DIGITALISATION WORLD

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

ISSUE I 2023

DIGITALISATIONWORLD.COM

View from a retail CIO

The rush into digitisation, the shortage of talent, and supply chain disruption

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

ninjaOne

Bring efficiency, automation, and scale to your MSP.

Learn more

Editor's View

By Phil Alsop Editor

Dangerous data?

THE TRUISM 'Garbage in; garbage out', remains as true as ever, whether we are talking about politics(!), our favourite sports teams or the world of business and, in particular, the data on which so many decisions are based.

The data dilemma is there for all to see. Collect the right, meaningful data and, properly analysed and acted upon, it can make a major contribution towards business development and prosperity. Become bogged down in the sheer quantity of data, with no idea of which bits (pun intended) matter and which don't, and the analytics effort can become a costly time-wasting exercise.

The chances of randomly analysing a random data set and coming up with a major, money-spinning insight as a result, are not far short of the much-fabled suggestion that, put enough monkeys with typewriters in a room and, at some point in the future, they will write the works of Shakespeare! Nevertheless, organisations are being encouraged to keep every piece of data and crunch the numbers.

To be fair, such number crunching is far less expensive or labour intensive now than it was even a few years ago. Data analytics as a service means that there's no longer the need to acquire the necessary infrastructure - the hardware and software - at major expense and disruption, against a somewhat vague return on investment. Data sets can be analysed via a cloud or managed service for a fixed, relatively inexpensive fee. However, as with many, many aspects of digital technology and infrastructure, it is the combination of the human brain and artificial intelligence which will bring the best results.

By all means keep hold of your data if you think it might be useful in the future, and the cost is not too prohibitive, but when it comes to analysing it, the chances are that one or more humans will be best placed to decide on the queries most likely to yield results, rather than trusting that AI will do the work for you. Of course, this may change over time but, as I think I have written before, the likelihood that AI will be able to replicate the complexities and random thoughts of the human brain, let alone understand why certain purchases have been made by certain individuals, is some way off.

Add in another of my favourite analogies – storing things in the attic – and I would urge companies to have a very clear idea of what it is they want to achieve from data analytics, rather than be guided by others, or, worse still, try some random enquiries of their own. Storing things in the attic – is there any household that doesn't have a room, an attic or a garage where things no longer needed are stored, 'just in case'? And how often are such objects ever retrieved? In reality, when it comes time to move house, the stored objects are the first things to be taken to the refuse dump/recycling centre. For a householder, the cost of storing no longer needed objects is zero, assuming they have the space to keep them.

For businesses, keeping data that appears to have no further value, does have a cost, and one that is rising. Yes, compliance regulations may require data retention for a period of time, but let's be honest, the main reason that companies do not delete any data is fear. Fear that, once deleted, such lost data might suddenly become valuable in the future.

DW DIGITALISATION WORLD

View from a retail CIO: A rush into digitisation, the shortage of talent, and supply chain disruption

The retail sector is just emerging from the backdrop of intense pandemic-induced digitisation, only to find itself in an environment with many more external pressures – from the tech talent shortage to outstanding technical debt and supply chain pressures

THE ANALYST

DATA ANALYTICS

DIGITALISATION WORLD

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

Sales & Marketing Manager
Shezhad Munshi
+44 (0)1923690215
shehzad.munshi@angelbc.com

Senior B2B Event & Media Executive
Mark Hinds
+44 (0)2476 718971
mark.hinds@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
Scott Adams: CTO
Sukhi Bhadal: CEO

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

Angel BUSINESS COMMUNICATIONS

Digitalisation World is published 10 times a year on a controlled circulation basis in Europe, Middle East and Africa only. Subscription rates on request. All information herein is believed to be correct at time of going to press. The publisher does not accept responsibility for any errors and omissions. The views expressed in this publication are not necessarily those of the publisher. Every effort has been made to obtain copyright permission for the material contained in this publication. Angel Business Communications Ltd will be happy to acknowledge any copyright oversights in a subsequent issue of the publication. Angel Business Communications Ltd.

ISSN 2396-9016 (Online)

Poly urges organisations must do a culture audit NOW or risk going to “hybrid hell”

New report explores the challenges of fostering hybrid culture as the workplace becomes more fragmented.

POLY has launched a new report - ‘Hybrid Heaven or Hell? The journey to hybrid working’ - examining the importance of culture in hybrid work. As a result of the findings, Poly is urging organisations to do a culture audit – evaluating aspects of their culture to work out what works and what needs to evolve for hybrid work success – or risk going to “hybrid hell”.

The report, written in partnership with WorkTech Academy, includes research from Gallup, Gartner, and Harvard Business Review, as well as Poly’s own insights and findings.

The broader research trends were also discussed and debated in a New York roundtable attended by senior workplace design and technology leaders. The report highlights that organisations have been faced with challenges of building and retaining culture which could have a lasting impact on innovation, talent retention and growth.

“Hybrid culture cannot be left to chance. Now is a crucial time for organisations to take stock and rebuild a culture that is fit for hybrid working,” says Sof Socratous, Head of Northwest Europe, HP Poly Hybrid Work Solutions. “This means relearning the expectations of work: how people like to work and where. Those that fail to do so will risk going to ‘hybrid hell’, leaving employees feeling unengaged and unhappy.”

These challenges are only being exacerbated by the workforce becoming even more distributed and fragmented. 2022 saw the rise of the shorter work weeks, employees applying for digital nomad visas, and trends such as workcations – where people work abroad to maximise annual

leave - taking off. As the world of work shifts and employees unshackle from the traditional 9-5, organisations need to ensure they foster a culture that supports hybrid working.

The report shows that one of the biggest barriers to fostering culture is redesigning the workplace, which should support and nurture culture, but shouldn’t drive culture. As a result, many organisations are struggling to make their old spaces work for new ways of working.

Poly office persona research found that, pre-pandemic, individual desks took up an average of 65 per cent of office space. In response to hybrid work, this is expected to fall to about 40 per cent. Organisations need to carefully consider how they redesign their spaces to support culture in a hybrid environment.

Poly’s research shows 77% of organisations are redesigning the office to support new ways of working. One trend that is on the rise is organisations taking inspiration from restaurants, both in the form of booking spaces to work and how they organise their space. For example, hotelling which is where employees make use of a corporate booking system to reserve desks in their own workplace, for a day at a time.

This shift will also see the rise in mobile workspaces as organisations introduce bench style desks and hot desks to ensure everyone has somewhere they can work when visiting the office.

“The shift to hybrid work presents an opportunity for organisations to remake cultures and their workspaces for the 21st century. This requires organisations to clearly define their core cultural values and frame what that means in a hybrid world,” says Sof Socratous.

“This includes taking a strategic approach to consider people, spaces, and technology. Firstly, analysing why people want to come together – what do people need to achieve and where does physical presence add value? Once the culture has been defined and employees’ needs are understood, then the spaces can be redesigned, and technology can be adopted to ensure equal experiences for everyone.”

Research reveals the gap between perception of 'Sustainability Transformation' preparedness and reality

61% of organizations claim to be advanced on their sustainability journeys, but in fact, less than one in 10 have completed major sustainability imperatives.

FUJITSU has published the results of new research commissioned by Fujitsu, carried out by FT Longitude, the specialist research and content marketing division of the Financial Times Group, indicating that sustainability impact is the number one priority for organizations surveyed, and that they are aiming to improve on the three pillars of Sustainability Transformation (SX): environmental, economic and societal.

The research shows, however, that few organizations have in fact completed important Sustainability Transformation initiatives, suggesting that many of them have not come as far as they think, despite the importance they believe sustainability holds for the future. For example, only 26% of the organizations surveyed have implemented health and wellbeing initiatives for employees, and only 12% are using or creating carbon-neutral products.

The report identifies that more than two-thirds (68%) of organizations say that Sustainability Transformation will not be a success without significant investments in technology. When asked about the support they needed to achieve their Sustainability Transformation, 42% said that they need help with transforming existing/legacy technology.

Key findings

The sustainability gap

While 61% of organizations believe that they have made substantial progress on their advanced sustainability journeys, less than one in ten have completed major sustainability imperatives such as developing sustainable supply chains (9%), achieving net zero status (2%) and preparing for environmental emergencies (7%).

Organizations need support with their technology transformation

The research shows that organizations are investing in modern technology, recognizing that this represents a fundamental step in supporting many Sustainability Transformation initiatives. However, the report identifies that getting help with transforming existing/legacy technology is one of the main concerns for organizations seeking to make progress with Sustainability Transformation.

The Changemakers

A small group of leading organizations was identified, the Changemakers. This group accounts for the 6% of organizations that are leaders in sustainability and technology. This group has made substantial progress on their sustainability goals, by powering their efforts with innovative technology. They lead the way on both sustainability imperatives and technology transformation.

Technology is key for a successful Sustainability Transformation journey

Being successful at Sustainability Transformation requires companies to be both sustainable and tech savvy. If organizations want to succeed in their Sustainability Transformation plans, focusing only on sustainability isn't enough.

Cost and fragmented data emerge as top barriers to reducing carbon footprint

And only 38% business leaders rate their decarbonisation efforts so far as very successful.

COLEMAN PARKES RESEARCH has published a new report that seeks to answer the question "How are companies and business leaders managing their decarbonisation efforts to reach net zero in Europe by 2050?". Commissioned by Atos and Amazon Web Services (AWS), Coleman Parkes Research surveyed 4,000 business people across three sectors, energy and utilities, financial services, and manufacturing, in four major European countries, France, Germany, Spain and the United Kingdom.

Against the backdrop of the Paris Agreement goals and the broader recognition to drive sustainable and digital transition towards an increasingly low-carbon society, almost all organisations surveyed (96%) have set emissions reduction targets. With this being merely the first step in a long journey, businesses across different sectors are facing diverse challenges in properly tracking their carbon footprint and delivering the necessary solutions to meet these targets. The report suggests that while three in four business leaders believe that cloud technology would accelerate their companies' journey to net zero by two years or more, there was still a fifth of the organisations who were yet to go cloud-first and thereby benefit from a reduced carbon footprint. Only 38% of business leaders surveyed rated their decarbonisation efforts to date as very successful.

Overcoming Fragmented Data

Among the key obstacles to businesses' decarbonisation journeys were the impact that rising costs and economic uncertainty were having on their budgets, as well as the fragmentation of their internal data sets and insights. Robust data can be harnessed to provide deeper insights into a business' environmental impact and to drive cost reduction, streamline operations and manage decarbonisation. In this study, over half of businesses cite 'accurate and reliable data' as one of the top three elements that they would find most helpful in the implementation of their carbon reduction plans.

Target Setting v. Performance Measurement Gap

Only just over half are measuring emissions scopes 1 (covering direct emissions from owned or controlled sources) and 2 (covering indirect emissions from the generation of purchased electricity, steam, heating and cooling consumed by the reporting company). Less than a tenth cover scope 3 (which includes all other indirect emissions that occur in a company's value chain), and just 14% are setting targets validated by the Science Based Targets initiative for all three emissions scopes. Slightly at odds with these findings was the high levels of confidence among business leaders in their ability to control GHG emissions: 75% reported being confident of achieving their carbon reduction targets.

The Role of Technology

Among the countries in scope, UK and Spanish businesses are slightly ahead of the average in their decarbonisation initiatives; their investment in the cloud is one of the key solutions in achieving carbon measurement and reduction. Among a proportion of French and German businesses, more needs to be done in helping them to understand the real value that cloud can bring in the long term.

Almost a third of businesses surveyed said their technology solutions could be improved, and one in five said they lack the appropriate technology to see through their plans. 75% of business leaders admitted that their environmental impact reporting would be improved by an emissions measurement tool.

63% of businesses fear that their IT estate cannot support the hybrid workforce

Research finds current IT setup is preventing effective collaboration, putting remote workers at a disadvantage and driving up cyber risks.

ALMOST TWO THIRDS (63%) of IT directors are not very confident in their IT estate's ability to fully support the hybrid workforce, but over seven-in ten (71%) of organisations are not placing IT investment at the top of the priority list. These are among the findings from new research undertaken by managed workplace services (MWS) provider, Apogee Corporation.

