meet the market's growing needs and continue to provide storage services with 100% customer satisfaction.

For more information about how StorPool helps cloud builders to create simpler, smarter and more efficient clouds, interested companies can submit their information at https://storpool.com/get-started.

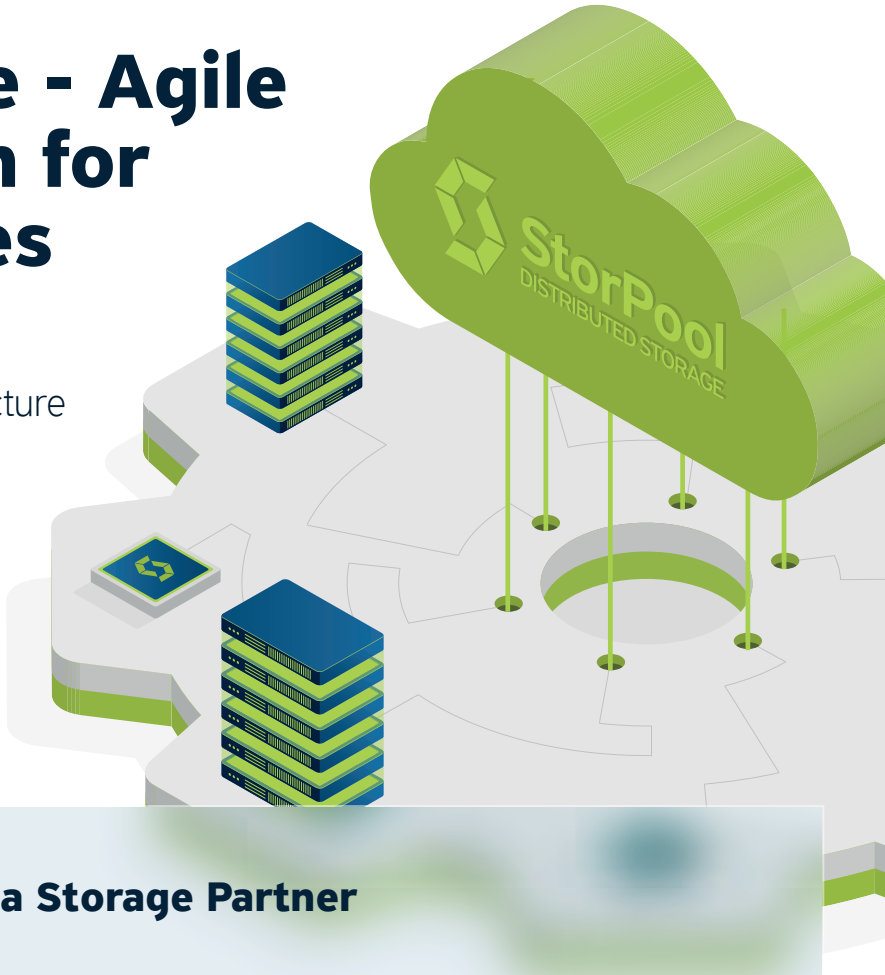
StorPool
DISTRIBUTED STORAGE

www.storpool.com/msp-storage

StorPool Storage - Agile Storage Platform for Managed Services Providers

The ideal foundation for cloud infrastructure serving the primary workloads of SMBs and Enterprises.

- Build powerful and robust clouds for your users.
- Retain control over your cloud infrastructure and ease the load on your people.
- Simplify your cloud Infrastructure and streamline your IT operations.



Your Data Storage Partner

Architect

We help you select the ideal architecture for your cloud at the physical, network, and logical levels, using only standard hardware.

Deploy

We install StorPool Storage in your servers and connect your storage system to one or more Cloud Management Platforms.

Fine-Tune

We analyse and tune your StorPool Storage system so that it runs optimally and reliably for your customers' workloads.

Monitor

We monitor hundreds of metrics per second to proactively open support tickets and deal with any issues that arise.

Maintain

We ensure that your storage system always runs optimally by installing non-disruptive updates and adding servers when needed.

StorPool Storage helps you get your data in order. It enables you to deploy and grow reliable, agile, speedy, and cost-effective clouds that meet the needs of your users. Bring your data home using the technologies you need, and pay as you grow – with no fixed term commitments.

Elevate Your Cloud by Building a Reliable and Speedy Storage Foundation!

Get Started

www.storpool.com/msp-storage | +44 (0) 20 7097 8536 | info@storpool.com

Minimising the impact of infobesity in today's digital workplace

EMMANUEL HELBERT, MANAGER INNOVATION, ALCATEL-LUCENT ENTERPRISE, has more than 25 years of experience in the Telecommunication industry. In charge of managing innovation, he's developing an innovative mindset within ALE while multiplying inspiring collaborations. He deeply believes that creativity comes from mixing talent and culture and that co-creation is the main engine for disruptive innovation.

OVER THE LAST TWO YEARS, most of us saw for ourselves the benefits of a digitalised workplace. Government-enforced lockdown measures, requiring people to work remotely in a bid to stem the spread of COVID-19, highlighted the importance of cloud services in supporting business continuity while allowing the workforce to remain safely at home.

A remote or, at least, hybrid approach to working is likely to remain the dominant model for the foreseeable future. A recent survey found that 79 percent of the C-suite would permit their employees to split their time between remote working and the corporate office if their job allowed it. And so attractive is the appeal of this new way of working that, according to another survey, a third of remote workers said they'd consider leaving their job if required to return to the office full time.

The benefits of a digitalised business don't come without costs, however. The associated data, generated by multiple users across multiple platforms, can be incredibly useful for informing business decisions. But it can also prove overwhelming, and threaten to counteract a company's efforts towards productivity. This is "infobesity", an issue that needs to be tackled now, before it irrevocably impacts the mood and efficiency of the workforce.

The digital workplace

As we emerge from the worst of the pandemic, remote and hybrid working are here to stay. With this comes the need for organisations to review both their existing operations and those measures introduced as an emergency during lockdown, to ensure they are robust, secure, and meet the needs of the business, its employees, and its customers.

This includes a shift from traditional location-centric operations to a more human-centric model, effectively moving toward the ideal of a digital workplace. Cloud services, in conjunction with a fast, resilient, high-bandwidth network infrastructure, will enable any service, anywhere, at any time. Not only is this essential for new working practices but, in a world where customer experience matters more than ever, the resultant, a more data-centric culture, will enable organisations to make more

informed decisions, and put their customers at the heart of their own journeys. But with the digitalisation of business comes a wealth of associated data. A decentralised workforce, accessing multiple applications on a variety of different devices, will cause an increase both in the volume and the type of data being generated. And this can lead to infobesity, a data and information overload so significant that it can be difficult for employees to process.

Introducing infobesity

Sharing information can, of course, be incredibly useful for informing business decisions, driving efficiencies, and improving customer experience. At the same time, though, an over-abundance of information can have an impact on a company's employees: it can reduce work output, lessen human interaction, and negatively affect the company culture.

Sharing information can, of course, be incredibly useful for informing business decisions, driving efficiencies, and improving customer experience. At the same time, though, an over-abundance of information can have an impact on a company's employees: it can reduce work output, lessen human interaction, and negatively affect the company culture

It can actually lead to a fall in productivity, for example, as people become more concerned with making sense of the data that informs a decision rather than the decision itself and its consequences for the business. And an increased focus on analysing and making sense of the sheer volume of data that can flow through a digital business can also have an adverse impact on the quality of interactions between teammates – whether face-to-face in the office or virtually.

Indeed, with more interactions taking place through the cloud, there's a growing risk that any historic sense of team spirit may soon be lost. This is particularly true of a digitally collaborative workplace. Although the ability to share more information than ever can deliver greater efficiency and effectiveness, it simultaneously pushes real human relationships into the background. There are environmental considerations, too.

According to a recent report from IDC, the amount of digital data created over the next five years will be greater than twice the amount of data created since the advent of digital storage. Storing this in data centres will no longer be viable, though. According to the International Energy Agency (IEA), data centres account for around one percent of global electricity demand, contributing to 0.3 percent of all global CO2 emissions. And, while this may not seem particularly high, predictive models suggest that data centre energy usage in some countries could rise as high as 15 to 30 percent of total domestic electricity consumption. It's clear, then, that fighting the effects of infobesity – on productivity, on culture, and on the environment – is one of the key challenges of today's digital workplace.

Exploring solutions

Recent technological developments like 5G and cloud form the backbone of the infrastructure that's responsible for infobesity. Importantly, though, they also support the technologies that will enable us to tackle it. Technologies such as AI, augmented and virtual reality (AR/VR), and edge computing are all examples of solutions we need to consider as part of our fight against infobesity.

AI and machine learning algorithms, for instance, will help ease the burden of analysing the vast – and growing – volume of data, while edge computing will improve the speed and efficiency of managing that data, while reducing the reliance on energy-hungry data centres. And, by enabling more direct and effective collaboration between employees, regardless of their location, AR and VR will go some way to re-establishing that much needed human connection.

Businesses need to focus on implementing better "digital hygiene" as well. Consider the fact that there's nothing stopping you from eating chocolate whenever you want. But, by learning how to eat it sparingly, you'll appreciate it more. It's the same with data. There's really no need for a business to acquire as much as data as it can, just because it can. Instead, thought should be given to what data is actually needed to inform important decisions and focus on collecting and analysing only that. Those decisions will still be supported, but with the involvement of far fewer resources.

The digital workplace is a reality. It's essential for the world in which we live and work today. But businesses need to be mindful of the risk of infobesity, and ensure they take steps to minimise the effects an over-reliance on an over-abundance of information can have on its productivity, its employees' wellbeing, and its environmental footprint.

Driving smart cities with edge analytics

One of the biggest catalysts in the adoption of edge computing is smart city development. With that, comes growth along with mountains of data and the needed for expanded networks to handle this data efficiently. Look, for example, at the LIDAR sensor on an autonomous car. This sensor can generate over 10TB/day, making the time window for sending such data back to a remote centre or server no longer practical.

BY NEIL STOBART, VP GLOBAL SYSTEMS ENGINEERING, CLOUDIAN

SMART INFRASTRUCTURE requires near-instant data processing for it to enable effective and timely decision making. As a result, the legacy model of moving data to a central hub to be processed isn't going to work with an expanded edge. However, with portable microservices, virtual environments, and a distributed computing platform, this model can be flipped to move compute to where the data resides. Developers can use technology such as Kubernetes to co-locate AI processing and data management together on a common hardware platform, thereby delivering low latency and minimising the physical equipment required.