Due to limitations with the current IT setup, 89% of respondents identify that it is preventing effective collaboration, with almost half (48%) admitting that remote staff don't have access to the same solutions as office workers. This is despite the top expectation among the workforce being the ability to collaborative effectively with technology, as cited by almost two fifths of respondents (38%). The opportunity to work flexibly is the second highest expectation (31%).

With remote workers at a disadvantage, security is also creating further concerns for the modern workforce, as a quarter (25%) reveal that security challenges with remote and hybrid working are affecting IT transformation progress. Businesses are also neglecting to secure the hybrid/remote workforce, with just 14% citing it as a top priority.

To further add to security woes, almost one-in-three (28%) directors say that they only audit their IT estate between once a month and once every 4-6 months.

Additionally, only 34% have endpoint security and 26% have device encryption in place, while under one-in-five businesses (19%) have an end-of-life plan for their devices to improve security among the hybrid workforce. All of these solutions are a necessity for organisations to continually safeguard against cyber-attacks.

This lack of technology adoption is culminating in organisations being unable to attract new talent, with 45% saying that offering the latest technology/devices is their top strategy to convince staff to join the business. Additionally, 26% say that ensuring access to high quality/reliable IT solutions is a top priority for attracting and retaining talent.

"Businesses are ultimately failing to invest in the technologies that meet the needs of today's workers. Hybrid strategies are now becoming the norm post-pandemic, while the digitally savvy generation is making up more of the modern talent pool.

By not addressing these issues, including the improvement of device security, organisations run the risk of poor morale among staff.

This will raise the likelihood of people departing the business and affect the ability to attract new talent," said Aurelio Maruggi, CEO of Apogee.

The potential for staff departures is likely to place further pressure on organisations which are already struggling with skilled staff shortages.

Over a quarter (29%) say that their employees are stretched across too many monitoring responsibilities due to the shortages and a quarter (25%) recognise that slow resolution of IT issues is also frustrating their staff.

Nine in ten consumers are curious about the metaverse

Organizations expect the metaverse and immersive experiences to be an important channel not only for consumer interactions but also enhanced employee and workforce experiences.

ACCORDING to a new report from the Capgemini Research Institute, 'Total Immersion: How Immersive Experiences and the Metaverse Benefit Customer Experience and Operations', 77% of consumers expect immersive experiences to impact how they interact with people, brands and services, and seven out of ten organizations say that they believe immersive experiences will be a key differentiator in their markets, particularly in relation to the customer journey. Out of the small group of metaverse-experienced consumers[1], three-quarters say they are currently using it and will continue to do so, which indicates there is potential for businesses that can harness the power of this much-hyped immersive experience.

In July and August 2022, the Capgemini Research Institute surveyed 8,000 consumers and 1,000 organizations in 12 countries to understand what potential consumers and organizations see in these immersive and metaverse experiences, whether delivered through headsets or mobile/web browsers etc. The report finds that while the actual decentralized "metaverse", based on blockchain technology, is still in development, the broad opportunities it presents to drive value across the business are already in the process of realization.

"We're starting to see a more thoughtful and nuanced approach to designing immersive experiences, and the metaverse specifically," comments Charlton Monsanto, Global Immersive Experiences Offer Leader at Capgemini. "This report supports the notion that early interest in the consumer-facing metaverse, propelled by investments from major players, needs to give enough thought to the real challenges around ergonomics, accessibility, safety and privacy, which organizations are now working to address. The potential of the metaverse is transformative and consumer curiosity remains high. Immersive experiences – including the metaverse – for internal use cases could be more impactful for organizations, certainly in the short term."

Consumers are clear about the immediate potential of immersive use cases

Research finds that consumers are intrigued by the prospects of immersive and metaverse experiences, and they would like to use the metaverse mainly as a place to interact with their family, friends (43%) and even their colleagues (39%). Amongst the brands they would be most interested in interacting with in the metaverse, they cite retail shopping (78%) and consumer product organizations (77%), i.e., enhancing their purchasing or try-on experience for high-engagement products such as cars, furniture, and household electronics.

There is significant potential for employee and workforce experiences
As indicated by the interviews, organizations have already successfully implemented immersive and metaverse initiatives, especially to improve operational efficiency, for example:

- Retail floor planning in CPR, where viewing a floor virtually enables organizations to plan their retail store design without teams having to travel there
- Training and education of medical professionals (and other industries), which allows surgeons to plan, rehearse and carry out procedures using headsets and 3D scans of patients
- Testing and digital prototyping in automotive, where VR is used for design and engineering reviews. By reducing the number of prototypes built, organizations can save millions of dollars while enabling considerable environmental savings.

However, many organizations lack a clear strategy to scale their immersive and metaverse initiatives

With the development of augmented reality (AR) and virtual reality (VR) technologies, the increased pace of digitization due to the pandemic and greater concern for sustainability, organizations across sectors have developed immersive experience pilots and demos at a fast pace in recent years. For the consumer products and retail (CPR) sector specifically, some businesses are piloting immersive use cases such as AR for virtual home decor, electronics and other items (24%) or to create new, more engaging, consumer experiences (25%).

According to the report, 66% of organizations now have a 1–2-year roadmap for immersive experiences and 15% of organizations aim to have some metaverse presence within one year, while 45% believe it will be mainstream within three years. However, many organizations are currently adopting a prudent approach. In addition to external factors hampering such initiatives (lack of maturity of the technology, lack of connectivity infrastructure etc.), the report finds that there are significant internal challenges for businesses to take full advantage of this consumer appetite and scale up - a lack of strategic planning, and for nearly 40% of organizations, immersive initiatives are still considered one-off projects rather than one link in a chain of continuous improvement.
Nearly two-thirds (62%) of businesses admit that there is no management commitment to immersive initiatives and over half (56%) cite that they have no clear roadmap to adoption.

Security doubts cost contracts

LogRhythm has published its report, "The State of the Security Team 2022: Can Security Teams Meet Internal and External Stakeholders' Requirements?" based on research conducted by Dimensional Research. One of the most compelling findings was security's impact on a company's bottom-line revenue as the majority of respondents (67%) indicated their company had lost a business deal due to the customer's lack of confidence in their security strategy.

DIMENSIONAL RESEARCH conducted a survey of 1,175 security professionals and executives across five continents representing a global view. The research investigated security solution capabilities, deployment strategies, gaps and the value of tool consolidation. The survey also looked to compare key data collected by LogRhythm and Dimensional Research in 2020 to identify and evaluate trends.

Security Is No Longer an Internal Affair

Respondents overwhelmingly indicated that customers and partners are demanding higher standards, highlighting that security has evolved beyond internal consideration.

Ninety-one percent reported that their company's security strategy and practices must now align to customers' security policies and standards. Partners also exert a new level of due diligence with 85% of respondents stating their company must provide proof of meeting partners' security requirements.

While LogRhythm's initial report in 2020 revealed significant misalignment between executives and their security teams with less than half of respondents (43%) saying they received enough executive support, the latest research found support nearly doubled over the last two years. The majority of respondents (83%) said they now receive enough support around budget, strategic vision and buy-in, suggesting an improvement in understanding between executive leadership and their security teams.

"Given the increasing complexity and severity of cyber threats organizations are experiencing, cybersecurity is now a business imperative," said Andrew Hollister, Chief Security Officer of

LogRhythm. "Security events hold the potential to significantly impact revenue, which begs the attention of executive leadership and pushes more organizations to align on expectations both internally and externally."

Security Teams are Feeling the Effects of Turnover

When asked if employee turnover reduces the effectiveness of their security teams, the overwhelming majority agreed regardless of their role with 77% of executives, 70% of directors and managers and 58% of security team members agreeing this has impact.

The research also found work-related stress for the security team is increasing for nearly 7 in 10 companies, with 30% reporting a significant increase, indicating many companies may be trying to do more with less amidst budget constraints.

The leading stressors for security team members include growing attack sophistication, more responsibilities and increasing attack frequency. When asked what would help alleviate their stress, the top responses included:

- 42% of respondents said adding more experienced security team members
- 41% of respondents said having more integrated security solutions

When asked if employee turnover reduces the effectiveness of their security teams, the overwhelming majority agreed regardless of their role

Data quality ‘chasm’ looms

Report from insightsoftware and Hanover Research reveals the gaps that need to be bridged to reach data fluency, noting challenges in data quality and connection.

INSIGHTSOFTWARE has released research that shows data quality is the biggest challenge organizations face when making data-driven decisions. The 2022 State of Analytics: Quest for Data Fluency asks businesses about their attitudes toward data literacy, the problems they face, and how close they are to reaching “data fluency”, the ability to fully understand data and information and garner insights to enhance the decision-making process. Large-scale adoption of cloud technology solutions over the last few years has led to higher volumes of data, but with it comes an urgent need to make sense of it and drive critical business decisions.

According to the report, the first hurdle for businesses is a lack of data quality. More than a third (39%) of respondents citing “completeness”, or a lack of comprehensive data, as an issue. Almost the same number see consistency (38%), and accuracy (35%) as major challenges. The next challenge is the inability to understand data through existing analytics tools, with complexity being a challenge for half (50%) and a lack of training (43%) for almost as many. This need for self-service capabilities is further emphasized by the top priorities for organizations seeking to improve end-user data literacy, which were “making tools more intuitive” (77%) and “enhancing custom reports” (66%).

“As workforces shift to hybrid environments, businesses will continue to adopt cloud technology and as-a-service solutions,” said Monica Boydston, Vice President, Product Management at insightsoftware. “When these new solutions operate in tandem with legacy systems, the result is a large pool of data from multiple sources – ”polluted” data that requires cleaning. Doing this takes time away from the critical work of gathering business intelligence. We can’t eliminate errors

and inconsistencies, but there are tools that can make things easier, paving the way for teams to achieve data fluency.”

Predictive analytics, which requires people, tools, and data to work together, represents the final stage of data fluency, and should be a goal for any data-driven business. Many organizations are not there, yet. Thirty-seven percent of businesses say they cannot extrapolate data to forecast future outcomes, while only 27% of organizations say most users are able to forecast using current analytics tools.

European businesses could unlock €622 billion growth with digital transformation

NEW RESEARCH released by Ricoh Europe reveals that digital transformation could increase EU and UK GDP by 3.4% over the next five years – equivalent to €622 billion of growth.

The research, conducted by Opinium and analysed by CEBR on behalf of Ricoh Europe, polled 6,000 workers and 1,500 decision makers across the UK, Ireland, France, Germany, Italy, the Netherlands and Spain. It finds that business leaders recognise the drain of time-intensive processes on their workforce, with 76% making the automation of tedious tasks a core part of their digital transformation strategy.

But with the average worker currently spending almost a third (30%) of their day on administrative tasks, businesses must accelerate their plans if they are to facilitate these productivity gains and the employee engagement needed to trigger sustained growth. Employees are clearly craving the right workplace technology to help them streamline activities and dedicate more time to fulfilling work. The majority (64%) think they would bring more value to their company if they had access to the right technology, with 78% of these welcoming automation tools as a means of reducing tedious tasks.

Those that implemented automation software in the last financial year experienced an average productivity increase of 14%. This marks a vital gain for businesses looking to remain competitive in markets that are subject to increasing turmoil.

The research also shows that a greater investment in the tools and systems employees are seeking can increase morale and reduce turnover. Workers at businesses which implemented automation tools last year are reportedly more satisfied with their jobs and likely to stay with the company for longer. In fact, of all the technology investments businesses have made, the introduction of automation tools corresponded to the lowest employee turnover of 17%, compared to an average of 19% across other technology options.

SEAGATE

The best of two worlds enables multicloud freedom.

Complement your Storage Solution with Lyve Cloud and Seagate Systems.

- **Multicloud Freedom**
- **Predictable TCO**
- **Always-On Availability**
- **World-Class Security**
- **Ransomware Protection**

SIMPLE TRUSTED EFFICIENT
LYVE™ Cloud

Enable multicloud freedom with Seagate® Lyve™ Cloud—object storage as a service with predictable costs and no hidden fees for better cloud TCO. Lyve Cloud offers you best-in-class security and availability with no egress fees, no API fees, and no lock-ins. This is the answer to storing more data without worrying about TCO, security, and data mobility.

Enhance the benefits of your Seagate brand of on-premises storage systems, protect against unforeseen disasters, and decrease operational burdens by storing data directly to an S3-compatible cloud solution.

More information: www.seagate.com

Top 10 predictions for the future of digital infrastructure

International Data Corporation's (IDC) highlights key, impactful trends for the future of digital infrastructure and its top 10 predictions for the next five years. The article also covers predictions for operations, work and intelligence.

DIGITAL BUSINESSES depend on digital infrastructure – compute and data management horsepower; network connectivity; operational support; and management – to power business applications, analytics, and activities.

IDC's Future of Digital Infrastructure framework provides a model for understanding how a successful digital-first strategy is built on critical digital infrastructure investments across dedicated on-premises datacenters, edge locations, and public cloud resources. Digital infrastructure spans compute, storage, network, infrastructure software (including virtualization and containers) and the automation, AI/ML analytics, and security software and cloud services needed to maintain and optimize legacy and modern applications and data. Ecosystem partners, including systems integrators and channel partners, are also important contributors.

Organizations that optimize hybrid and multicloud digital infrastructure environments consistently realize higher levels of operational resiliency, security, revenue growth, and overall productivity at scale.

"Digital infrastructure provides the underpinning for digital business agility and innovation," explains Mary Johnston Turner, research vice president, Future of Digital Infrastructure. "IDC's 2023 predictions for the future of digital infrastructure identify critical shifts in governance, operations, architecture, and sourcing that need to be factored into enterprise digital transformation

strategies going forward."

IDC's top 10 predictions for the Future of Digital Infrastructure are:

Prediction 1: By 2026, 65% of tech buyers will prioritize as-a-service consumption models for infrastructure purchases to help restrain IT spending growth and fill ITOps talent gaps.

Prediction 2: By 2026, 65% of IT organizations will only purchase infrastructure solutions that incorporate predictive cyber-resiliency mechanisms proven to reduce post-cyberintrusion recovery efforts.

Prediction 3: By 2027, AI-enabled automation will ensure consistent digital infrastructure configuration, performance, cost, and security by reducing the need for human operations intervention by 70% and improving SLOs.

Prediction 4: By 2023, amid ongoing IT supply chain disruptions, 80% of G5000 infrastructure customers will adopt proactive multisourcing strategies to protect themselves against future IT supply risks.

Prediction 5: By 2024, 40% of digital business apps will depend on contractually guaranteed cross-provider data transfer and operational/financial data sharing agreements between public clouds and on-prem tech partners.

Prediction 6: By 2026, 95% of companies will invest in fit-for-purpose, heterogeneous compute technologies that deliver faster insights from complex data sets to drive differentiated business outcomes.

Prediction 7: By 2025, 70% of the G2000 will prioritize the trusted infrastructure of sovereign clouds to ensure consistent security and local/regional regulatory compliance for specific sensitive workloads and data.

Prediction 8: By 2025, to ensure data and workflow integrations spanning distributed clouds and edge environments, 50% of enterprises will deploy multicloud networking, bringing consistency and simplicity to NetOps.

Prediction 9: By 2027, the need for faster, higher-quality data-driven decisions will cause 80% of G2000 CIOs to mandate companywide data logistics strategies for data management, protection, and integration.

Prediction 10: By 2024, due to economic pressures, 50% of G2000 will prioritize infrastructure vendor selections based on tech partner ecosystems that offer cost savings provided by preferred pricing and support deals.

Top 10 predictions for the future of operations

The top 10 predictions for the Future of Operations from International Data Corporation (IDC) illustrate how the next five years will be transformational for operations as organizations find new and more effective ways to manage, analyze, and collaborate around their operational data. The impacts will extend beyond the data, affecting how decisions are made and who makes them. It will also impact which roles are needed, who fills those roles, and how organizations manage their operations. Operational excellence and resilience continue to present challenges across industries, as businesses struggle with supply chain disruptions, rising energy costs, talent constraints, and pressure to improve sustainability metrics.

Becoming a data-driven organization is a journey that requires an honest assessment of the current state and a willingness to embrace the changes necessary to improve operational performance. Recognizing the need for new approaches and technologies, IDC has developed the Data-Driven Operations (DDO) framework and maturity model to help organizations benchmark themselves and develop plans to improve operational performance across multiple dimensions – efficiency, productivity, quality, safety, reliability, and sustainability.

According to Leif Eriksen, research vice president, Future of Operations at IDC, "Data-driven operations is a journey but this should not be interpreted as a reason to be complacent. The pace of change in operations is beginning to accelerate and will result in significant realignments across a range of industries. Organizations that recognize the opportunity will thrive; those which fail to see it will not survive."

IDC's predictions for the Future of Operations are:

Prediction 1: By 2025, 50% of G2000 industrial organizations will make real-time decisions balancing economic and sustainability metrics, simultaneously improving both sets of metrics by 5% across the enterprise.

Prediction 2: By 2026, 40% of product-centric organizations will use digital tools to measure life-cycle carbon footprint, creating demand for better integration between PLM and operational data.

Prediction 3: By 2023, talent shortages and pressure to improve operational performance will force organizations to reevaluate their approach to digital transformation, resulting in greater use of outside services.

By 2024, due to economic pressures, 50% of G2000 will prioritize infrastructure vendor selections based on tech partner ecosystems that offer cost savings provided by preferred pricing and support deals

Prediction 4: By 2027, the use of extended reality technology, including AR/VR/MR tools, will increase by 40%, creating a new breed of digital worker and reducing operator/field worker errors by 30%.
Prediction 5: By 2026, the use of robots in nontraditional sectors, most notably remote inspection and maintenance, will increase by 35%, resulting in a 50% drop in inspection errors.
Prediction 6: By 2023, digital-first operations enabled by 5G connectivity will improve worker safety, resulting in a 20% reduction in lost time accidents.
Prediction 7: By 2027, 50% of remote operations will use satellite-enabled AI/ML technology to collect and analyze data at the edge, reducing costs and improving yields and energy usage in the natural resource sectors.
Prediction 8: By 2024, the cloud will surpass on-premises infrastructure as the primary location where operational data is stored, managed, and analyzed for 50% of G2000 organizations.
Prediction 9: By 2024, 30% of industrial organizations will have become leaner and more agile than their competitors as a result of making real-time operational insights available anytime, anywhere, to anyone.
Prediction 10: By 2025, 50% of organizations will increase the use of IoT and OT cybersecurity solutions at the edge, cutting OT cybersecurity breaches in half.

Top 10 predictions for the future of work

International Data Corporation (IDC) has also announced its Future of Work predictions for 2023 and beyond. With global attention divided between many disruptors, the future of work is fraught with many unknowns, from where and how work will be done to how economic pressures will change job opportunities to how social, skills, and climate concerns will have a broad impact. Hybrid work, once thought to be a temporary means of enabling enterprises to continue business operations through the COVID-19 pandemic, has become a mainstay for our global future work landscape.

The reality of our current global economic, climate, and business challenges requires workers to be a part of dynamic and reconfigurable teams that can quickly adapt to business demands and new market requirements — anytime, anywhere, and from any physical location.

The promise of such hybrid work models is clear. Rapid adoption of more automated, cloud-based, and artificial intelligence (AI)-enabled work practices drives increased work productivity and introduces new, more agile ways of working. Insights from more digital-first ways of working are enabling organizations to be responsive to the needs of customers and employees alike, driving improvements in talent acquisition, employee retention, and customer satisfaction.

“The next five years will mark a period of distinct change in both the mechanics and social attitudes surrounding normalized work practices,” said Amy Loomis, research vice president, Future of Work at IDC. “As organizations wrestle with different elements of work transformation from technology adoption to new policies and practices, hybrid work will drive new technology solutions across functions and industries alike.”

IDC’s 2023 Future of Work predictions outline the framework for technology-related initiatives in the years ahead that can be leveraged by IT, human resources (HR), and other line-of-business (LOB) decision makers and influencers. The predictions are:
Prediction 1: To address health, sustainability, travel, and other disruptions, 30% of G2000 organizations will adopt immersive third-party metaverse conferencing tech services to enable client engagement by 2027.
Prediction 2: By 2024, the business developer role will be ubiquitous, with more than 60% of enterprises training and supporting business users to build their own applications and automated processes using low-code tools.
Prediction 3: Driven by skills shortages, CIOs that invest in digital adoption platforms and automated learning technologies will see a 40% increase in productivity by 2025, delivering greater speed to expertise.
Prediction 4: By 2024, organizations deploying employee micro-monitoring measures (camera/keystroke) will see a 20% decrease in actual employee productivity.
Prediction 5: G2000 companies that deploy reactive and tactical hybrid work models will see a 20% revenue loss in 2024 due to job attrition and underperforming teams.
Prediction 6: By 2025, organizations that have created dedicated hybrid security policies and developed a culture of trust will be 3x less likely to suffer a security breach.

Prediction 7: By 2024, companies offering frontline workers democratized access to digital collaboration, process automation, and similar tools will see a 20% increase in revenue due to improved productivity.
Prediction 8: Holistic and integrated analytics within an intelligent digital workspace (IDW) ecosystem will drive a 70% increase in differentiated business outcomes for adopters by 2026.
Prediction 9: Effectively blurring space and place, by 2025, 65% of G2000 companies will consider online presence to be at parity to «in real life» across their engaged workforce.
Prediction 10: By 2024, 55% of C-suite teams at global enterprises will use intelligent space and capacity planning technology to reinvent office locations for gathering, collaborating, and learning.

Top 10 predictions for the future of intelligence

IDC's enterprise intelligence benchmarking research shows that maturity in enterprise intelligence makes a material difference to business outcomes. Top-quartile enterprise intelligence performers are 2.7 times more likely to have experienced strong revenue growth over 2020–2022 and 3.6 times more likely to have accelerated their time to market for new products, services, experiences, and other initiatives.

Improving enterprise intelligence performance will often require concerted investment and action at multiple levels: from data platforms (to enable more openness, flexibility, scale, and connectivity) and pipelines and processes (to enable more effective, consistent processing of data to make it "insight ready") to tools (to build and deliver analytics and insights), decision-making and action-taking processes, and culture.

Organizations that invest in enterprise intelligence will find that they are more digitally resilient, agile, innovative, and dynamic than their peers. "Enterprise intelligence allows organizations to thrive in all macroeconomic conditions. Predictions in this IDC FutureScape detail key trends that are going to occur in the next one to five years that executives should be aware of as they strive to increase their enterprise intelligence," said Chandana Gopal, research director, Future of Intelligence at IDC.

The following ten predictions represent the trends IDC expects to see across the four pillars of enterprise intelligence: data culture, information synthesis, information delivery and collective learning.
Prediction 1: By 2024, organizations with greater enterprise intelligence will have 5x institutional reaction time, resulting in persistent first-mover advantage in capitalizing on new opportunities.
Prediction 2: By the end of 2025, vigilant C-suite leaders of G2000 will invest 40% more on enterprise and market intelligence, helping them counter the recession and slice through the storms of disruption.
Prediction 3: By the end of 2024, 30% of enterprises using video surveillance technologies will also be using video data analytics to support operational decision making requiring more oversight.
Prediction 4: By 2024, 80% of G2000 companies will increase investment in intelligence about threats/opportunities to local operations posed by external threats such as supply chain disruptions.
Prediction 5: 30% of G2000 organizations will fail to deliver on their enterprise intelligence goals by 2026 because they have not centered trusted capabilities in their efforts to develop data culture.
Prediction 6: By 2025, real-time intelligence will be leveraged by 90% of G1000 to improve outcomes such as customer experience by using event-streaming technologies.
Prediction 7: By 2027, 66% of large enterprises will make major investments in data control plane technologies that can measure the risk inherent in data and reduce risk through security and screening.

Prediction 8: By the end of 2025, more than 50% of G2000 organizations will face penalties if they do not use AI for detection and automatic remediation of data due to growing complexity, volatility, and resource scarcity.
Prediction 9: Facing increased demand for enterprise intelligence skills and to meet employee expectations, 70% of G1000 will have formal programs fostering data literacy and upskilling by 2028.
Prediction 10: By 2026, 30% of G1000 companies will extend investments in AI infrastructure to performance-intensive computing to solve the most complex problems using HPC-driven simulations to improve outcomes.