From there, edge devices can be linked to the core, allowing for the edge storage device to only store the data needed for immediate use. Recorded data can then be offloaded to a central data centre where the data is held for analysis. Taking the autonomous cars example, they need to process and store data at the edge to make real-time auto-pilot decisions. At the same time, that data can be shared with other data sources at a central location enabling efficient data archiving, combined ML model training, and further collective analysis.

Moving compute to the data

All of this is what makes edge analytics so important in smart city development. By analysing data at the edge, information that's not essential for immediate decision making can be fed back to a central hub, allowing for the edge computing to focus on the more critical data. With traffic management systems, continuous streams of data can be stored centrally

and analysed for ML training. This ML model can then be applied to the edge application through updates at regular intervals.

Edge processors should be used as additive and complementary to a networked central hub – it can't be all edge or all hub. Working at the edge is best for local decision-making, needed instantly, such as filtering data and implementing decisions. Hub processing is better for more large-scale and detailed analysis such as training an ML model and long-term, archival storage for compliance purposes. Another great example of smart city applications is automated waste management. Rather than the usual pre-planned schedule collections, sensors can track waste levels in public litter bins or even across entire residential neighbourhoods. In this scenario, local authorities and waste management providers are alerted when waste levels meet the criteria for collection. Companies are able to better manage collection times, reduce unnecessary trips and operate more sustainably.

In this scenario data collected from long-term monitoring can be used to train new ML models, which are then applied to the applications at the edge. These regular updates help improve the waste monitoring, ensuring alerts are only set at the most optimum time. There is the added benefit that these "smart bins" can sense when there has been increased footfall around them and call for a preemptive collection.

To summarise, rather than a move to the cloud, real-time analytics demands a move to the edge, pulling compute to the data. With the proliferation of data sources at the edge generating continuous, high volume data, edge processors need to be integrated with hubs/clouds to form this hybrid architecture of a well-connected edge and centre.

Predict the future

One of the aspects of edge analytics that isn't as highly discussed is the additional security benefits. Many early IoT devices have struggled with automating security patches. Early developers never imagined that a permanently connected appliance would be the perfect launching ground for distributed denial of service attacks.

As we've seen over the last few years though, anything and everything is a target for hackers. Whether it be cars or water treatment systems, nothing is off limits. This is why some organisations are starting to adopt anomaly-detection algorithms to identify new threats sooner. These applications analyse large quantities of data at a central hub, spotting patterns, identifying new faults and developing new rulesets to run at the edge.

For smart cities to benefit the public who live within them, they need to react quickly to changing conditions. Edge applications need to be able to spot anomalies before they fully develop and react accordingly. In the case of traffic management systems this would manifest as the edge sensors spotting a broken down vehicle (the anomaly) and then making decisions near-instantly to divert traffic to less congested routes. All of the data taken in by the cameras during the incident could be offloaded and analysed centrally. The edge application would then be updated at a later time, making it possible to spot similar conditions earlier in the future and prevent disruption.

Rather than a move to the cloud, real-time analytics demands a move to the edge, pulling compute to the data. With the proliferation of data sources at the edge generating continuous, high volume data, edge processors need to be integrated with hubs/clouds to form this hybrid architecture of a well-connected edge and centre

Anomaly detection isn't just for the minute-by-minute situations. Vibrations and noise pollution can cause severe problems for buildings in built up urban environments, leading to structural damage, costly repairs and disruption to homes and businesses. Placing a series of accelerometers throughout a building in busy city centres allows structural engineers to monitor the effects of passing heavy goods vehicles, public transport and outdoor events, which can be tracked in real time. In the longer term, these vibrations, impacts and effects can be modelled by architects, quantity surveyors and development planners to better understand the strain placed on buildings when developing new real estate.

What Next?

Edge computing is still a work in progress, but with smarter deployment it could become the norm very soon. The first wave of digital transformation using the edge helped IT-focused companies gain a competitive edge. The next wave will extend existing development practices, applications, and data models to the edge to help accelerate the digital transformation for smart cities.

Out with the old and in with the new

The shift towards a more modern future.

BY CHRIS HARRIS, VICE PRESIDENT, FIELD ENGINEERING AT COUCHBASE

THE INCREASED PRESSURE following on from the pandemic means developers must ensure that they are equipped to meet the demands of today's digital-first world. However, this doesn't come without its challenges.

Many organisations still heavily rely on ageing legacy technology that isn't built to accommodate the requirements of modern businesses, as they fear the cost and complexity of updating their systems. Some also still have an attitude of "if it ain't broke, don't fix it" – but this can land them in hot water. If outdated systems are not upgraded, organisations will lag behind in their digital transformation projects, losing out on business value and potential revenue streams.

Legacy belongs in the past

Most organisations were built on a foundation of legacy technology, and it can be tough to part with these tried and tested applications. Take databases, for example. It is well understood that legacy systems and infrastructure are holding back digital transformation initiatives – and legacy databases are one of the largest constraints to innovation. In fact, recent Couchbase research found that 61 percent of digital architects reported past technology decisions made completing digital transformation projects more difficult – in particular, cloud infrastructure (48%) and database (43%) decisions.

Traditional relational databases (RDBMS) were built in the 1980s and reflect the infrastructure reality of those times. While they perform very well for their core functions, they were not built with the cloud in mind, often lack mobile compatibility, have high maintenance costs, and can be inflexible. These legacy databases can be a major setback as they are not suited to modern-day business processes.

The needs of a modern organisation have now stretched beyond what legacy databases have to offer. Although relational databases have the familiarity and comfort of old legacy technology, architects are aware that their days are numbered. According to a recent survey, 79 percent of organisations are currently actively planning to reduce their reliance on relational databases –

showing that the relational vs. NoSQL debate is very close to being over, once and for all.

The way forward

The perfect scenario to fix this problem is adopting technology that is as familiar as legacy, but brings all the benefits of modern infrastructure. Turning back to the database example, it won't be difficult to convince developers of the benefits of modern databases – the challenge is making it as easy as possible for them to transfer their skills from one technology to the other (64 percent of organizations are locked into using legacy technology because they have invested heavily in the relevant skills, while the same percentage say legacy databases hold their systems of record).

This is where NoSQL steps in. The right NoSQL database can operate on the same principles as a legacy database, offering the familiar concepts of relational databases on a more modern system.

IT teams now do not have to immediately adapt to new technology that requires a completely different skillset. This minimises the need for investment in new training for developers, as this technology complements their existing skills – therefore saving organisations time, resources, and money. Crucially, it is now easier than ever for developers to migrate their monolithic applications of the past into modern microservices that meet the current and future demands of a modern organisation.Developers can now use modern NoSQL databases to step away from legacy and gain better performance, flexibility, and scalability – without having to compromise on any of their needs. NoSQL systems are designed to be reliable and perform at scale, enabling developers to quickly build new applications and meet the needs of a modern digital business.

Making the transition

Databases play a key part in supporting the development of digital initiatives, and this is all the more important given the increased pace of digital transformation during the pandemic. Against this backdrop, we are likely to see the trend for widespread adoption of NoSQL databases continue over the next few years. While casting off the shackles of legacy databases may once have been a difficult task, the switch from relational to NoSQL can be a cleaner transition as organisations are now able to make technical improvements while still utilising their developers' current skill sets.

While it doesn't take much to convince developers of the benefits of NoSQL, the debate between relational vs. NoSQL is slowly coming to an end. Organisations must now bite the bullet and upgrade their ageing infrastructure – leaving relational back in the 1980s where it belongs.

Data mesh:
How businesses can get ahead

In our digital age, every business is striving to become more data-driven. The rapid growth in data has brought with it the potential for exploitation but it is a 'double-edged' sword for many businesses, as it also brings greater complexity, especially when it comes to the challenges associated with aggregating data from different sources.

BY CHARLES SOUTHWOOD, REGIONAL VP AT DENODO

It is not only the volume of data that has grown over the years; it is also the variety, with an ever-increasing number of data lakes, applications and other sources, all with different formats and protocols. Some of these sources are huge. Clickstream data, IoT data, or even human-generated data - including inbound emails, webchat and social network messages – it's a stream that keeps on flowing. Needless to say, it's also a lot to keep on top of.

This data is being curated into multiple data stores and applications, some of them on-premise and some in the cloud, or in multiple clouds. With different business needs, the storage of analytics data is often spread across a variety of different platforms, often with similar or overlapping content. This results in different analytical workloads running on different analytical systems, typically creating

Data mesh is emerging as a new hope for organisations looking to truly understand and utilise their data. It aims to remove bottlenecks and take data decisions closer to those who understand the data. It proposes a unified infrastructure enabling domains to create and share data products, while enforcing standards for interoperability, quality, governance, and security

silos. The same data is repeatedly extracted, cleaned and transformed in each silo, resulting in delays and bottlenecks for multiple teams. As a result, the demand for real-time streaming, democratisation and scalability is simply not being met.

The future of data architecture

Data mesh is emerging as a new hope for organisations looking to truly understand and utilise their data. It aims to remove bottlenecks and take data decisions closer to those who understand the data. It proposes a unified infrastructure enabling domains to create and share data products, while enforcing standards for interoperability, quality, governance, and security.

At the core of this philosophy is a distributed model where each organisational unit – or "domain"- has its own data product owners. This allows the company to achieve greater analytical velocity and scale. This is because domains have a better understanding of how their data should be used, which results in fewer iterations until business needs are met as well as higher quality results.

Instead of being a by-product, data becomes a decentralised, self-contained product that can be consumed by anyone in the organisation. This also removes the bottleneck of the centralised infrastructure and gives domains autonomy to use the best tools for their situation.

There is no doubt that data mesh is the future of data architecture. But how can organisations ensure that they are ready to implement and embrace it?

No 'mesh'ing around with data virtualisation

Once an organisation decides that data mesh is the way forward, its IT leaders then need to decide which technologies can be utilised to help implement it. Data virtualisation is a great candidate because it has been specifically designed to provide a unified, governed, and secure data layer on top of multiple distributed data systems.

It does this through creating virtual models on top of any data source. These virtual models implement a semantic layer, exposing all data in a business-friendly form while decoupling consumers from complexities such as the data location and native source formats. Thanks to the simplicity of use and the minimisation of data replication enabled by data virtualisation, the creation of data products is much faster than using traditional alternatives.

In the advanced solutions on the market, data products can be made accessible through any method such as SQL, REST, OData, GraphQL, or MDX, without the developer needing to write any code. Data products can also be automatically registered in a global, company-wide data catalog that acts like a data marketplace for the business.