The top trends impacting infrastructure and operations for 2023

Gartner, Inc. has highlighted the six trends that will have significant impact on infrastructure and operations (I&O) over the next 12 to 18 months.

"THE CHANGES that I&O teams face are shifting views of how to purchase, deploy, and manage technology solutions for optimal business results," said Jeffrey Hewitt, research vice president at Gartner. "Furthermore, the rapid increase in solution complexity and deployment scenarios is challenging I&O leaders to approach skills, roles and career path management from a different perspective."

Here are the top trends impacting I&O in 2023:

Trend No. 1: Secure Access Service Edge (SASE)

SASE is a single-vendor product that is sold as an integrative service which enables digital transformation. This trend connects and secures users, devices, and locations as they work to access applications from anywhere. Gartner forecasts that total worldwide end-user spending on SASE will reach $9.2 billion in 2023, a 39% increase from 2022.

"Hybrid work and the relentless shift to cloud computing has accelerated SASE adoption," said Hewitt. "SASE allows users to connect to applications in a secure fashion and improves the efficiency of management. I&O teams implementing SASE should prioritize single-vendor solutions and an integrated approach."

Trend No. 2: Sustainable Technology

Sustainable technology encompasses sustainable IT within the context of a tech-enabled enterprise and customer sustainability. This trend involves four key aspects: environmental, social, governance (ESG) and economic. With a recent Gartner survey revealing that 87% of business leaders expect to increase their organization's investment in sustainability over the next two years, I&O must embrace sustainable technology to support organization-wide ESG goals.

"I&O has an opportunity to be a key part of enterprise sustainability efforts," said Hewitt. "From improving the sustainability of data centers and the cloud to embracing the IT circular economy for devices, I&O can promote sustainable technology by improving efficiency and performance of infrastructure assets."

Trend No. 3: Platform Engineering

Platform engineering is the unity of management tools and various components of infrastructure technologies such as application resource management (ARM), application performance monitoring (APM), digital experience monitoring (DEM), and digital platform conductor (DPC) tools. This trend enables user-driven, self-service infrastructure and deployments that extend the principle of continuous integration and delivery, furthering I&O agility, speed, efficiency, safety, and compliance.

I&O can embrace platform engineering by determining what skills and competency gaps exist within I&O organizations and creating a plan to fill those gaps. Adopting practices such as automation can enable self-serviceability.

Trend No. 4: Wireless Value Innovation

I&O can leverage multiple wireless technologies to extend business disruption opportunities beyond connectivity. Overlaps between various technologies including Wi-Fi, 5G, Bluetooth and high frequency (HF) facilitates connectivity solutions and creates innovation opportunities.

"Wireless value innovation creates a scalable return on wireless investment and makes networks a strategic innovation platform," said Hewitt. "However, there is significant complexity at play and several new skills that are required to achieve this innovation, such as wireless integration capabilities and wireless tracking implementation experience."

Trend No. 5: Industry Cloud Platforms

Public cloud is not one-size-fits-all. Industry clouds are an alternative to enterprises purchasing a variety of cloud offerings, as they provide a pre-integrated solution that coincides with specific vertical market needs.

Industry cloud platforms are a combination of traditional cloud services with tailored, industry-specific functionality. Organizations looking to accelerate time to value, leverage composability to build differentiating digital products and services and benefit from cross-industry innovations are turning to these solutions. Gartner predicts that by 2027, more than 50% of enterprises will use industry cloud platforms to accelerate their business initiatives.

Trend No. 6: Heated Skills Competition

As digital implementation continues to grow, there is a greater demand for a wide variety of skills within I&O organizations. Yet, there is a limited talent pool available for high-demand skills, including expertise in cloud, automation, and advanced analytics. Simultaneously, some organizations are creating I&O positions within business units, which increases internal competition for skills.

"While competition for new skills creates more career opportunities for I&O leaders, it can also cause talent gaps within an organization to be more costly to fill and can create challenges retaining employees," said Hewitt. "I&O leaders must become more sophisticated in their thinking around the value proposition of their teams. Consider tools to identify upcoming skills requirements and new training approaches to enrich the skills of existing employees, to reduce the risk of them moving to other business units or competitors."

Customer data and analytics are top priority

Customer service and support leaders cited customer data and analytics as a top priority for achieving organizational goals in 2023, according to a survey from Gartner, Inc.

IN A GARTNER ONLINE SURVEY of 283 customer service and support leaders from August-October 2022, 84% of customer service and service support leaders cited customer data and analytics as "very or extremely important" for achieving their organizational goals in 2023. Eighty percent of respondents ranked digital channel effectiveness as "very or extremely important," along with employee performance, development and quality assurance.

The Gartner survey revealed improving operations and growing the business are the two most important business goals for 2023.

"Understanding customers' needs and expectations for their service experience is integral for improving loyalty and creating customer value, especially when organizations are up against economic headwinds," said Jonathan Schmidt, Sr Principal, Advisory in the Gartner Customer Service & Support practice. "Executing on this vision requires investment in customer data and analytics, knowledge management, and an enduring partnership with IT."

In light of recent economic headwinds, customer service and support leaders plan to devote more resources to improving, automating or eliminating inefficient processes (59% of respondents), migrating service volume to digital and self-service channels (51%) and contributing to the top-line by creating customer value (46%) in the near future.

"In tough economic times, customer service and support leaders are often encouraged by their CFOs to make do with what they have," said Schmidt. "Given how difficult it is to hire and retain talent, it makes sense that they are tackling inefficiencies and prioritizing digital channels as a strategy for driving down costs without reducing headcount or sacrificing customer experience."

With these survey findings in mind, Gartner recommends customer service and support leaders:

- **Collect actionable customer data across channels** through a robust VoC program that goes beyond surveys and incorporates more advanced methods such as speech, text and digital experience analytics. Leveraging these methods for decisions on personnel, processes and technologies, is key to a successful customer service function.
- **Build digital self-service teams** to oversee the digital channel strategy, manage channels like products, and work closely with data analysts to develop and measure success metrics.
- **Enable customer service agents with technology,** such as connected desktops, to help them better guide customers through resolution.

Worldwide low-code development technologies market to grow 20% in 2023

The worldwide market for low-code development technologies is projected to total $26.9 billion in 2023, an increase of 19.6% from 2022, according to the latest forecast from Gartner, Inc.

A RISE IN BUSINESS TECHNOLOGISTS and a growing number of enterprise-wide hyperautomation and composable business initiatives will be the key drivers accelerating the adoption of low-code technologies through 2026.

“Organizations are increasingly turning to low-code development technologies to fulfill growing demands for speed application delivery and highly customized automation workflows,” said Varsha Mehta, Senior Market Research Specialist at Gartner.

“Equipping both professional IT developers and non-IT personas – business technologists – with diverse low-code tools enables organizations to reach the level of digital competency and speed of delivery required for the modern agile environment.”

Low-code application platforms (LCAPs) are projected to be the largest component of the low-code development technology market, growing 25% to reach nearly $10 billion in 2023 (see Table 1). While LCAP is the largest market segment, citizen automation development platform (CADP) is projected to grow at the fastest pace, with a 30.2% growth forecast for 2023. Typical use cases of CADP include automating workflows, building web-based forms, bridging data and content across multiple software-as-a-service applications and creating reports and data visualizations.

“The high cost of tech talent and a growing hybrid or borderless workforce will contribute to low-code technology adoption,” said Jason Wong, Distinguished VP Analyst, at Gartner. “Empowered by the intuitive, flexible and increasingly-powerful features of low-code development tools, business technologists and citizen technologist personas are developing lightweight solutions to meet business unit needs for enhanced productivity, efficiency and agility — often as fusion teams.”

Gartner predicts that by 2026, developers outside formal IT departments will account for at least 80%

of the user base for low-code development tools, up from 60% in 2021.

Hyperautomation and Composability to Drive Low-Code Adoption

Interest in hyperautomation continues to grow due to rising operational optimization demands, a widening skills gap and increasing economic pressures. Gartner forecasts that the spending on hyperautomation-enabling software technologies will reach $720 billion in 2023. A portion of this spending will be directed at low-code development technologies including LCAP, iPaaS, RPA, CADP and MXDP, to support process automation, integration, decision analytics and intelligence use cases.

Investments in low-code technologies that support innovation and composable integration will also grow as organizations embrace the composable enterprise. Composable enterprises require better reuse of existing packaged business capabilities (PBCs) for agile application development and to create custom user experience for new workflows and processes.

"Low-code development technologies are supporting the composable enterprise by enabling the creation of more agile and resilient software solutions," said Wong. "These technologies can be used to compose and recompose modular components and PBCs, to create adaptive custom applications for changing business needs."

	2021	2022	2023	2024
Low-Code Application Platforms (LCAP)	6,324	7,968	9,960	12,351
Business Process Automation (BPA)	2,416	2,585	2,761	2,940
Multiexperience Development Platforms (MDXP)	2,081	2,508	2,999	3,563
Robotic Process Automation (RPA)	2,350	2,892	3,401	3,879
Integration Platform as a Service (iPaaS)	4,680	5,668	6,668	7,838
Citizen Automation and Development Platforms (CADP)	554	732	953	1,232
Other Low-Code Development (LCD) Technologies*	92	109	126	146
Total	**18,497**	**22,462**	**26,869**	**31,949**

➤ Table 1. Low-Code Development Technologies Revenue (Millions of U.S. Dollars)

Source: Gartner (December 2022)

*Other low-code development technologies include rapid mobile app development (RMAD) tools and rapid application development (RAD) tools. RAD tools are/were on-premises only and desktop-bound applications mainly. Low code is the evolution of RAD to cloud and SaaS models.

Notes: *Gartner defines a no-code application platform as an LCAP that only requires text entry for formulae or simple expressions. The LCAP market, therefore, includes no-code platforms. Furthermore, "no code" is not a sufficient criterion for tasks like citizen development, as many complex tooling configuration tasks are no code but still require specialist skills. Columns may not add to totals shown because of rounding.*

View from a retail CIO:

The rush into digitisation, the shortage of talent, and supply chain disruption is changing the role of the CIO for ever

The retail sector is just emerging from the backdrop of intense pandemic-induced digitisation, only to find itself in an environment with many more external pressures – from the tech talent shortage to outstanding technical debt and supply chain pressures. Here, **NEIL HOLDEN, CHIEF INFORMATION OFFICER, HALFORDS,** reflects on the lessons Halfords has learned even before the pandemic, and offers some best practice advice to CIOs and CTOs as they plan and execute digitisation strategies in the current retail industry landscape.

FROM MY POSITION as a retail group CIO, the demand for digital services in the sector has increased exponentially, and I'm talking prior to the impact of the pandemic. What the pandemic did do, was shorten IT planning horizons almost by half – tech projects that might have initially been specified for six months, may have needed to take place in three months. This led to retail CIOs, CTOs and IT teams working to shorter timelines than ever before, but the ripple effect is still being felt across the sector.

Retail pressure points

As things have returned to a new normal, there are a number of pressure points and challenges facing retailers that are still looking to digitise their front and back-office operations. Here's the list:

- **Tech Talent Shortage**
  A lack of in-house technology experts, can

hold back most digitisation initiatives. Deloitte, for example, has recently highlighted the software engineering shortage, where stats show more than 90% of IT leaders plan to expand their modern software engineering and cloud environments, yet 80% say inadequate employee skills are holding them back.

- **Tech Talent Retention**
  On the flip side of a shortage of new employees, there is an increased focus on already available in-house skills and retaining current staff. This means retail leaders and CTOs need to look at making current staff feel gratified and rewarded, while even offering them opportunities to train, upskill and cross-skill in new areas to keep them in their organisation.
- **Guaranteeing Consistency –** then there are the overwhelming demands for a consistent customer experience, regardless of their retail channel of choice. This means harmonising in-store and online experiences for an extremely discerning customer-base.
- **Technical Debt**
  Legacy systems, often using older hardware and software do not lend themselves to the flexibility and consistency required for modern retail. This means balancing investment in new solutions vs. rationalising or customising what may already be in place.
- **Supply Chain Pressures**
  Then there are the global factors that can be out of the control of even the best-laid retail digitisation plans. Hardware availability can cause project delays and budget inflations – for example lead times are growing for critical network equipment including routers and SD-WAN equipment. Consider this assessment from EY: "Physical and digital retailing will not be an either-or choice". Given this, it's hardly surprising that the EY Reimagining Industry Futures 2022 study confirms how external factors have spurred the pace of digital transformation in retail. Seventy-five percent say the COVID-19 pandemic has accelerated their digital transformation plans. As retail activity continues to ramp back up and net out between the digital and physical worlds, there are clearly still a lot of obstacles to navigate for industry technology projects.

Halfords has walked the walk and its tech talks the talk

In my time at Halfords my focus has been on delivering the technology to support the business strategy to evolve into a consumer and B2B services-focused business, with a greater emphasis on motoring and motoring services.

A key part of this involved bridging Halfords's physical assets - now over 400 stores, 656 garages, 253 consumer vans, 440 commercial vans and 9 warehouses - and the putting all the digital elements into one end-to-end, consistent customer experience.

We already had a data lake, the perfect launchpad for a new approach to service delivery

Operational and technological integration forms a key part of this strategy – at the group level across retail, garage and mobile – to provide a de-siloed and holistic view from a centralised data lake. The Halfords web platform plays a critical role in this strategy, replacing different sites for different parts of the business and consolidating down to a single user experience. With people cautious about leaving their homes in the early days of the pandemic, we saw online sales figures jump from 20% to 80% of total overnight.

On the mobile and garage management side, the company built its own end-to-end service platform, Avayler, which tracks the skills level of a technician, work hours and the work undertaken. The platform currently manages more than 70,000 services per week. The Halfords Mobile Expert van operation, which has a 4.8/5 Trustpilot rating, has seen a 70% increase in job productivity and more than 200% increase in utilisation since it started using the platform, demonstrating the potential for greater customer satisfaction.

Five keys that unlock the power for CIOs and for CTO strategy

I have found that there are five key strands for retail CIOs, CTOs and other tech leaders to keep in mind for their digital strategies.

1. **Empower your workforce**

Given the aforementioned talent shortage, this is even more important than pre-pandemic. In-store employees and mobile technicians alike are used to easy to operate apps and services in their everyday lives. Any retail digitisation strategy should reflect these expectations.

This means designing choosing the right devices,

apps and portals that deliver the right information and the right services to the employee in question – allowing them to execute

their task and log information quickly and effectively. Pass on this ease of service to your workforce and the benefit will be passed downstream to customers as well.

2. Have the customer at the heart
This is easy to say, but harder to actually achieve from a technology perspective. This applies not just to the end result of digital transformation programs, but during design and implementation as well. Customers still need to access your products and services throughout the course of a digitisation strategy, so this needs to be factored into planning, testing and roll-out. There also needs to be no disconnect between colleagues and customers when it comes to using the technology deployed.

cloud-based deployments can be easily enhanced with additional functionalities such as artificial intelligence. Again, our Avayler solution is an example here, where dynamic job/technician scheduling or dynamic pricing can be overlayed on top of existing systems to increase efficiency and profitability from every customer interaction

3. Understand your data
It's all fine implementing smart devices across stores and service operations, but retailers – particularly large group organisations – are missing a trick if they don't harness data from all channels. Disparate pockets of data can lead to inaccurate analysis and that could mean leaving revenue on the table and less optimal tech performance for employees and customers.

This is where deploying in the cloud can help with data collection, analysis and action – giving retailers a single picture of the truth, governance, ownership and control over every data stream in across operations.

4. Go modular
Gone are the days of big monolithic retail implementations. APIs, microservices and modularisation are the way to go for modern cloud-based retail software implementations. This means retailers can pick and choose what solutions make sense for their business goals, keep implementation times down, but also make sure they are keeping that digital thread of data at the core of their business operations.

The Avayler platform for example, is split into a suite of software products that can be deployed for mobile service, or in-store/garage processes, depending on the needs of the retail organisation.

5. Automate and adopt new tech
The advantage of this modular approach is the ability to quickly introduce new technologies and processes across the organisation into the future. Manual processes or legacy technology is very difficult to adapt and even more difficult to automate.

Again here, cloud-based deployments can be easily enhanced with additional functionalities such as artificial intelligence. Again, our Avayler solution is an example here, where dynamic job/technician scheduling or dynamic pricing can be overlayed on top of existing systems to increase efficiency and profitability from every customer interaction.

Tightened collaboration with tech vendors in the retail ecosystem

The same EY report I cited earlier found 63% of the retail respondents say that the pandemic has driven a closer collaboration between their organisation and technology providers. The report concludes "However, if they are to get to where they need to be at the required pace, it is simply not possible to recruit or train the right talent fast enough. They will have to find alternative ways to get the skills they need – and collaboration is the only feasible option." It's inevitable that the path to retail digitisation will involve more integrations and collaborations with technology vendors. Perhaps the role of the Chief Information Officer should now be renamed Chief Integration Officer? Thoughts?

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

The six mistakes keeping business from dominating the decade of data

It has been said, not least by my business, that we are living in the 'defining decade of data'. I can say this because of the unique place we've arrived at in human history.

BY DAMIEN BROPHY, VICE PRESIDENT EMEA, THOUGHTSPOT

IF 'data is going to change the world' sounds like something you've heard before, that's because you have. For years, technologists, futurists, and business leaders have predicted a revolution in every pocket of society, powered by data.

It would be perverse to argue that data hasn't changed the world, though it would be fair to say it's been a hard road to get to the place where a modern cloud analytics stack makes data monetisation, sticky apps, and embedded analytics practical and easy. And that's saying nothing of the basic promise of business intelligence that is merely timely and useful. But now these things are here and in practice daily throughout the world, from neobanks to restaurants and even global technology giants.

Behind these changes are a swathe of massive technology trends. The cloud has gone mainstream. With cloud analytics, businesses can get real-time insights based on real-time, live data. And anyone in an organisation that wants to take on the role of a business analyst, can, with self-service analytics powered by search (think a 'Google for data' approach to asking questions) and AI - providing the guardrails and support to channel our curiosity to appropriately secure the right answers.

In this defining era, there is massive opportunity for organisations who can turn these trends into tailwinds that drive the next decade of success. Doing so, however, requires recognizing and ending the data mistakes that have held our industry back. Here are the six I see data leaders make most often that will hold you back from dominating the era ahead:

Six mistakes that knock you back a decade

"It's good enough now." No. This should be a simple one. Don't settle for the technology offering the features that gave us dead-end dashboards with inert, past data, slow requested analytics turnaround times, restricted only to a select and expensive few. Get the best of breed solutions to create your own modern data stack. Many existing solutions are SaaS based and making change isn't particularly disruptive. There isn't so much of a price trap set by one preferred vendor anymore that means settling for several OK solutions makes financial sense. Plus, set that against the very real fact that 'good enough' doesn't lead to greatness. It never has and never can.

"I only want the specialists investigating our data." No. That slows down the analytics process and ensures a divide between insights and domain experts. Now everyone can be a business analyst, even in small ways. Search and AI guardrails exist

to empower everyone through truly self-service analytics. No learning to code, not necessarily sending insights off to an analytics specialist. They have a very real role to play, but not every organisation needs one, and where they are employed most usefully isn't by being locked away in a cupboard as part of an insights team.

"We have to pass this through the existing process." No. No more dashboards, no more slow processes, no more multi-person reviews. Action based on data should be really easy. Insights and ideas really are great but can't die on an unread report sitting on a desk. Plus, to put the boot into dashboards again - insights don't spark action if all they do is raise another question that can't be immediately acted on. Question, answer, insight, action – in real-time. This is what breaks the rocks in front of organisations today. Be active and reactive, not part of the passive legacy data queue.

"But our execs really love their dashboards." No. Stop using the d-word. Dashboards are dead. There's no perfect data warehouse. Create freedom by building flexible data foundations. Practitioners and domain experts should be able to use the data platforms and solutions that work for them. Teams have different needs and need to interact with data the way they must to do their jobs. Solutions should offer governance, structure, and automation that allows them to work in the way they want. Cloud solutions now offer this.

"Our data is all we need." No. Your data is good, but their data will combine to make it better. Don't' neglect to make use of third-party data to make smarter models, solutions, apps, and services. The cloud and APIs make this so easy, there's no excuse to be backward. Now business leaders can have truly holistic views on their industry and customers, and offer powerful services to customers. Think of an app like Uber. Mapping data is part of the power, but knowing where all these other parties are, the drivers, gives it its power. Sharing data with trusted partners makes a more powerful product for everyone.

"We had to make it this way, for us." No. Put users first. We are not in the world of 'do as I say' anymore, that's a relic of older, unwieldy, technologies. Users know what good UX looks like stubborn and they want a personalised experience that lets them do their job. Changing a role to fit pre-packaged software is a very 1990s concept - it;s as dead as those dashboards. Analytics can become part of an engaging user experience in any business application. Embedding it where users want to use it means their decision-making becomes data-led. Getting over these six mistakes enables teams to make better decisions based on the signals that matter, combined with their existing domain knowledge. That means bright people working the way that they want to achieve better results. Sounds like a good way to create a legacy of innovation and success.

Moving your database to the cloud – what are your options?

Attitudes to cloud databases have changed massively in recent years. Research firm Gartner estimates that cloud-hosted databases accounted for $39.2bn of market revenue in 2021, growing significantly over the last two years to almost become the favoured choice overall compared to on-premises equivalents (49%).

BY MARC LINSTER, CTO, EDB

AS BUSINESSES PLAN their cloud migration, they look for technologies that can help them compete and react in a landscape that values speed and quality over everything else. This means solutions that provide agility, scalability, high performance, and security, while also minimising the time spent on maintenance, provisioning, and administrative overhead. Choosing the right database strategy, and along with it, the right cloud migration, is particularly critical for overall success.

That being said, choosing the right approach can be confusing, with many options available. Let's look at why enterprises are considering cloud migrations and what choices they have for their database strategy.

Key drivers for moving from on-premises to the cloud

Enterprises are looking to the cloud to get more freedom, flexibility, and greater agility for their technology infrastructure in order to innovate faster. The automation and abstraction cloud services

provide enterprises allows them to be more flexible, responsive and focused on activities that drive business value instead of activities that are routine and overhead. We're far enough along in the existence of cloud computing to know that on-premises technology can limit the ability to innovate quickly.

Moving to the cloud helps with agility because we can separate the work to innovate, that is, write new code, new queries, and new business procedures, from the work to run and maintain the infrastructure. In an on-premises scenario, when the business needs a new database, the enterprise team has to procure hardware, rack and stack it, install the OS, and integrate everything into the corporate infrastructure before turning it over to the application team, who will focus on the actual business value add. That's a process that can easily take weeks. In a cloud environment, the new database can be provisioned in 20 minutes!

Similar issues limit the ability to be innovative. Cloud database platforms offer a wide range of services that allow for experimentation and use of speciality technology for single projects. This is essential for prototyping new ideas. On-premises deployments commonly require a bigger commitment to technology regarding licences, hardware, and operational skills. This makes it much harder for enterprises to quickly try something new. And once they do try something new, they tend to be committed to long-term licences – which makes 'fail fast' impossible.

Globalisation is another contributing factor for the move to the cloud. Data needs to be stored close to the user for performance and compliance reasons. On-premises models for these needs are prohibitively costly and are too complex to meet the rigorous demands of global internal teams, suppliers, and customers.

Databases are historically resource-intensive to keep highly available and maintained. On-premises, they require whole teams to maintain, update, and provision the database, perform backups, plan for disaster scenarios, and implement recovery. These overhead activities are prime targets to delegate to an 'as a service' deployment.

'As a service' options for cloud databases

There are three options to take a database to the cloud: virtual machines (VM), containers, or Database-as-a-Service (DBaaS). The DBaaS market is growing at an exponential rate, with recent research predicting the market size to grow to $2.8 billion by 2025, doubling within five years.

While DBaaS is currently the most popular option for moving to the cloud, VM deployed through Infrastructure-as-a-Service (IaaS) and containers with Kubernetes also have significant success in the market.