Data virtualisation also ticks the box when it comes to governance. Not only does it reduce data duplication and provide a single point of access, but its virtual layer also enables organisations to automate the enforcement of global security policies. For example, leadership teams can mask the salary data in all data products unless the user has a certain HR role or is at a certain level within the business.

There's no doubt that data mesh offers a new and unique environment to support decision-making and analytics systems. Its focus on delivering, managing, and using data to minimise silos, avoid duplication and ensure consistency will remove the bottlenecks that have plagued organisations for decades. Supporting this architecture with modern technologies, such as data virtualisation will enable businesses to take their operations to the next level and truly maximise their data's potential.

Continuous actionable intelligence through real-time data analytics

Organisations across every industry are seeking to extract greater insights from their data. Whether it's to improve operational performance, outpace competition or change business models entirely. A deeper understanding of data generates the business intelligence to drive fast, successful change.

BY JAMES CORCORAN, SENIOR VICE PRESIDENT OF ENGINEERING, KX

THIS PACE of change is being forced through by two key factors: the exponential growth in data volumes and the speed at which that data enters organisations. Particularly real-time data from devices and sensors often at the edge of networks. In 2020, nearly all businesses (97%) saw an increase in the volume and variety of data entering their business, driven by the explosion of sensors and the accelerated digital transformation of all industry sectors.

Research has also shown that organisations across all sectors recognise the importance of extracting more insight and intelligence from their real-time data. 90% of businesses plan to increase investment in data analytics technologies over the next three years. In addition, there is a growing post-Covid demand for greater automated decision-making as part of digital transformation initiatives. It's not hard to see why Gartner is forecasting that by 2022, most business systems will feature real-time data capabilities.

Insights on and off the track

Much can be learnt from the experience of companies in the Financial Services sector in order to understand the transformative potential of real-time analytics. Banks, hedge funds, exchanges and regulators have long relied on technologies that enable sub-second decision making for a range of

use cases from optimising trades to identifying and mitigating crime.

Although the datasets may be different, any scenario where big data meets fast data is an opportunity for businesses to benefit from the introduction or enhanced application of real-time analytics. For example, in the automotive industry; from processing edge data from sensors in autonomous vehicles to analysing trackside telemetry and aerodynamics in wind tunnels in motorsports, real-time data analytics is a game changer. Both for enabling new technologies and services and significantly enhancing existing processes.

There are many similar use cases in industries as diverse as marketing, manufacturing, utilities and telecommunications. As the volume, variety and velocity of data continues to increase, so does the need for technologies that can unlock the value of data in real-time, using the context of historical time-series data to capitalise on perishable business moments.

Fast data

The demand for ultra-high-performance analytics is giving rise to a new 'fast data' layer within the wider data management and analytics architecture. In this layer, the best in class real-time decisioning engines can augment the storage and batch analytical capabilities of partner technologies, including those offered by the hyperscale cloud vendors and sector-focused platform providers.

Whether deployed on-cloud, on prem or in a hybrid model, these fast-data solutions enable companies to add deep and wide historical data as context to inform their real-time decision making. These also tend to be simple to deploy and manage, and so are appealing to businesses struggling to make legacy data management and analytics systems fit for purpose when faced with the realities of their ever-growing data landscape.

Continuous actionable intelligence

Ultimately, combining ultra-high performance analytics with time-series data means companies can build a model of Continuous Actionable Intelligence (CAI). This is where artificial intelligence (AI) and machine learning models are applied to real-time and historical data to deliver greater automation of business processes and decisions.

In addition to significantly improving operational efficiency, CAI offers the promise of both solving previously unseen business problems and unearthing new opportunities, providing companies have the right talent with the relevant skills to build and promote the data models.

Across all industries, many organisations are struggling with having access to the right people with experience in DataOps and machine learning. By getting this right, companies can experience the genuinely transformative results that these technologies offer.

Chief Data Analytics Officers: The key to data-driven success?

The role of a CDAO and their importance in ensuring an organisation's success.

BY TERADATA EMEA'S FINANCIAL SERVICES INDUSTRY CONSULTING LEAD, SIMON AXON

BANKS were among the pioneers of the new role of Chief Data Officer in the early 21st century, yet the role remains hard to define and under-utilized. Nearly 64 percent of financial services organisations claim to have a CDO, but 72 percent of organisations still feel that it is an unsettled role. Getting it right can accelerate your data strategy and help save the bank of the future from the clutches of Big Tech.

In many banks they started out as a data policy wonk in the IT team, responsible for writing rules to manage data quality. They had little power and no budget and were certainly not connected to wider business decision-making. At leading banks however, they are now evolving to become powerful champions of data strategy with wide purview and a seat at the top table.

The best, now often called Chief Data and Analytics Officers, are change agents, working closely with functions across the bank to make data less scary and more useful. They play a multi-faceted role as evangelists, teachers, sages and enforcers focused on ensuring the organisation gets the best value from its data. They lead teams of data scientists and ensure they are integrated and aligned with the business. A good CDAO should be the right arm to the CEO as they deliver a data strategy. Given the right responsibility and budget, they can quickly become a vital strategic partner for the business.

Core to the role is the experience and desire to use data to solve real business problems. Combining an overarching view of the data across the organisation, with a well-articulated data strategy, the CDAO is uniquely placed to balance specific needs for data against wider corporate goals.

They should be laser-focused on extracting value from the bank's data assets and 'connecting-the-dots' for others. By seeing and effectively communicating the links between different data and understanding how it can be combined to deliver business benefit, the CDAO does what no other role can do: bring the right data from across the business, plus the expertise of data scientists, to bear on every opportunity.

Balance is critical. Leveraging their understanding of analytics and data quality, the CDAO can bring confidence to business leaders afraid to engage with data. They understand governance, and so can police which data can be used for innovation and which is business critical and 'untouchable.'

They can deploy and manage data scientists to ensure they are focused on real business issues not pet analytics projects. Innovation-focused CDAOs will actively look for ways to generate returns on data assets, and to partner with commercial units to create new revenue from data insights.

The CDAOs are the catalysts that turn the theory of a data-driven bank into reality. Having set the vision, developed the data strategy and roadmap, the CEO should look to the CDAO to operationalize it. To be effective CDAOs need power and budgets, and this means executive sponsors at the highest levels. As the hinge-point between strategy and execution, and between board and business, a good CDAO will quickly become indispensable across functions and business units.

Chief Financial Officers may be the most effective board sponsors for the CDAO since, as they share an enterprise-wide view of assets. But chief marketing officers and chief risk officers will also come to rely on the CDAO as the data strategy is operationalised across the organisation. Making the right decisions now to set up CDAOs to succeed in the bank of the future, getting them onside, invested, empowered and incentivised as evangelists and facilitators of data driven innovation, will accelerate growth and effective defence against Big Tech encroachment.

Financial Markets Network

Global Connectivity Throughout the Trade Lifecycle

Worldwide Data Connectivity

Cloud Computing

Infrastructure

www.ipc.com

Designing data centres for MSPs and IT service providers

Since the start of the pandemic, the Managed Service Provider (MSP) and IT Service Provider marketplace have radically changed. As the post-pandemic business landscape begins to take shape, it's critical for MSPs and ISPs to choose the right data centre partner to support growth.

BY AMY YOUNG, SALES DIRECTOR AT CUSTODIAN DATA CENTRES

AS MANY BUSINESSES begin to re-draw their digital transformation roadmaps in the wake of Covid-19, today's end-users are looking to evolve how they structure their IT services, and more critically, streamline whom they buy these services from. For the MSPs and ISPs responsible for such digital strategies, agile, resilient and secure data centre capacity is crucial – especially for those delivering disaster recovery, business continuity and cloud services. Here, the role of the data centre operator is, in many respects, simple but critical. Their primary requirement is to deliver power, cooling, connectivity, and secure physical infrastructure to support MSP service delivery.

Challenges in the face of digital transformation

In recent years much has changed. MSPs and ISPs are faced with a host of challenges, including the need to keep pace with the speed of constant technological change. There's also a highly competitive marketplace to contend with, where often vendors and other service providers, even those that a business is partnered with, can compete on the same tenders.

Other challenges include the need for greater resilience of the IT facet and thereby increased levels of due diligence, where customers will want to see their whitespace before signing contractual agreements. Finally, with accelerated digital transformation, there is a need to future proof while meeting strict SLAs regarding data, security, and uptime.

The role of the data centre operator has, therefore, become even more critical for MSPs and ISPs planning to scale and grow. And with more end-users now looking to their external suppliers as trusted advisors, in-house technical expertise, agile critical infrastructure and dynamic service have become key differentiators for those providers in the channel.

Digital architectures are changing According to research from Accenture, over three-quarters (77%) of executives state that their technology architecture is becoming critical to the overall success of their organisation.

One key area of growth for all MSPs is digital security, and research from Datto into the impact COVID-19 found 84% of MSPs report advanced endpoint security, data loss protection (79%) and password management policies (72%) as the most requested services by their customers. Having a partner that specialises in state-of-the-art physical infrastructure and security is vital for MSPs, and will likely form a major component of their services, especially those around zero trust approaches to data security.

Research from Gartner also states that by 2025, 85% of infrastructure strategies will integrate on-premises, colocation, cloud and edge delivery options, compared with 20% in 2020. This dramatic shift in IT infrastructure is redefining how MSPs are delivering end-user services.

Mission-critical IT, whether deployed on-premises, hosted in a colo, or indeed at the edge of the network is, therefore, paramount for end-user digital transformation. Now, as more MSPs and IT Service Providers are called upon to expand their service portfolios with capacity for AI, machine learning and edge infrastructure, all of which require integration with cloud services, the support of specialist colocation providers have become vital. But what are the considerations for choosing a colo?

Key considerations for outsourcing

As with any service provider, cost is a key aspect of the decision-making process. MSPs cannot, however, put a price on reputation, so reliability, connectivity, security, and efficiency all play important factors. Efficiency, especially in the form of power usage, can be critical, and the more energy efficient a data centre provider can be, the lower the total cost of ownership (TCO) for the user. A data centre provider with a lower PUE can provide a cost-effective and scalable platform to support MSP growth, something highly appealing where cost and consolidation are influential.

Diverse connectivity and low latency are also determining factors, and MSPs will often seek out carrier-neutral colocation providers who have access to dark fibre rings, 100Gb wavelengths, and who can deliver enterprise-level connectivity solutions. Many end-users are moving towards hybrid IT environments with a mix of on-premise infrastructure and cloud, so real-time access to data and application availability are indeed business-critical.

Size, in terms of scalability, alongside physical security and customer experience, are also crucial. Many MSPs are looking to partner with operators that have a demonstrable track record in supporting their key customer demographics. Further, with human error, network, and power failures key causes of outages there is also a need to meet strict compliance and regulatory standards, and to provide policies for zero downtime. For any service provider, it pays to have a data centre partner who can consistently meet strict SLAs.

Finally, speed of deployment and dynamic service is crucial. Any Managed Service or IT Service Provider will tell you that adding value, or the having ability to go the extra mile, can be the very difference between a customer renewing their service agreement or migrating to another provider. The trust that a data centre operator can act as an extension of your team, can understand complex infrastructure deployments, or who can meet strict timescales, especially where speed of installation, security and operational reliability are concerned.

The need for new partnerships

As the business landscape continues to change, so have the ways in which data centres are looking to support the MSP and ISP communities. Cost predictability is always a key factor, but so too are the pressing needs to consider technical competence, alongside environmental factors - especially as sustainability moves to the top of the business agenda.

In the wake of Covid-19, MSPs are looking to their data centre providers as trusted advisors, and often, as an extension of their technical or sales teams. The right operator can help an MSP win business, answer complex technical questions, and instil confidence in the end-user at every stage of the journey.

Further, transactional relationships have become a thing of the past, and long-term collaboration has become a focal point of business discussions. As such, many MSPs are looking for providers that can support their growth across different geographical regions and can continue to do so in a low cost and environmentally sustainable way.

Finally, trust and transparency are vital, especially in a channel where tenders are often taken in-house, and where partners can find out that they are competing on the same bids. In essence, by partnering with a data centre operator that focuses solely on colocation, and without its own services division, MSPs can avoid many of the complications associated with challenging tender processes, while developing mutually beneficial relationships that are designed to support long-term growth.

At Custodian we're dedicated to setting a new standard in dynamic, multi-site colocation services. Our agile-mission-critical data centres have been expertly designed to underpin MSP and IT Service provider growth - combining expert technical insight with unparalleled customer service and a reputation for industry-leading uptime. We believe that in the era of digital transformation, MSPs deserve a new kind of partner that can help them diversify and grow, and we are committed to making that vision a reality.

The importance of digitalisation in the aviation industry's recovery

NIELS STEENSTRUP, SENIOR VICE PRESIDENT OF INMARSAT AVIATION, discusses the significant role digital technology is going to play in the recovery of the aviation industry following the pandemic

PREDICTING THE FUTURE can be a foolhardy business at the best of times. With that in mind, some might shy away from making forecasts at the tail end – we hope – of the worst global pandemic in living memory.

However, when it comes to the recovery of the aviation industry – a sector, lest we forget, that has been among the hardest hit by the fallout from COVID-19 – it is clear that digitalisation will not only be crucial to aviation's rebound, but a catalyst for it. This is stated without the whisperings of a soothsayer or a crystal ball, but by listening to the insights of many of the industry's leading experts, who can all agree on one thing.

Digitalisation will enable a whole suite of connected services on-board, services reliant on predictable, resilient and seamless high-speed inflight broadband. This will help airlines rebuild passenger confidence, and is also central to the safe, sustainable and profitable recovery of the aviation industry.

At our recent FlightPlan: C-Suite Week broadcast, the CEOs of Qatar Airways, AirAsia, United Airlines and TAP Air Portugal, plus the Director General of aviation trade body International Air Transport Association (IATA), all echoed this point: digitalisation is critical to aviation's future evolution. But it's not only business leaders and thought leaders who know what digitalisation can bring. Passengers want it too, after more than a year of living our lives online. In our latest Passenger Confidence Tracker, a common theme was that digital technology is helping to rebuild much-needed passenger confidence.

Connectivity meets passenger needs

Clearly the pandemic didn't herald the start of society's digital transformation. That has been underway since the end of the last century. But analysts believe that during 2020's first lockdown we witnessed three years of digital transformation in just three months – at home and work.

This newfound desire to remain constantly connected – with family, friends or just keeping pace with rapidly changing world events – is just as applicable, perhaps even more so, when looking at passengers returning to the skies. Connected technologies will allay passengers' concerns, and demonstrate that airlines appreciate the 'new normal', giving them confidence in travelling again.

This much is apparent from the results of our Passenger Confidence Tracker 2021, which demonstrated that confidence in air travel is rising, with 60% of passengers feeling happy to fly by the end of this year, compared to 47% in 2020.

In order to maintain and even accelerate this, passengers' confidence and evolving needs are met in a post-COVID world. And this is where digitalisation

comes in. Globally, travel factors underpinned by digital technology such as pre-flight COVID testing (56%), digital health passports (47%), thermal scanning (42%) were cited by passengers as improving confidence – and in turn passenger experience, another key metric to consider.

Inflight connectivity (IFC), then, is one way to enhance the onboard experience and improve confidence in the future. Airlines that neglect digitalisation may very well miss out as more and more passengers return.

The platform to unlock IFC

So, if passengers want a connected experience while in the air and airlines want to meet these expectations, what technologies are needed to realise the full potential of inflight connectivity?

Innovative customer experience platforms will allow airlines to offer a rich airline-branded digital platform to enhance and personalise the passenger experience onboard flights. They act as a one-stop shop for passenger experience – a smart, customer-centric platform that brings together a host of inflight services and partners in one place, delivered straight to passengers' own devices.

In practice, passengers will be able to order food and beverages, receive the latest flight and destination information, sign-up to the airline's frequent flyer programmes, browse the internet, stream videos, shop online and enjoy other ecommerce offerings, all in real-time from the comfort of their seat.

Not only will these platforms transform passengers' digital inflight experience, they will also enable airlines to finally monetise IFC by allowing airlines to offer Wi-Fi free-of-charge through sponsorship and advertising features – a real commercial opportunity for airlines.

And in an age where brand differentiation is key, these platforms, such as Inmarsat's OneFi, allow airlines to completely customise the portal, enabling them to gain a critical competitive advantage in the marketplace.

Digitalisation central to airlines' recovery strategies

The full digital experience is no longer just a buzzword, but a reality that airlines need to offer and embrace. The pandemic had brought the worth of customer experience front of mind when it came to recovery strategies, and technology is a major part of this. Recognising this, many airlines have used the downtime of the pandemic to invest in new solutions.

We know that top airline executives are also in agreement about the importance of digitalisation – from Bluetooth and power points to the best Wi-Fi in the sky, Scott Kirby, CEO at United Airlines, agrees that digital services are essential to fostering a strong relationship between airline and passenger in the current climate. Digital technology is central to the airline's future plans, helping the airline not only run more efficiently, but create more customer-centric solutions too.

One way United is using technology to create a more innovative, passenger friendly airline is digital bag tracking – dubbed an Uber for bags on the ground – allowing United to monitor every bag's location at any one time.

We are also seeing this investment in technology at Air Asia, where digitalisation is a fundamental part of making the company more than an airline. Air Asia aims to be a travel company, using its massive customer database – encompassing services from currency to grocery delivery – to turn AirAsia customers on the plane into customers on the ground.

The time to act is now

So from helping improve passenger confidence to monetising the passenger experience, the importance of digitalisation in aviation's post-Covid recovery is there for all to see.

Passengers – in particular the digital natives of Gen Z who will make up a much greater proportion of flyers in the years to come – no longer see connectivity as a nice-to-have, but a necessity. Meeting, and hopefully exceeding, their expectations will not only boost those airlines that embrace digital transformation, but provide a timely shot-in-the-arm for an entire industry. Conversely, those airlines that fail to look ahead and invest in the right technologies won't be able to say they weren't warned – and will certainly struggle to compete.

Why AI is now table-stakes in cybersecurity

AI is an essential part of every modern cybersecurity solution. There's no other practical way to deal with the volumes of information that are now required to stop modern threats.

BY DR. SVEN KRASSER, SENIOR VICE PRESIDENT AND CHIEF SCIENTIST, CROWDSTRIKE

WHEN WE STRIDE DOWN the aisles at our local grocer, shelves are full of products vying for our attention. To make their way into our shopping carts, some tout their superior performance on their packaging, and some even try to back their claims up with some magical ingredient. Yet when the rubber meets the road, few of us expect a laundry detergent empowered by such a magical compound to truly get rid of all traces of stains from holiday cooking.

While the stakes may be high if our favorite pair of trousers is involved, they are surely higher when picking a security solution. In cybersecurity, most offerings tout some level of AI. Sometimes it's qualified further, such as an especially "deep" AI or a comfortingly "autonomous" one (which may or may not take care of your laundry, too).

What all the extra adjectives try to cover up is that AI is now the bread and butter of the security industry. And like with bread, we have a pretty good idea what's in it. In other words, at this point I would expect that the vast majority of security solutions have adopted AI. Why wouldn't they? It is easy to get started, and one can get to results quickly. But like with bread, both the quality of the ingredients and recipe for the process of making it determine the outcome.

Why is there so much interest in doing more with AI in the security industry? We are all still jaded

from the signature days. Back then, signatures got deployed, signatures started to miss new threats, humans wrote new signatures, and the cycle would restart on the next day. This is obviously a losing proposition -- not only is this approach purely reactive, its speed is indeed limited by human response time. This is specifically where AI has promise, detecting threats that have not even been conceived yet, without updates.

What does it take to train an AI model that can do such a feat reliably? First and foremost, it takes data. A lot of it. Cloud-based solutions have a clear advantage with their broad visibility of the threat landscape, allowing correlation of global observations across organizations and networks. To process such large amounts of data a lot more technology than just AI is needed – but once the data has been correlated, AI is a powerful tool to make sense of it. With AI, we can process more data at scale, and we can spot more complex relationships than a human mind can uncover.

More data allows us to spot fainter signals. Let's say you start plotting the latitude and longitude of European cities onto graph paper. Initially, you will see some randomly scattered points. But if you do this for a larger number of cities, the familiar shape of Europe will slowly emerge out of a cloud of points. This simply won't work if everyone has a "local" piece of graph paper to plot a handful of cities in their area. However, with a global view the combination of Cloud and AI really shines. None of this is possible on an appliance. And none of this is possible with hybrid cloud solutions, i.e., those clouds that are merely stacks of vendor-managed rack-mounted appliances.

Not all data is created equal. There is another type of data to which humans can contribute. We call this type of data ground truth, and it has a large impact on the training of AI models. Ground truth is the type of data that describes how we want an AI model to behave under certain input. When certain types of AI learn, they leverage ground truth as examples and learn to interpret other data based on these roots of knowledge -- this way of learning is called supervised learning.