Pros and cons of DBaaS

In DBaaS, the cloud database operator (CDO) assumes key responsibilities: managing the software, the hardware, and the network, while assuming responsibility for the service availability. That's the biggest advantage – the DBaaS customer doesn't have to worry about those tasks. However, the biggest consideration is that you, the customer, are completely dependent on the CDO to discharge these tasks well and in a timely manner that does not interrupt the database service. You also may not dictate when your CDO decides to update, or not, your database. For example, one major DBaaS vendor for Postgres, the free, open-source relational database management system, lagged in providing the latest version of open-source Postgres by over two years.

Another challenge arises from the lack of customisation. As the CDO is responsible for maintenance of the operating system and the installation of the database software the user will not be granted operating level access, which means that certain configuration parameters, logs, and software add-ons will not be accessible for tuning and diagnostics.

But even with these few drawbacks, more and more enterprises want their IT resources focused on innovation and business-oriented value add, such as data stewardship and analytics. In our experience, businesses are more than happy to leave the behind-the-scenes grunt work that keeps the lights on to a cloud database provider.

Overcoming the drawbacks

Some public cloud providers will offer Postgres to varying degrees, however, there are benefits to choosing a provider that offers a fully managed Postgres service.

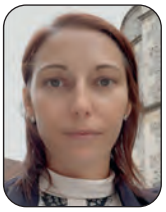
IT leaders should be looking for service providers that offer a choice of Postgres. For example, there is the choice of open-source PostgreSQL or EDB Postgres Advanced Server, which includes additional enterprise features not found in the open-source version – things like compatibility with Oracle. Certain providers will also be more up-to-date with Postgres, and support the latest versions. A second major advantage in finding the right provider is the Postgres expertise available within their team. Only a handful of providers can boast that they have decades of experience in Postgres, and those that do will be able to provide some of the best support available in the industry.

In an increasingly hybrid cloud world, businesses are looking for providers that can gradually shift workloads from on-premises to the cloud, and having the freedom to choose which cloud provider they want. Whether it's AWS, Azure, or another CDO, having a provider that offers flexibility is vital when looking at options in moving your database to the cloud.

Navigating data overload in the life sciences sector

With digital transformation and rapid advances in technology meaning change in the market is swift and constant, businesses must keep up, or face being left behind. While it has always been the case that being responsive to needs and trends better positions you for business success, there is no doubt that in 2022, such agility is essential to it. The life sciences industry is no exception.

BY MICHELLE GRAFTON, REGIONAL HEAD OF SOLUTION SPECIALISTS ESA, IRON MOUNTAIN



Agility is key to growth

A recent McKinsey study found that businesses that had gone agile typically delivered 30% gains across key areas like efficiency, operational performance, customer satisfaction, innovation, and employee engagement. And, just as in any other industry, the best way to stay agile in the life sciences sector is by leveraging insights into your users and markets to make data-driven decisions and inform your future roadmap and forecasting.

Such data is in plentiful supply these days. Around the world, data is being generated at a tremendous rate, particularly since Covid drove a sharp increase in remote and hybrid working. Predictions from the International Data Corporation suggest that the amount of digital data created between 2020 and 2025 alone, will be more than double the total data created since the advent of digital storage.

Data informs development

In the life sciences sector, data is accumulating at speed. Patient information is increasingly transacted and processed online and post-Covid, patients receiving virtual consultations has become a commonplace fixture of modern healthcare and increasingly, virtual clinical trials are taking place. There is valuable data everywhere that has the potential to impact enormously on industry development and innovation, but those benefits cannot be realised if life sciences organisations do not have the tools to analyse the data they are collecting.

Data insights have the power to do so much in the life sciences industry if the data is aggregated, synthesised and presented effectively. From the discovery of revolutionary therapies and faster product development processes, to system

efficiencies and improved patient experiences, data has endless power to unlock new routes within the industry. However, the reality is that most businesses are focused on their day-to-day, rather than investing in the time and expertise needed to make the most of these insights. Especially now, when data is piling up at such volume in the sector, life sciences companies need to be embracing tech solutions that can process it for them and identify opportunities to improve care and research. There are technology-based tools available to do all the heavy lifting and these solutions enable us to draw out all the information our data is trying to tell us.

Enter Machine Learning

As the quality, volume and frequency of new data improves, life sciences have a golden opportunity to improve too. Widespread digital transformation offers incredible new avenues of information. When legacy systems are updated and formerly analogue processes digitised, reams of new data points and insights are generated. Companies can use their data to innovate more, create better products, services and experiences for their customers and patients, and provide better employee experiences for their own staff.

The problem is, so much of the data being collected and stored is unstructured and incompatible with other data. It also tends to be spread out over multiple cloud providers. Therefore, the first challenge is harmonising all the data across the organisation and the services it delivers. The second is determining which data should be kept and which deleted. A lot of data is superfluous, but without being able to process and analyse the data effectively, it is impossible to identify what falls into this category and the most useful data is obscured from view. The third challenge is assessing, classifying and interpreting the data effectively, so that it can be utilised for decision-making.

This is where automated analysis comes in. Machine learning (ML) technology is the key to dealing with so much data and extracting the meaning and value that it offers. With automated data solutions, companies can use algorithms to assess, classify and interpret their data at scale, without the need for explicit programming. They can groom their unstructured data so that not only will it work in synchronicity with other kinds of data, but all unnecessary data can be identified and removed. Automated analysis also enriches the data with metadata, which makes it easy to retrieve – another benefit in terms of efficiency.

In all, processing unstructured data with technology-driven solutions can give pharmaceutical, clinical research, and other life science organisations a real competitive advantage. ML and artificial intelligence (AI) are being deployed to speed up drug development processes and ensure that drugs are delivering optimal benefits to patients. Because ML technology can process and interpret large data sets at speed, it can make predictions around bioactivity, toxicity and physicochemical properties beyond what human analysis is capable of. Furthermore, AI and ML can be used to identify traits and characteristics in imagery that the human eye cannot detect or process on the same scale – cutting down on waiting times and aiding diagnostic accuracy. All this to say, that ML and AI in life sciences can empower leaders to make better strategic decisions with the previously untapped information now available within their teams – improving the very future of medicine and healthcare for everyone.

Machine learning is also being utilised to improve supply chains. With longitudinal data, ML can identify production bottlenecks, reduce the length of batch disposition cycles and monitor in-line manufacturing processes to ensure safety and quality. The encouraging reality is that cloud computing is now more accessible and scalable than ever before. As more and more businesses move to the cloud, tailored data solutions are available to life sciences organisations from start-up to multi-national. Using a cloud-native services platform like Iron Mountain Insight, businesses can easily capture, classify, index, enrich and visualise their data, whether physical or digital. This tool, which uses machine learning technology and Google's AI capabilities, enables teams to present their data in a usable format and pull out the information that is relevant to their needs.

If analysed properly, data can deliver all sorts of invaluable insights about patients, therapies, operational processes, and more. Those in the life sciences industry should be taking advantage of the technology at their disposal today, because there are so many opportunities to be realised from the insights their data can provide. Ultimately, the chances that the next big medical breakthrough is discovered due to analysing data are higher than they've ever been.

Data minimalism: How to practice this and the benefits of it

According to IDC, the amount of data that companies, governments, and individuals create in the next few years will be twice that of all the digital data generated thus far and since the start of the computing age – that's 35 Zettabytes in 2018, growing to 175 by 2025.

BY TIM SKINNER, UK CLOUD LEADER AT NETAPP

EXPERTS SAY that as much as 70% of that data will never be used again, making it an unnecessary drain on resources for businesses. Between rising energy costs and a tough market environment, data storage has therefore become an increasingly expensive endeavour. In this piece, I'll discuss why data minimalism is the answer, and how businesses can practice it in order to cut down on costs and streamline their data storage.

Data minimalism

For businesses to maximise their chances of success in the new digital economy, they must develop and embrace a digital presence, and cultivate digital assets. As they improve their business processes, and become more data-driven, they must find ways to create an environment that's conducive to the use of digital technology.

One way of doing this in a systematic and effective way is by creating and following a data strategy which has data minimalism at the heart of it. By ensuring you only store the data you need, business will be able to cut costs, while also being one step closer to meeting Environmental, Social Governance (ESG) targets.

How to implement data minimalism

So how can businesses refine and evolve their data strategy to ensure they are practicing data minimalism? Well, it starts with truly understanding the data footprint that they have. Asking questions such as:

- How much resides on-premise, in the cloud or in other locations?
- What data does an organisation need to collect and how is it being used?
- What data is mission-critical, and what can be retained on more of an archive basis?

Making informed decisions can only happen once leaders are across all these details. Once a business knows what their current data footprint looks like, they can then start to consider their options. Bringing on board a trusted advisor at this stage might be useful to help provide extra support here. For example, are there ways to become more efficient in where data is being saved? Can some storage locations can be consolidated to save costs? Could an organisation move more of their data into the public cloud, and work with one of the hyperscaler providers to improve the environmental impact storing and managing their data is having?

Benefits of data minimalism

The sheer amount of data organisations are producing, collecting, and accessing today means that informal and ad hoc approaches to collecting and managing data is no longer enough. And that's not even before you start to think of the environmental and sustainability impacts – something that is higher on the boardroom agenda in a world where stakeholders are much more focused on a business' Environment, Social and Governance credentials. Data strategies are tailor-made and specifically designed to improve data management across a whole organisation, giving departments the guidance they need to work in alignment with each other, rather than against each other.

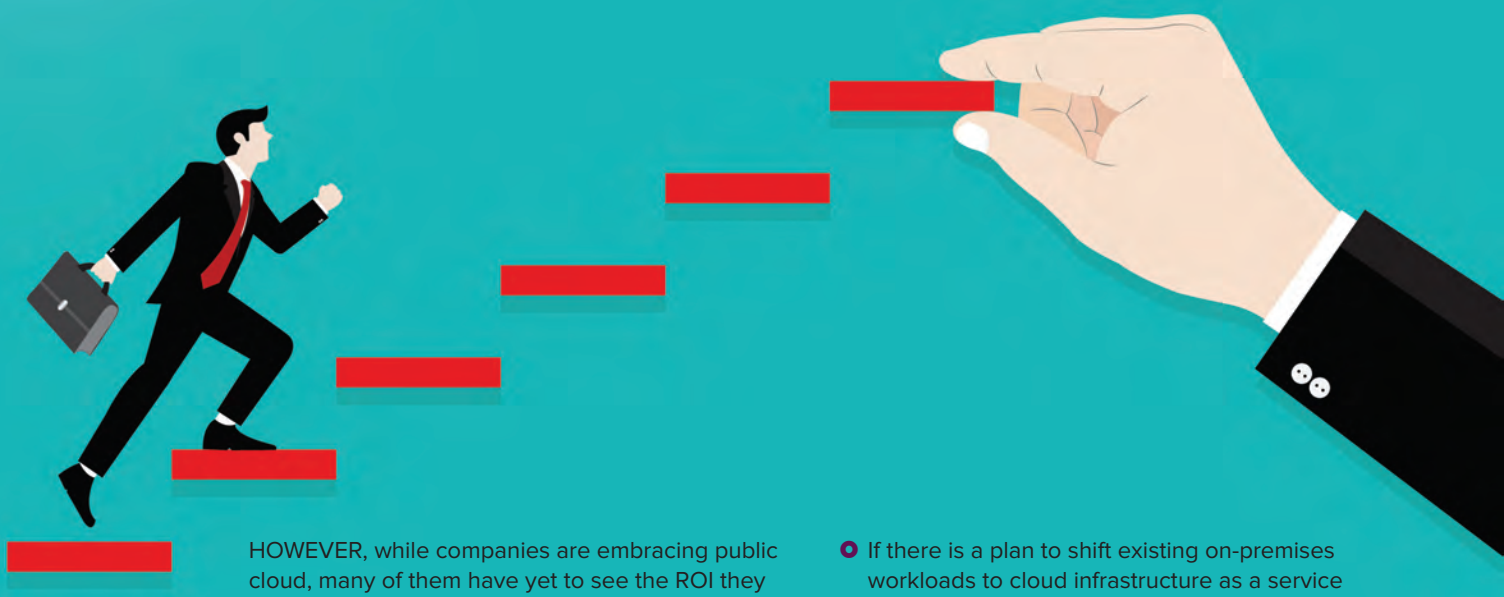
Data minimalism may sound counter-intuitive, especially at a time where the value of data is sky-rocketing. However, implementing data minimalism can reduce your workload for your business, while ensuring data is clean, of a higher quality, and well governed, in order to reduce security and privacy risks, as well as unnecessary power usage that lead to increased CO2 emissions. Some sectors have additional mandates to follow when it comes to data. Financial services organisations for example must collect and retain a great deal of historical data as part of reporting requirements. They must put in place the right mix of storage technologies together to support these needs, in a way that is as cost-effective and sustainable as possible.