Supervised learning is a powerful way to create highly accurate classification systems, i.e., systems that have high true positive rates (detecting threats reliably) and low false positive rates (rarely causing alarms on benign behavior). Not all learning needs to be conducted using ground truth (the domain of unsupervised learning is concerning itself with those other approaches). But as soon as it›s time to evaluate whether such an AI system works as intended, you will need ground truth, too.

Well-designed cybersecurity systems strive to maximize the generation of ground truth. For example, take a managed threat hunting service

such as Falcon Overwatch. Whenever a threat hunter discovers an adversary on a network, those findings become new ground truth. Similarly, when the threat hunting experts evaluate suspicious activity as benign, it is also added to the pool of ground truth. Note that this all happens independently of AI models stopping threats in real-time. Those new data points can then be used to train or to evaluate AI systems. Generating this kind of data at scale, every day, using the cloud as the vantage point allows for training better models. In other words, the AI system is getting better every day.

With so much opportunity and new technology allowing us to process more and more data, when will AI completely handle the security of our computing systems for us? Not in a while. Artificial intelligence is not, indeed, intelligent. Have a conversation with your smart speaker to reassure you of that fact. AI is a set of algorithms and techniques that often produce useful results. But sometimes they fail in odd and unintuitive ways. AI even has its own distinct attack surface that adversaries can leverage if left unprotected. Looking at it from another angle, if AI is such a powerful tool, could an AI outsmart another AI? The field of Adversarial Machine Learning concerns itself with that question, and the short answer is "yes." Ignoring these inherent risks and limitations by treating AI as the panacea fixing all woes of our industry is dangerous.

AI is, however, an essential part of every modern cybersecurity solution. There's no other practical way to deal with the volumes of information that are now required to stop modern threats. Those threats are driven by motivated adversaries with strong financial incentives that will not cease their attempts to evade detection. But the mere use of AI is not what makes a security solution superior. What matters most is what drives the AI: the breadth of data it consumes, the volume of that data, the ground truth it can leverage, and its human teachers.

Why cloud service providers need to get serious about MFA

Most of us are now familiar with a two-factor or multi-factor authentication (2FA/MFA) experience. It may be receiving an SMS one-time passcode (OTP), a push notification, or using biometrics to log into accounts. In Europe, PSD2's mandate for strong customer authentication (SCA) has certainly made 2FA ubiquitous when shopping online.

BY ANDREW SHIKIAR, EXECUTIVE DIRECTOR AT FIDO ALLIANCE

FINANCIAL SERVICES are not the only industry that needs to get smart about authentication. And, in 2021, we saw some of the world's biggest online consumer service providers make meaningful progress towards pushing their users to MFA, including:

- Google committed to requiring MFA for all G-Suite users
- Microsoft launched fully passwordless account options
- Twitter shared its data on 2FA adoption
- Facebook Protect launched and expanded globally
- Google gave away thousands of security keys to high-risk individuals

This is remarkable progress. The ineffectiveness and vulnerabilities of relying on passwords as an online security method is now widely reported on, but just a couple of years ago, this was standard practice.

MFA - even if on top of passwords – can protect users of any online service from a whole host of remote attacks. But it's not perfect, and there is still much work to be done from both the tech giants listed above and other consumer-centric cloud service providers (CSPs).

Here's four things CSPs should be thinking about right now:

1. More MFA mandates for consumers

Undeniably, the industry has moved from 'if' to 'when' for MFA adoption. But for consumers to change their behaviour, we know that requiring usage of MFA mandates will be key. Barring the few that are very tech-savvy, people are very unlikely to go out of their way to replace how they access accounts, especially if it means adding more friction.

We're seeing some traction towards requiring MFA. For example, it was great to see Meta expand Facebook Protect to more users and geographies in early December, which requires high-risk profiles to use MFA. Google similarly announced plans to require MFA for more and more of its users and is also offering free security keys to high-risk individuals. This is a great start, but for the online world to truly protect itself, we'll need to see more service providers follow suit - and for a larger segment of their customers.

2. Be transparent

This leads quite neatly into my next point. CSPs also need to be open about the state of MFA adoption. Last summer Twitter revealed its 2FA adoption figures and just 2.3% of accounts had this enabled. 80% of those used SMS-based backup which, for reasons I'll explain more shortly, is actually the least secure 2FA due to its susceptibility to hijacking and phishing attacks.

While the data itself is far from great, this level of transparency is outstanding as it provides a powerful benchmark for improvement and gives the industry a reality check that considerable work needs to be done to get consumers on board and more accounts protected. We'll be monitoring how Twitter's adoption rates evolve and hope to see more CSPs follow their admirable lead by opening up about the reality of 2FA adoption – ideally working together to help address the barriers to slow uptake.

3. The UX Factor

Moving away from legacy 2FA authentication is more than just a matter of security, too. The user experience offered by factors like SMS OTPs and push notifications is disruptive, laborious, and off-putting for consumers. eCommerce is one industry where it's clear the damage poor user-experience has on service usage and ultimately, a company bottom-line. Forrester suggests brands can lose over $18bn a year from cart abandonment, caused in large part by friction at the checkout authentication process.

For MFA to be fully embraced by consumers, it needs to be as seamless as possible - after all, hesitancy to deploy is largely a result of CSPs playing a balancing act between security and customer experience. Here again, possession-based authentication comes into its own. Biometrics and security keys are generally one-gesture, super-simple authentication methods, meaning users can achieve greater security without compromising the log-in experience.

4. Out with the old, in with the new

As Microsoft has documented, any form of MFA is better than a password alone to protect an account. However, not all 2FA is created equal. New 'toolkits' of malicious software are increasingly readily available online to work-around MFA (especially SMS OTPs), showing these types of attacks are not only more sophisticated, but more prolific. Many of these toolkits even have customer services support – yep, it's truly never been easier to be a hacker.

The truth is that any one-time passcode – whether from an SMS or an authentication app – is still a 'shared secret'. This means that they are still susceptible to hacker manipulation, intersection and replay attacks, and social engineering.

As such, it's time for CSPs to look beyond these 'legacy' authentication methods and optimise possession-based MFA. Think on-device biometrics or security keys: as these are protected by the robust hardware on-device and need to be with the consumer during authentication, these simply cannot be spoofed or compromised in the same way. The unrivalled security of possession-based MFA factors is why Google's Advanced Protection Program only supports FIDO Security Keys.

MFA's Holy Grail – the quest is on

The industry has come a long way in innovating upon and implementing MFA, but we can't stop here. As the MFA conversation moves from necessity and viability to tactics and timings, CSPs need to get serious about their authentication roadmap. Emphasis on tactics is going to be key, and we're going to see more really scrutinise how user-friendly and ubiquitous new authentication methods are.

Happily, most devices today – and virtually every device being unboxed as you read this – have built-in support for FIDO authentication. This means an un-phishable alternative to passwords is literally at the fingertips of billions worldwide.

For CSPs pushing to gain more widespread MFA adoption, taking advantage of built-in device capabilities might just make the journey easier than it seems.

Why securing data against threats is all about zero trust

Organisations are increasingly aware of the many cybersecurity threats they face, with the majority of conversation focusing on threats originating from outside the organisation.

BY ANDY WOOD, TECHNOLOGY STRATEGIST, CYBERSECURITY, NETAPP

RANSOMWARE continues and will continue to dominate this conversation, which is unsurprising given that IDC research suggests that over a third of businesses globally have fallen victim to some form of ransomware in 2021. Despite the tendency to focus on external threats from criminal gangs and nation states, it's important to remember is that cybersecurity threats can also come from within.

Insider threats are cyber-attacks caused by people within an organisation. They can be the result of attempted sabotage by former employees or contractors with an axe to grind. However, insider threats also include cyber breaches caused by negligence, human error, poor digital hygiene and a lack of awareness or training when it comes to cybersecurity. This is one of the reasons data security experts talk about the concept of zero trust. While we shouldn't rush to suspect that our colleagues are working against the business, measures need to be taken to protect ourselves from ourselves.

As well as a general rise in cyber-attacks and more diverse array of attack types, the increase in remote working we have seen over the past two years has

Zero trust is not a new concept. In fact, the term has been used for over a decade - initially developed by John Kindervag at Forrester Research. It describes adopting a view of networking security from the inside-out rather than the outside-in

generally made organisations more vulnerable to both external and insider threats.

Zero trust in a data security context

Zero trust is not a new concept. In fact, the term has been used for over a decade - initially developed by John Kindervag at Forrester Research. It describes adopting a view of networking security from the inside-out rather than the outside-in. The inside-out zero trust model comprises of a microcore and perimeter (MCAP). The concept of a security outer perimeter, therefore, becomes obsolete as insiders (employees) are already within the perimeter.
To counter the threats to zero trust employees, contactors and partners need appropriate controls for accessing data and an organisation's wider infrastructure.

The first step is identifying the locations where your organisation's data is situated, behavioural analytics can identify user behaviours and from that insight classifications and policies can be constructed. Secondly, data needs to be classified - in particular, toxic data that could pose compliance or reputational issues when it gains external exposure. Zero trust architectures can be frameworks for compliance, in addition to the security benefits.

After data is classified, some data may no longer be necessary and should be deleted due to the liabilities posed by unnecessary data. Advanced mechanisms should be used to cryptographically erase sensitive data. The principle of least privilege needs to then be applied by giving employees access to the data they need to perform their roles, using role-based access control which can be applied to both data and administrative access. Additionally, multi-factor authentication (MFA) is advised for both administrative and data access to prevent accounts from being compromised.

Furthermore, data should be encrypted both at rest when drives are changed and in flight when accessed by users. Data then needs to be monitored actively using behavioural analytics to alert for suspicious activity that is irregular and to deny access, if necessary. The steps listed above are necessary for a zero trust data-centric zero trust data-centric MCAP (microcore and perimeter) model to be adopted and to counter the threats posed by zero trust.

Time to implement zero trust

The business case for zero trust has arguably never been greater. According to IBM, the cost of a breach for organisations with a zero trust approach is £1.3 million less compared to organisations without one. Furthermore, Gartner has predicted 75% of organisations will be using containerised applications by 2022. So zero trust has taken on a new level of importance to organisations looking to mitigate security risks as data is transferred to the cloud.

It's clear that cybersecurity threats can come from both outside and inside the business. This means that organisations need to think differently about how to counter insider threats by adopting a zero trust framework to IT. With remote working here to stay, cloud use growing year on year, and data volumes increasing exponentially, the time to implement zero trust is now.

What to look for in a TIP

Five pointers for choosing a Threat Intelligence Platform

BY ANTHONY PERRIDGE, VP INTERNATIONAL, THREATQUOTIENT

AS 2022 gets under way and the new financial year looms, many companies are starting to identify the key strategic focus areas for the year ahead and the technology investments needed to deliver them. Given the aggressive cyber threat environment experienced over the past 18 months, cybersecurity investment is high on the list for many. Increasingly, organisations are building out their own Security Operations Centre (SOC), incident response capabilities and threat intelligence teams, as they aim to meet risk management and compliance demands and proactively defend the business.

However, building a SOC unleashes a deluge of data from disparate sources which often overwhelms in-house teams and prevents the SOC from functioning effectively. The solution – one which is on many 2022 shopping lists right now – is a Threat Intelligence Platform.

A Threat Intelligence Platform, or TIP, serves as a central repository for all threat data and intelligence from internal and internal sources. Correctly configured, the TIP should be able to deliver essential context around threats that helps the team understand the who, what, when, how and why of a threat. Crucially, it should also help prioritise threats, based on the parameters set by the organisation, filtering out the noise so the resulting actions are clear.

A good TIP benefits a range of stakeholders, from the board aiming to understand strategic risk to CISOs focusing on improving defence while staying on budget, and from security analysts collaborating more effectively to incident response teams benefiting from automated prioritisation of incidents. Knowing what you need to invest in is the first step. The next is to understand the key features you need and why. There is a lot to consider, but in my view the following are five key areas that should be on your checklist as you evaluate TIPs:

1. Ability to consume structured and unstructured data

A TIP must be able to import data from every possible source – internal and external, proprietary and open source – and in every format, whether structured or unstructured. This includes data from the full ecosystem of modern security tools such as endpoint detection and response (EDR), Network Detection and Response (NDR) and Cloud detection and response (CDR). Where unstructured data, such as blogs and social media posts is concerned, the platform must be able to parse and extract “de-fanged” or “neutered” data such as neutralising potentially risky URLs while leaving them readable by analysts.

The threat environment changes constantly, so the facility to create new custom connectors to ingest intelligence around new threats as they emerge is

also key. So, too, is the ability to define additional objects to fit specific use cases, allowing teams to tailor the platform to their preferred workflows.

2. Context is king!

Context is the crucial piece of the jigsaw allowing teams to make sense of what the mass of indicators are telling them and respond appropriately. Due to the importance of the supporting context, it is important to determine if the TIP vendor imports all the data and/or if they modify any of the data. Modification can be helpful as a layer of normalisation is critical to de-duplication efforts.

However, normalisation and unification of data must be done while preserving context. For instance, if Feed X publishes https://www.badguy.com, Feed Y publishes http://www.badguy.com and Feed Z publishes www.badguy.com, all three should be reconciled into a single IOC entry. Those are all "technically" different indicators, however the goal is to efficiently maximise detection strategies with minimal duplication. Data feed normalisation helps to consolidate analyst comments, better organise associated intelligence and effectively export one IOC in lieu of three IOCs, which makes for greater efficiency.

3. Scoring and prioritisation

The sheer volume of indicators published today means it is impossible - and indeed undesirable - to monitor them all. This makes scoring and prioritisation a key feature of an effective TIP. Teams need a mechanism to prioritise which indicators should be detected to investigate, blocked or disregarded as a non-threat.

Scoring is highly specific to the organisation and the mission of the team and should not simply reflect vendor or community opinion. A progressive TIP will let you set your own scoring algorithm based on any piece of data in the system, making it a more tailored and accurate threat management solution.

4. Multiple integration options

Integration with the full ecosystem of security tools is central to the value proposition of a TIP. The tighter the integration, the less manual work is required of analysts and the greater the efficiency of operations teams. Uni-direction integration - from the TIP into an endpoint solution for example - is a given. This is a purely defensive strategy and is the most common integration, moving the automatically scored highest threats from the intelligence platform into the trenches of the organisation's sensor grid for detection and/or blocking.

The next wave of TIP integration is bi-directional, with data pushed out from and pulled back into the tool. Key use cases for bi-directional integration are SIEM or log repository, ticketing systems, vulnerability management solutions and SOAR solutions. These combine to drive efficiency, improve prioritisation and reduce incident response times and vendors should offer software development kits (SDKs) and open APIs to facilitate powerful integrations.

5. Data-driven automation and investigations

For under-pressure security teams, the ability to automate repetitive, time-consuming, low-level tasks is essential. If a tool can combine this automation with the real-time data and context needed to empower analysts to investigate high impact, time-sensitive incidents, even better! Effectively, teams need a balance between automation and manual investigation and the threat intelligence platform should deliver that using a native, data-driven approach. Business considerations when choosing a TIP

Beyond the technical considerations – of which the above provide a snapshot and are not exhaustive - organisations also need to evaluate business factors.

Pricing is usually on a subscription and per user licence basis, which is a straightforward initial calculation based on the number of tactical users you have. However, a successful implementation should see a broader set of stakeholders realising the value of having access to the platform, so it is worth forecasting for access by teams such as risk management.

As discussed above, integration is central to the TIP value proposition, and vendors should provide an SDK and open APIs to facilitate this, but some charge a fee per integration. This can significantly increase the budget when you consider the number of different tools you want to integrate, so it is vital to know this upfront. Similarly, should the business undertake mergers or acquisitions, this will entail integrating the acquired company's tools into the TIP, which will have a financial implication if a fee is payable each time.

Finally, understand the cost implications of hosting the TIP on-premise or in the cloud. If you are evaluating a cloud-based service but know you will need to deploy a private cloud instance for compliance or privacy requirements, be sure to understand if there are any additional costs and trade-offs in functionality/features. A TIP designed to run in the cloud often cannot offer full functionality on premises.

The right Threat Intelligence Platform has the potential to dramatically boost the performance of the SOC and selecting one should be a carefully researched and rigorous decision. As organisations aim to improve proactivity and embark on activities such as threat hunting, while effectively prioritising response to incoming threats, a powerful TIP will allow them to get the most out of existing resources and maximise the return on historical investment in security tools.

Almost everything you ever wanted to know about 6G

6G is the latest generation of wireless technology under development, with new generations emerging approximately every 10 years. With promises of futuristic technology that many can only dream of, there is much room for speculation leading up to the arrival of this latest technology.

BY TED CURTIS, SENIOR ENGINEER AT NETSCOUT

TYPICALLY, each new generation of mobile communication technology features an increased spectral efficiency – the amount of data transmitted over a given bandwidth – which makes the broadcast of additional information and communication more available through the same or similar resources. With this in mind, what can we really expect from 6G when it arrives?

The previous generations

Service networks have come a long way since the humble beginnings of the first-generation technology that introduced analogue voice communications. 2G went on to bring the world digital communications, SMS text, multimedia messaging and mobile services such as global positioning systems (GPS).

3G enabled mobile Wi-Fi services such as video calls, voice over IP (VoIP), and online streaming. As web connectivity became standard and GPS services expanded, accompanying international roaming services were also introduced.

4G brought with it high-quality video streaming, allowing better quality video calls and online gaming apps. Long-term evolution (LTE) networks increased service provider speeds for mobile ultra-broadband internet. Even today, 4G still provides enhanced data, voice, and online streaming services that most users continue to use.

Thanks to 5G, the world now has semi-autonomous vehicles, virtual reality, ultra-high-definition video, and enterprise Internet of Things (IoT). Its speeds are

much faster – between 40 and 1,100 Mbps – with lower latency and it is better equipped to support additional demanding uses unlike ever before. With 5G released only recently, there is still much left to be appreciated.

5G vs 6G

Only introduced in 2020, 5G technology still has a lot to offer – currently taking on the heavy-duty applications to make digital services much more efficient and secure. 5G has undertaken the immense demands of application and online services which supported the world's connectivity during international lockdown mandates.

6G is not expected to arrive until 2030, and is still in the theoretical and development stages. However, what can be expected is for 6G to pick up where 5G left off, likely operating with greater terahertz (THz) frequencies and addressing even lower latency requirements. 6G networks are also expected to continue with 5G sustainability efforts – using hydrogen fuel cells instead as an alternative energy source, along with other methods to reduce energy consumption. With expected developments in automation technology, communications service providers (CSPs) will be able to recycle 5G network equipment in efforts to reduce global e-waste.

However, because THz frequencies can only be used for short range transmission, this may result in cellular networks evolving into hybrid, meshed networks. This involves providers creating microcells which can only be accessed by 6G devices or smart surfaces.

What to expect from 6G

Although 6G's arrival is quite a while away, there is still a lot to look forward to, such as information and communication technologies (ICT) improvements to critical infrastructure, enhanced network sustainability, and lower-cost coverage expansion. One thing is certain, 6G is going to be fast. With a new and innovative framework, for the first time ever, users will be able to experience 6G network speeds of 1 terabit per second (Tbps) or 1,000,000 Mbps.

Also exciting are the futuristic, near science fiction-like, advances that are yet to come, according to industry sources. Holographic-type messaging and fully driverless vehicles may seem farfetched now, but could become standard features with 6G. Fully tactile haptics and five-sense services are fascinating additions to anticipate, expanding all five senses of the human body into the VR experience. This represents a major advancement for prosthetic users and those with physical challenges, enabling effortless and instantaneous interactions with their mobile devices without physical limitations.

Just as important, 6G networks will be accessible to more global users. As current networks continue to operate more affordably and simplistically, transitioning away from hardware to software, network coverage will expand into further regions around the world. The reductions in general costs to end users and CSPs will make this technology more affordable to those who may have had limited access to network services before. Additionally, 6G should continue 5G networks' increasing sustainability, with improvements in automation and with communications service providers (CSPs) able to reuse network equipment.

When considering the prospects of what 6G will offer, it can't be helped but to imagine and speculate upon the exciting possibilities that the new innovative technologies will enable. Although new features are always exciting and greatly anticipated, the potential of expanding its accessibility affordably to connect many more users is a powerful aspect to bridge the digital divide.

In data we trust: building customer confidence in a digital economy

In the modern, digital world, online shopping is becoming the norm within the retail market. Accelerated by the pandemic, the UK's proportion of online retail sales soared to the highest on record, reaching 35.2% in January 2021. And with digitisation continuing to evolve the online shopping experience, it is unlikely that we will see a shift back to pre-pandemic norms anytime soon.

BY PETER BOYLE, CTO OF BURNING TREE

SO, WHAT DOES THIS MEAN for business-customer relationships in the digital era? Without the experience of in-person shopping, online user experience has a strong influence over consumers' buying decisions. As a result, brands must define their reputation as trustworthy and reputable providers by shaping their processes around customers' online behaviours.