As businesses face ongoing economic uncertainty and turbulence, now is an ideal time to examine their digital capabilities and find ways to make data work harder and smarter for them. Building and implementing a robust data strategy, with data minimalism at the heart of it, will help them put their best foot forward.

Three step to build a cloud business case that gets funded

With worldwide end-user spending in EMEA on public cloud services forecast to grow from $111 billion in 2022 to $131 billion in 2023, and cloud software spending set to represent 34% of total enterprise software spending in EMEA - cloud has never been more important in business strategy.

BY DAVID WRIGHT, SR DIRECTOR ANALYST AT GARTNER



HOWEVER, while companies are embracing public cloud, many of them have yet to see the ROI they expected because of flaws in their original business cases. Mounting a business case for cloud adoption that is fit for purpose is key to set the organisation up for success and secures the funding it deserves.

To do so, infrastructure and operations (I&O) leaders should follow three key steps.

1. Start with Proven Templates

First, start with a framework that accounts for the typical issues that cloud migration projects often face. It is not enough to simply estimate the cost of cloud infrastructure and operations. Realistic forecasts need to include the costs of workload migration, application modernisation, organisation transformation, and the "sunk cost" of left-over, on-premises IT capacity.

An effective cloud business case will use detailed internal assessments to establish a strong business justification, including a full scope of costs:

- If there is a plan to shift existing on-premises workloads to cloud infrastructure as a service (IaaS), assume that an ongoing investment in operational cost optimisation will be required to achieve lower total cost ownership (TCO). Build a business case that goes beyond fast cost savings to estimate the true business value of cloud adoption.
- The business plan must also account for the time and investment needed to master "cloud native" ways of purchasing, deploying, automating, securing, and optimising IT resources. Forecast the expected benefits of cloud adoption based on a realistic assessment of the organisation's pace of internal transformation.

2. Gain and Hold Executive Attention

I&O leaders are often inclined to model the benefits of cloud adoption in IT terms: higher scalability, tighter security, greater efficiency, etc. However, business decision makers rarely view IT performance improvements as sufficient justification

for making a strategic investment. They may believe they are being fooled by IT into throwing money at a problem that should properly be addressed through existing IT budgets.

To build a compelling business case for new investment, identify the key business objectives executives care about. Then assess the impact that cloud infrastructure will have on those objectives and compare the business value of this approach with other available options. Ensure new investment is being aimed toward the organisation's most urgent business issues.

After identifying the high priority objectives, collaborate with business leaders to review the critical business processes that support these objectives and help them assess the ways that public cloud infrastructure could be used to significantly improve them.

Demonstrate that the business cannot easily obtain those outcomes some other way. Providing a comparison of different approaches will build confidence among executives that the business case for cloud is scoped to the areas where it will have the most impact.

3. Mount a Campaign for Change

I&O leaders with a vision for the future must ensure that their cloud business cases are as adapted to continuous change as the cloud itself. They must embrace change in how their business cases are structured, as well as how the value of those cases is communicated.

They must work to free their business cases from waterfall thinking and, instead, propose a linked set of investment cycles needed to gradually adopt a new way of delivering IT infrastructure to the business. The investment case for a transformation to cloud computing is not often landed through a single, detailed presentation, but through a gradual

socialisation of ideas. It is crucial that I&O leaders equip themselves and their CIOs with the material needed to convey the cloud business case to others and sustain interest in it at executive levels.

In the real world of cloud adoption, there is no such thing as a beginning and an end. I&O leaders must view their cloud strategy as a continual work in progress and prepare a business case that anticipates common cost problems, aligns with business needs, offers a staged investment plan, and embraces continuous improvement.

Medical data is moving to telemedicine, but security hasn't kept up

The last few years have borne witness to a mobile revolution. It is now a centrally important piece of technology for seemingly every industry, upholding the next flexibility and speed which we now expect of a modern workforce.

BY ASH PATEL, GENERAL MANAGER FOR EMEA, ZIMPERIUM

UNFORTUNATELY, attackers will go where there are targets to attack. With that growth, mobile devices have also become one of the main attack vectors. As so often happens with rapid adoption of new technologies - security has not kept up.

The Growth of telemedicine

Telemedicine seems to be growing in all directions. Patients can now get check-ups from their doctor via their own mobile phones and doctors can share sensitive medical information with patients and other medical specialists quickly and easily.

In the meantime, consumer focused healthcare apps are enduringly popular. From calorie counters to sleep tracking apps, to water consumption apps - people seem highly interested in measuring and tracking their own health metrics.

This can be especially useful for those with long term health problems. For example, diabetes patients are now using apps to track their intake of sugars and carbohydrates, thus allowing them to better manage their condition. The amount and richness of that data is proving marvellously useful to legitimate users and medical practitioners.

However, it's this kind of data which is coveted by cybercriminals, and so often, easily within their grasp.

The healthcare sector is in a unique position when it comes to cyber-risk. It both possesses some of the most valuable data that a cybercriminal can steal, and is often not well positioned to fend off those attacks. Its full-throated adoption of mobile devices, may ultimately provide another attack vector through which threats can exploit the sector.

The value of medical data

Medical information is some of the most sensitive data that one can give out, and one of the most lucrative that a cybercriminal can get their hands on. According to one 2019 report from Trustwave, healthcare data can be sold at up to $250 per record, set against the comparably small $5.40 for payment card records which is the next highest value data category.

That could be one of the reasons why the previous years have seen a precipitous rise in attacks on this sector. According to Sophos' 2022 report - The State of Ransomware in Healthcare - 66% of

healthcare organisations were attacked in 2021, up from 34% in 2020.

Healthcare organisations are also more also likely to pay those ransoms - 61% - compared to the cross sector average of 46%.

Vulnerabilities in medical environments

On the other hand, medical environments are often not designed for security, but ease of access. Hospital IT systems will often be filled with a diverse collection of endpoints and designed so that doctors, nurses and other medical practitioners can easily find what they want, when they need it. These are also typically large networks, in which multiple parties might need access to the same data quickly. Security controls are often perceived as an obstacle to quick access, thus, they can sometimes be side lined in the perceived service of enabling quick access to data.

A powerful example of exactly this was revealed when the WannaCry attacks hit in 2017. The ransomware attacks - which eventually spread all over the world - paralysed 42 of the UK's National Health Services (NHS) trusts. Many of those trusts were running outdated versions of the Windows Operating System, which could no longer be updated to avoid attacks like WannaCry.

Mobile devices and the threats they pose

One of the principal values that has ushered mobile devices into the medical sector is the ease with which both healthcare professionals and patients can access data. This is undoubtedly a valuable asset to possess, it also represents an enduring problem within medical IT - easy access for users often means easy access for criminals too.

BYoD

One of the main challenges arrives when medical practitioners use their personal devices in a Bring Your Own Device (BYoD) scheme. In fact, a recent Zimperium survey found that nearly half - 44% - of all healthcare professionals do indeed access patient data with a mix of organisational and personal devices.

This represents a stark problem for the security of that patient data. When using personal devices, medical practitioners are exposing patient data to the variety of threats - through software vulnerabilities, malicious applications and more - that may exist on their device.

Compliance

Given the sensitivity of medical data, there are a range of regulations which govern it and punish noncompliance.

The European General Data Protection Regulation (GDPR), for example, lays out strict rules for the handling of personal data and threatens harsh fines for those that don't follow them. In the US, a variety of state-level regulations - such as the California Consumer Privacy Act (CCPA) - perform a similar function. Other regulations compel organisations to engage in forms of telemedicine. For example, the Health Insurance Portability and Accountability Act (HIPAA) and the 21st Century Cures Act demands that healthcare organisations adopt Application Programming Interfaces (APIs) in order to allow patients to access their health information through apps.

How to secure mobile devices in medical environments

Telemedicine grants both patients and medical practitioners incredible capabilities and benefits. However, in order to capture those benefits - security needs to be a central concern of healthcare organisations. Even if a security breach or regulatory fine never happens to an organisation, patients will turn away from Telemedicine if they don't believe it to be secure. In one 2021 survey from Arlington Research, 52% of organisations said that Telemedicine patient numbers declined directly because of security concerns.

Securing those devices requires intervention at several stages of the device supply chain.

The manufacturers of devices - both medical and personal - need to think about the security of the broader ecosystem and how their devices share data. Their communications should be continuously monitored and transport security should be established to prevent Man In the Middle attacks from altering or corrupting data in transit.

At the application level, medical apps need to be secured against potential device vulnerabilities. If, for example, it detects that a phone has been rooted - that app can prevent itself from starting up - thus protecting the medical data that the app would otherwise handle.

Developers of medical mobile applications also need to think about the security of their code too. Cybercriminals will often download apps from app stores in order to reverse-engineer and thus exploit them and organisations need to guard against this possibility.

Healthcare providers will need to do thorough risk assessments of the products and devices they use, so as to ensure both compliance and privacy. Furthermore, they can look to Mobile Device Management (MDM) to secure the personal devices that medical practitioners will be using and the data that they'll exchange. By permitting the central management of a healthcare organisation's mobile devices - MDM can automatically enforce policies around data handling, ensure that the correct practices are being carried out and encrypt sensitive data. Furthermore, it allows for the remote installation of the necessary settings, policies and security applications and while blacklisting apps and devices it deems unsecure.

Uncovering the true risk of connected devices in 2022

Connected devices and risk is a widely acknowledged by-product of the rapidly evolving digital era in which we now operate.

BY DANIEL DOS SANTOS, HEAD OF SECURITY RESEARCH, FORESCOUT VEDERE LABS

THE RATE at which IT, Internet of Things (IoT), Internet of Medical Things (IoMT) and Operational Technology (OT) devices are susceptible to being compromised, varies. Some are considerably more at risk than others, especially as cybercriminals continue to innovate at a rapid pace to gain access to, and exploit, connected devices to achieve their goals.

The growing number and diversity of connected devices in every industry presents new challenges for organisations to understand and manage the risks they are exposed to. The attack surface now encompasses IT, IoT and OT in almost every organisation, with the addition of IoMT in healthcare, which is fuelling increased vulnerabilities across interconnected networks.

In fact, according to a recent report by the Ponemon Institute, 65% of responding organisations say that IoT and OT devices are one of the least secured parts of their networks, while 50% say that attacks against these devices have increased. IT and IT security practitioners in 88% of those organisations have IoT devices connected to the internet, 56% have OT devices connected to the internet and 51% have the OT network connected to the IT network.

The reality is that connected devices now exist in every vertical and they continue to pose considerable and wide-reaching security risks to organisations across all sectors, as many are still susceptible to both known and older vulnerabilities. To identify points of risk inherent to device types, industry sectors and cybersecurity policies, recent research has analysed the risk posture of over 19 million devices across financial services, government, healthcare, manufacturing and retail to reveal the riskiest connected devices of 2022.

The findings have shown that:

IT devices are still a favourite target

IT devices including computers, servers, routers and wireless access points are among the riskiest, as they remain the main target of malware, including

ransomware, and the main initial access points for malicious actors. These actors exploit vulnerabilities on internet-exposed devices, such as servers running unpatched operating systems and business applications, or use social engineering and phishing techniques to dupe employees to run malicious code on their computers.

Routers and wireless access points, as well as other network infrastructure devices, are becoming more common entry points for malware and advanced persistent threats. Routers are risky because they are often exposed online, interfacing internal and external networks, have dangerous exposed open ports and have many vulnerabilities that are often quickly exploited by malicious actors.

Hypervisors, or specialised servers hosting virtual machines (VMs), have become a favourite target for ransomware gangs in 2022 because they allow attackers to encrypt several VMs at once - ransomware developers are moving toward languages such as Go and Rust that allow for easier cross-compilation and can target both Linux and Windows.