'Digital trust' is defined as the confidence users have in the ability of processes, people and technology to create a secure digital world, dividing the dependable services from the corrupt ones. In a world where most people understand that not every online service is legitimate, establishing digital trust helps users decide which companies will keep their personal information safe. So, how can businesses gain the trust of their digital customers — and what will happen if they do not?

Why should businesses build digital trust?

When people make a purchase or interact with an online retailer, they demonstrate their digital trust in that business. However, the quality of the service is no longer defined by how an interface looks or how easy it is to navigate.

Customer expectations have evolved with digitisation. Driven by rapid device proliferation and improved internet connectivity, the modern online shopper expects to encounter seamless digital processes from sign-in to purchase – particularly since the pandemic, which increased the number of people using online services regularly.

Today, customers are more aware of how their data is being used and stored and base their shopping behaviours on a provider's ability to ensure security. The Okta Digital Trust Index (2021), which surveyed 13,000 office workers, found that 88% of people in the UK were unlikely to purchase from a brand they did not trust. And according to a recent report on the 20 most-trusted UK retailers, 58% of consumers are highly conscious about their safety when shopping online, citing identity theft as a significant concern.

Plus, with most businesses working online in some capacity, the government is introducing more regulations for using technology to use and manage digital identities. A new digital 'trust framework' was announced earlier this year to make sharing digital identities between users easier and safer, allowing more control over what personal information is available to different services and organisations. There are several ways businesses can generate a loyal digital customer base — from generating positive customer reviews to providing excellent customer service. But when it comes to digital trust, three main factors make people in the UK more likely to trust a brand: its service reliability, good security policies and quick response times — all of which can be facilitated by successful digital transformation.

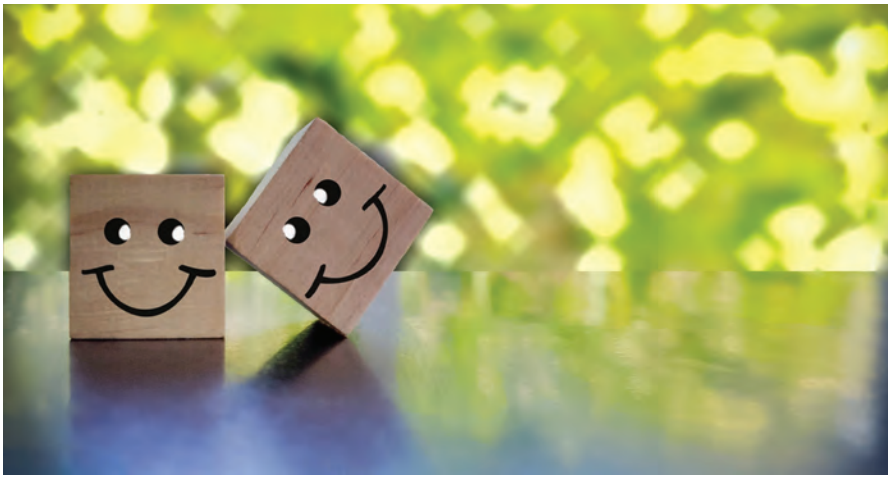
Building digital trust with digital transformation
Cyber security is an essential consideration for organisations undergoing digital transformation, which involves implementing technology to automate processes, encourage a more cyber-aware business culture, increase security and refine the user experience. As such, retailers must ensure data is protected from a cyber breach to remain compliant and secure digital customers — and keep them coming back.

According to Okta's survey, 47% of UK people permanently stopped using a firm's services after hearing of a data breach. As such, IT professionals are harnessing advancements in artificial intelligence and machine learning to support existing traditional threat models and automate risk management to reduce the overall probability of falling victim to a cyber attack.

Customer expectations have evolved with digitisation. Driven by rapid device proliferation and improved internet connectivity, the modern online shopper expects to encounter seamless digital processes from sign-in to purchase – particularly since the pandemic, which increased the number of people using online services regularly

Many organisations are also taking a 'zero-trust' approach to cyber security, which means that no activity within a network is trusted straight away. Every device, service, application or user connected by a network must go through a robust identity and access management process to gain a least privileged level of trust and associated access entitlements. As such, implementing a zero-trust framework helps bolster cyber security and minimises the likelihood of a breach.

Effective customer identity and access management (CIAM) solutions will also enable organisations to capture and interpret customer profile data to inform customised user experiences whilst controlling secure access to services and applications. A robust CIAM solution may involve implementing multi-factor authentication (MFA), self-service account management and single sign-on (SSO) to minimise friction, increase engagement and develop trust in business processes over time.



DCA Data Centre Anti-Contamination, Filtration & Cleaning SIG

An Introduction from DCA CEO Steve Hone

AS THE Trade Association to the Data Centre sector the DCA understands that it is imperative that key issues affecting the sector have a point of focus. The DCA SIG's (Special Interest Groups) / Working Groups regularly come together over shared interests to discuss issues, resolve problems and make recommendations. Outcomes result in best practice guides, collaboration between group members, participation in research projects, this includes clarification and guidance for decision and policy makers. Members find these groups are a great way to ensure their opinions and views are considered in a positive and cooperative environment.

The DCA currently facilitates nine Special Interest or Working Groups. DCA members can join any of the groups (although the Chair has final say) and contribute find out more here: **https://dca-global.org/groups**

The DCA Anti-Contamination, Filtration & Cleaning SIG is chaired by Gary Hall, Operations Director at Critical Facilities Solutions UK

The demands and growth of digital services has driven radical changes to ICT equipment and this in turn has driven equally radical changes to data centre designs. This has been caused by wider and greater ranges in temperature and humidity in the data centre together with new technological schemes and upgrades to meet these changes, which in many cases requires a new approach to anti-contamination strategy to ensure the desired reliability and energy efficiency goal of the data centre remains intact.

This group examines the risks posed to data centre facilities of contamination from dust, dirt, airborne particulates that enter data centres. Through a collaborative approach a range of data centre M&E and design experts and several data centre technical cleaning specialists the SIG produces a Best Practise Guide each year. The objective is to provide an independently written guideline for owners and operators to benefit from the collective experience of the industry with the trusted peer review of the DCA.

To request to join this group as a guest or to find out more please contact the DCA - **mss@dca-global.org**

DCA Anti Contamination & Filtration SIG Update (February 22)

Gary Hall, Critical Facilities Solutions & Chair

Overview

ASSOCIATIONS run by individuals, or teams of individuals with solid first-hand experience and an in-depth understanding of the Data Centre industry are of huge value. The DCA Special Interest Group (SIG) for Anti Contamination & Filtration have been raising the profile of contamination control in critical environments since 2013.

The SIG Anti-Contamination and filtration committee examine the risks posed to Data Centre facilities from contamination such as dust, dirt, airborne and gaseous particulates, and other foreign objects that enter mission critical spaces. The ultimate objective is to provide independent advice and guidelines for owners and operators of mission critical Data Centres to benefit from the collective experience of the industry with the trusted review of the DCA.
Anti-Contamination & Filtration Guide

The first major milestone achieved by the SIG was the creation of the Anti-Contamination Guide that was first released in 2013 with revisions released each year since. The guide is the product of industry professionals including individuals from Data Centre cleaning and air filtration companies who have contributed years of experience and an in-depth knowledge on the best practices that should be adopted in mission critical spaces.

The guide covers a variety of topics such as how certain contaminates impact operational performance, what level of vetting or experience your specialised cleaning company should hold and how to select and evaluate a company, based on risk, before engagement. The guide has received exceptional feedback from Data Centre owners and operators and in its current release being referenced in a global standard operating

procedure document for a world-wide Data Centre facilities management company which is testament to the credibility of the information it contains. In the annual reviews the SIG evaluates and updates the guide with new standards and best practice, it adds innovative solutions and products and access industry drivers. These are all aimed at helping drive efficiencies through keeping the Data Centre free from dirt, particulate matter, and gaseous contaminates.

In 2019, the SIG introduced a 'risk register' into the Anti-Contamination Guide, this new section of the report listed out in detail all the high-risk contamination elements that could impact operational activities within the Data Centre, and a weighted percentage score was introduced as a representation of what could happen if contamination is not managed correctly. The risk register is under constant review and updated yearly by the group. The latest release of the Anti-Contamination Guide was released in February 2022 and can be downloaded from the Data Centre Alliance website.

Continuous Awareness & Promotion

Specific industry targeted blogs and thought pieces have been carefully written over the past three years by the SIG. One of the highlights was raising awareness of the changes listed in the EU Code of Conduct for Data Centres (Energy Efficiency) Report. The EU Code of Conduct for Data Centres (Energy Efficiency) report highlighted that air quality is monitored and managed in Data Centre environments to ensure that critical equipment is not damaged by particulates or corrosive elements which might impact both IT equipment and cooling equipment in terms of performance, energy efficiency and reliability. Section 3.2.12 of the document was listed as an optional practise in early releases of the report until the 2019 release which moved "Monitor and Manage Air Quality" from 'optional' to an expected application to all existing IT, Mechanical, and Electrical equipment within the Data Centre.

This was a significant shift in the report to highlight the importance of Data Centre cleanliness and the SIG felt the need to raise the profile of this change. The SIG felt that it should highlight the importance of managing contamination through the construction phase of a Data Centre. Contamination onsite should be managed progressively over time instead of the traditional 'one pass clean' at the end of the build programme, the benefits to the process are, cleaning of pre-installed containment, items such as cable trays, cable baskets, internal ducting, pipework. The daily management of anti-contamination products, ensuring plant and machinery are clean before being used in the Data Centre or critical space. This information is extremely valuable as we're seeing Data Centres being built in abundance across the globe.

Additional documents have been produced by the SIG on COVID-19 related measures and the best practices in a very different world we are currently living in, selecting the correct cleaning contractor and the risks of not performing due-diligence, and what the future holds for Data Centre cleaning.

Look Forward

The SIG have set a target in 2022 of obtaining real-time information from Data Centre owners and operators in regard to their approach of controlling contamination in their critical spaces. The SIG will be producing a factual information sheet based on results obtained from a set number of questions submitted to Data Centre managers. The information received will be reviewed for 'trends' and used to analyse if keeping Data Centres free from physical and gaseous contaminants are high on DC managers agenda. All information received will be treated in total confidence, and no clients will be named in the information gathering exercise.

The SIG are trying to establish if Data Centres are being cleaned on strict schedules, are they regularly being inspected for signs of zinc whiskers, are they being monitored for any gaseous contaminations, are they utilising anti-contamination products, do they have contamination control work permits in place? All these questions will help us build up an accurate picture of what is or isn't being done across the industry. The contamination control survey will also be used to educate the IT market on what precautions should be undertaken, frequencies, and why they should be done.

Summary

With the world becoming more and more dependent on everyday IT applications, the spaces in which run these services should be free from physical & gaseous contaminants, and maybe in the future, Data Centre air cleanliness testing and monitoring will become a mandatory requirement across the globe.

The DCA - Anti contamination, filtration & cleaning SIG

Chaired by Gary Hall of Critical Facilities Solutions

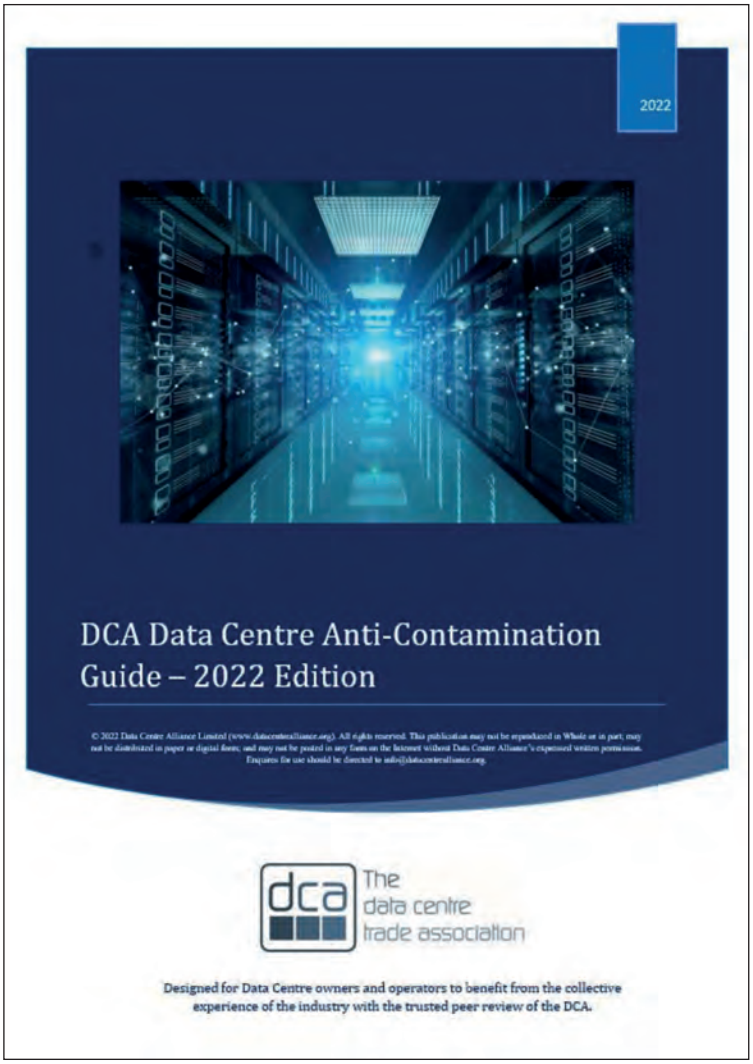
THIS SPECIAL INTEREST GROUP is made up of individuals from various organisations with relevance to this important area of focus for Data Centres.

The group meets on a regular basis to discuss, advise and recommend practical solutions on the control of dust, dirt and contamination. In particular, preventing damage to equipment; loss of data and conservation of energy. The output from this group has included a Best Practice Guide for Anti-Contamination. This was introduced in 2019 with fourth guide, the 2022 guide now being available.

DCA Data Centre Anti-Contamination Guide - 2022 Edition

Introduction

The demands and growth of digital services has driven radical changes to ICT equipment and this in turn has driven equally radical changes to data centre designs. This has been caused by wider and greater ranges in temperature and humidity in the data centre together with new technological schemes and upgrades to meet these changes, which in many cases requires a new approach to anti-contamination strategy to ensure the desired reliability and energy efficiency goal of the data centre remains intact.



This document examines the risks posed to data centre facilities of contamination from dust, dirt, airborne particulates and other foreign flora and fauna that enter the data centre.

The information provided is the result of a collaborative approach by members of the Data Centre Alliance, an independent industry association. This involved a range of data centre M&E and design experts and a number of data centre technical cleaning specialists.

The objective is to provide an independently written guideline for owners and operators to benefit from the collective experience of the industry with the trusted peer review of the DCA.

Here is an except related to choosing the correct cleaning contractor

Avoid using office or “IT” cleaning contractors who cannot demonstrate specialist Data Centre knowledge and experience. In-house cleaners are often not insured to work in Data Centres. Ensure specific tools are used, such as ‘HEPA’ filtered vacuums, specialist cleaning agents, tak cloth etc.

Do not use cleaning contractors that advocate the use of brooms, feather dusters, non-specialist vacuum cleaners. Ensure contractors have knowledge of using the correct power points, the fire protection and warning system(s) needing to be isolated, the correct lifting of Data Centre floor tiles and a general good understanding of the data centre environment and awareness of its functions.

Ensure specific tools are used, such as ‘HEPA’ filtered vacuums, specialist cleaning agents, tak cloth etc

When considering a cleaning provider, assess the following:

Experience Profile	Should have vast experience of delivering Data Centre cleaning.
References	References should be obtained to vet performance/ability of the cleaning provider.
Training – documentation and proof	All cleaning operatives should be fully trained in Data Centre cleaning and understand the environment they work in (including all risks).
Dedicated data delivery preferable	The cleaning provider should preferably be dedicated to Data Centre cleaning operations.
Accreditations	The cleaning provider should have gained the correct accreditations to engage in Data Centre cleaning, (quality management for example).
UK Geographical cover	The cleaning provider should have full geographical reach to service the needs of the Data Centre owners.
Labour resource and sufficiency of cover	The cleaning provider should also be able to respond to emergency incidences within the Data Centre or supporting locations (plant/UPS rooms).
Back-up, reporting and supporting systems	The cleaning provider should have clear reporting systems in place, air quality statistics should be backed up in reports for the client.
Ability to carry out site survey to properly assess	The cleaning provider should have the capability/ability to perform project surveys and give recommendations on the best delivery model tailored to the client's needs.
Health & Safety record	The cleaning provider should have a good Health & Safety record of working in Data Centre environments, all cleaning operatives should also be trained in delivering toolbox talks and completing dynamic risk assessments when onsite.
Sufficient insurance cover	The cleaning provider should have sufficient insurance cover for working/operating in mission critical spaces.

Data centre planned preventative maintenance

Question, why do you have your car serviced regular? The answer is to ensure it runs smoothy and reduces the risk of it breaking down and incurring an expensive and unexpected repair.

Gary Hall – Chair of the Anti-Contamination SIG

Maintaining Data Centre's and the critical space that supports these buildings are just like maintaining cars. ASHRAE (American Society of Heating, Refrigeration and Air Conditioning Engineers) realized that all Data Centre's should be cleaned and maintained to a specific air cleanliness level, and the air cleanliness should be measured against ISO 14644-1 (ISO 14644-1 is the International Standard for Clean Rooms and Associated Controlled Environments).

ASHRAE's recommendation to the IT industry was to have a facility that would have an air cleanliness rating of ISO Level 8 as a minimum, this standard would be achieved through correct air conditioning filters being installed and removing all visible traces of contamination. The ultimate aim behind this statement and drive was to reduce dirt, dust, carbon, construction debris, calcium carbonate, metallic, paper dust, synthetic fibers, human and non-human organic fibers and other often unseen sources of contamination from Data Centre's as they are leading causes of internal corrosion and equipment malfunction in computer systems.

The reason for a clean IT space is very clear, at the heart of the worlds digital activity are everyday services and applications that have become staple in all our lives, collectively, these produce unimaginable quantities of user activity and associated data, to let systems become at risk from downtime due to contamination is unacceptable in this modern day, especially when simple steps can be taken.

For example, this is what happens every 60 seconds in the modern world we live in, Microsoft Teams connects 100,000 users, 6 million people shop online, Facebook Live receives 44 million views, YouTube users stream 694,000 videos, Tiktok users watch 167 million videos, and the stats are ever growing. In 2022, we will begin to see autonomous vehicles on our roads, technology will be taking over human judgement, and everything dedicated to making this a reality must be checked, checked, and double checked.

End users of everyday applications should have the confidence that tech facilities have implemented planned preventive maintenance cleaning regimes to stop unexpected outages.

When implementing a planned preventative maintenance routine for Data Centre environments, it's vital that the correct service partner is selected. You should ensure cleaning providers have knowledge of using the correct power points, the fire protection and warning system(s) needing to be isolated, the correct lifting of Data Centre floor tiles and a general good understanding of the Data Centre environment and awareness of its functions.

The following criteria points should be evaluated,
Experience Profile - Should have vast experience of delivering Data Centre cleaning
References - References should be obtained to vet performance/ability of the cleaning provider
Training, documentation, and proof - All cleaning operatives should be fully trained in Data Centre cleaning and understand the environment they work in (including all risks)
Accreditations - the cleaning provider should have gained the correct accreditations to engage in Data Centre cleaning, (quality management for example)
Back-up, reporting and supporting systems - the cleaning provider should have clear reporting systems in place, air quality statistics should be backed up in reports for the client
Health & Safety record - the cleaning provider should have a good Health & Safety record of working in Data Centre environments, all cleaning

operatives should also be trained in delivering toolbox talks and completing dynamic risk assessments when onsite

Sufficient insurance cover - the cleaning provider should have sufficient insurance cover for working/operating in mission critical spaces.

To give you an idea of what some of the large technology companies have implemented in terms of Planned Preventative Maintenance cleaning, Sun Microsystems/Oracle recommends in their site preparation guide, the following cleaning schedule: "Bi-annually decontaminate the subfloor void and air conditioners; quarterly decontaminate the hardware and room surface", HP recommends in their site preparation guide that "twice a year, remove any contamination found underneath the raised floor and clean raised floor perforated panels".

The DCA Ani-Contamination and Filtration SIG would recommend that a yearly deep clean of the Data Centre be undertaken, this should include cleaning all plenum voids (floor & ceiling), and all fabrics of the room, including the removal of contamination from internal facias of the IT equipment.

Remember, plan, plan, and plan again to keep these vital services online now, and for the future!

Hospital Trust leans on EcoStruxure™ IT Expert for continuous uptime.

Discover how Birmingham Women's and Children's NHS Foundation Trust leveraged EcoStruxure™ IT Expert to enhance it's reliability and continuous uptime.

Read the case study

Life Is On | Schneider Electric