IoT devices are harder to patch and manage

A growing number of IoT devices on enterprise networks are being actively exploited because they are harder to patch and manage than IT devices. IoT devices are compromised due to weak credentials or unpatched vulnerabilities primarily to become part of distributed denial-of-service (DDoS) botnets.

A growing number of IoT devices on enterprise networks are being actively exploited because they are harder to patch and manage than IT devices. IoT devices are compromised due to weak credentials or unpatched vulnerabilities primarily to become part of distributed denial-of-service (DDoS) botnets

IP cameras, VoIP and video conferencing systems are the riskiest IoT devices because they are commonly exposed on the internet, and there is a long history of threat actor activity targeting them. For instance, in 2019 APT28 compromised VoIP phones for initial access to multiple networks, in 2021 Conti targeted cameras to move internally in affected organisations and, in 2022, both UNC3524 and TAG-38 have targeted video conferencing and cameras for use as command and control infrastructure.

ATMs appear in the ranking because of their obvious business criticality in financial organisations and also because data indicates that many ATMs are adjacent to other IoT devices such as security cameras and physical security systems that are often exposed.

Printers include not only multifunctional printing and copying devices used in the connected office but also specialised devices for printing receipts, labels, tickets, wristbands and other uses. Although printers are not widely associated with cyber risk, they should be.

Like IP cameras, they have been exploited in intrusions by threat actors such as APT28 and spammed by hacktivists on multiple occasions. And just like ATMs, printers are often connected to sensitive devices, such as point of sale systems in the case of receipt printers and conventional workstations with privileged users in the case of office printers.

X-ray machines and patient monitors are among the riskiest IoMT devices

Connected medical devices are obviously risky because of their potential impact on healthcare delivery and patient safety.

There have been many ransomware attacks on health system corporate IT networks that spilled over to medical devices, rendering them unusable, such as WannaCry in 2017, the attack on a hospital in Alabama affecting foetal monitors in 2019 and several attacks affecting radiation information systems in the United States and Ireland since 2020.

Ranked as the riskiest, DICOM workstations, nuclear medicine systems, imaging devices and PACS are all devices related to medical imaging and have a few things in common: They often run legacy vulnerable IT operating systems, have extensive network connectivity to allow for sharing imaging files and use the DICOM standard for sharing these files.

DICOM defines both the format for storing medical images and the communication protocol used to exchange them. The protocol supports message encryption, but its usage is configured by individual healthcare organisations. Through unencrypted communications across different organisations, attackers could obtain or tamper with medical images, including to spread malware.

Furthermore, patient monitors are among the most common medical devices in healthcare organisations and also among the most vulnerable.

Like medical imaging devices, they often communicate with unencrypted protocols, which means attackers can tamper with their readings.

OT devices are mission critical yet insecure by design

In the past decade, state-sponsored attacks against OT systems and devices have become commonplace. The research has found that manufacturing has the highest percentage of devices with high risk (11%), but what's even more troubling is the rise in cybercriminal and hacktivist activity targeting these devices. Recently, ransomware groups gained access to the SCADA systems of water utilities on several occasions and hacktivists gained access to the HMI of a water treatment facility in Florida.

Overall, PLCs and HMIs are the riskiest OT devices because they are very critical, allowing for full control of industrial processes, and are known to be insecure by design. Although PLCs are not often connected to the internet, many HMIs are connected to the internet to enable remote operation or management. These devices are not only common in critical infrastructure sectors, such as manufacturing, but also in sectors such as retail, where they drive logistics and warehouse automation.

However, other observed risky OT devices are much more widespread than PLCs and HMIs. For instance, uninterruptible power supplies (UPSs) are present in many corporate and data centre networks next to computers, servers and IoT devices. UPSs play a critical role in power monitoring and data centre power management. Attacks on these devices can have physical effects, such as switching off the power in a critical location or tampering with voltage to damage sensitive equipment.

Environment monitoring and building automation systems are critical for facilities management, which is a common need in most organisations. Smart buildings perfectly exemplify a cross-industry domain where IT, IoT and OT are converging on the same network. There are several examples of smart buildings exploited by threat actors to render controllers unusable, recruit vulnerable physical access control devices for botnets or leverage engineering workstations for initial access.

These devices dangerously mix the insecure-by-design nature of OT with the internet connectivity of IoT and are often found exposed online even in critical locations.

Proactively protecting devices on multiple levels

Both device manufacturers and users are responsible for developing and maintaining their cybersecurity defences, which is an outlook that's being reinforced by regulatory developments.

It's imperative that manufacturers utilise secure software development lifecycles. This includes processes, such as code reviews, vulnerability scanning and penetration testing. Most importantly, these processes must not be limited to the software the manufacturers produce, but to all the components that go into a device, including third party libraries.

As for the regulatory developments, the proposed EU regulation for cybersecurity requirements, if implemented, will make it compulsory for vendors to obtain cybersecurity certification for IoT devices. From a user perspective, there's also a big push towards making the disclosure of cybersecurity incidents mandatory, which would undoubtedly force companies to increase their security posture.

Unfortunately, there isn't a single quick fix to protecting connected devices. But there are practical measures all organisations can adopt, which starts with creating a complete, automated and continuous inventory of all network assets. Once all devices and their configurations are known, a risk assessment can be conducted to highlight the devices that need special attention either because they are insecure or because they are business critical.

Mitigation actions can then be implemented. Measures include patching known vulnerabilities, hardening devices by disabling unused services, using strong and unique passwords, segmenting networks to isolate risky devices and using comprehensive network monitoring to detect attempts to exploit devices.

Protecting connected devices from attack is a shared responsibility. We all have a part to play in uncovering the risks and safeguarding our infrastructures from increasingly sophisticated tactics. And exposing any potential chinks in our armour is where it all begins.

MANAGED SERVICES SUMMIT EUROPE

13 JUNE 2023

NOVOTEL AMSTERDAM CITY
AMSTERDAM NETHERLANDS

The Managed Services Summit Europe is the leading managed services event for the European IT channel. The event features conference session presentations by specialists in the sector and leading independent industry speakers from the region, as well as a range of sessions exploring technical and operational issues. The panel discussions and keynotes are supported by extensive networking time for delegates to meet with potential business partners. This C-suite event will examine the latest trends and developments in managed services and how they have influenced customer requirements and the ability to create value through managed services for your organisation and customers.

THEMES, TOPICS AND TRENDS

The Managed Services Summit will address the key trends and issues that impact the managed services sector including:

- How to build differentiation within an increasingly competitive market
- Maximise value and increase efficiencies for MSPs and their customers
- Increasing knowledge of new technologies, processes, and best practice
- Analysing trends in buyer behaviour and successful sales strategies
- Changes and trends in regulatory compliance
- Successfully adoption of Zero trust architecture (ZTA)
- Emerging advances in AI, automation and XaaS
- The state of cloud adoption, and hybrid and edge computing
- Hybrid and remote working best practice
- Addressing the growing cyber security skills gap
- Participation with local business community leadership organisations

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

Sukhi Bhadal
sukhi.bhadal@angelbc.com
+44 (0)2476 718970

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

Leanne Collins
leanne.collins@angelbc.com
+44 (0)2476 718970

https://europe.managedservicessummit.com/

What does the EU's Cyber Resilience Act mean for businesses?

Given today's socio-political landscape, questions of cybersecurity continue to gain traction.

BY MANOJ BHATT, HEAD OF SECURITY AND ADVISORY AT TELSTRA EMEA,

RANSOMWARE, phishing, and DDoS attacks have all claimed a large share of the conversations around business security, and while these are crucial considerations, some others have often been overlooked in comparison or considered too hard to tackle. IoT, or smart devices, is one of the most notable examples of this.

Smart devices have quickly become ubiquitous, and for consumers and businesses alike they are a non-negotiable part of everyday life.

With the number of smart devices in use expected to hit 13.1 billion by the end of 2022, it's clear that smart devices are here to stay. But they introduce a number of new targets for cyber attackers to hit. Businesses and consumers alike are increasingly aware of this, with research by Which? finding that smart devices are targeted by cyber criminals at least 12,000 times per week. As such, the news that the EU Commission is proposing a new Cyber Resilience Act has come at the right time to help manage this growing threat. But what will the implementation of this mean for businesses?

What is the Cyber Resilience Act?

In September, the European Commission proposed a new law, the Cyber Resilience Act, which is designed to prevent attacks upon IoT devices by implementing new rules for manufacturers. Of note, it aims to put pressure on manufacturers to heighten their security from the design stage, and provide proof of this. The EU's digital chief, Margrethe Vestager, explains that the Act 'will put the responsibility where it belongs, with those that place the products on the market'.

The proposed Act will require manufacturers to monitor cybersecurity risks, and the vulnerabilities associated with their products, and respond to these to ensure security is maintained either for five years, or to match the predicted lifetime of the product. If they fail to do this, they will receive a considerable fine: either €15 million or up to 2.5% of their global annual turnover. It seems that the EU is taking a similar approach to GDPR.

This is a really encouraging step forward in alleviating the pressure on security departments who use third party products which they cannot secure within their own ecosystem. It's well-known that businesses are facing a wider range of cyber threats than ever before and while an increasing number of nation-state and corporate ransomware attacks typically make the headlines, for most businesses it's issues of unsecured IoT devices in their working environments that cause problems and risks on a daily basis.

The IoT risk today

Given how commonplace smart devices are, it's easy to forget that they are a relatively new technology. These days it's not uncommon for houses to be almost fully kitted out with smart devices - from the doorbell, to the light switches, to the fridge. Understandably, people are excited by a new technology that revolutionises their day-to-day lives, but this means they often forget that with any new technology there's a risk of as-yet unknown vulnerabilities. We should also recognise that these devices can be used to mount attacks utilising IoT botnets where attackers can install botnets on IoT devices without the user's awareness.

A number of security researchers have discovered vulnerabilities and have asked manufacturers to resolve these. However, manufacturers seem to be reluctant to address these. The proposed Cyber Resilience Act could ensure that manufacturers cover vulnerabilities in all of their devices, meaning that the threat of compromise will reduce significantly, and is handled from the outset.

Along with this, there are unique challenges associated with the implementation and use of enterprise IoT devices but we shouldn't forget the connectivity of Operational Technology (OT). Enterprises are connecting OT equipment which traditionally might not have been connected to the internet, and in doing so they are making them IoT devices. These devices tend not to have considered security from the outset and the new Cyber Resilience Act will definitely put more of an onus on manufacturers to consider this for new OT devices.

This broadens the range of risks considerably, as we are faced with the internet connectivity of highly complex devices and operations. The use of internet-connected equipment that uses a standard username and password, with no multifactor authentication, and which has never been patched, can lead to severe business disruption as it is so easily compromised.

Bolstering security culture should remain top of mind

The Cyber Resilience Act is a positive step forward for more than one reason. In the first instance, it emphasises the role of the manufacturer in maintaining security standards rather than leaving this to the consumer or enterprise alone.

More than this though, it has ignited conversations around security culture. Discussion of the benefits of increased IoT security also naturally brings up questions of what organisations could improve on too. With so many IoT compromises associated with devices that may not be company-issued, or maybe older OT technology that is becoming IoT, it's clear that educating employees is key regardless of the standard manufacturers are held to.

Regardless of how strong regulations are, businesses will always benefit from fostering a security-aware culture. The Act mandates the availability of security credentials in product descriptions, which is an invaluable resource in helping drive broad security awareness, but organisations shouldn't stop there.

Finally, we hope that this new Act will have some teeth to ensure that the manufacturers will come to the table to have proactive conversations with enterprises to address these risks that we have been facing for some time. One would also hope that manufacturers understand how security controls within their products are an important part of product development, and that security must be baked in from the outset and not considered as an afterthought.

Why DRM is fast becoming a critical component in secure file transfer solutions

In today's highly connected business world, sharing data is faster and simpler than ever. But with this ease of sharing also comes concerns, particularly regarding the security of file transfers.

BY CHRIS BAILEY, PRODUCT LEADER AT FORTRA, THE NEW NAME FOR HELPSYSTEMS

MANY ESTABLISHED file transfer systems rely on encryption to keep data secure. However, with the rise of remote working, sensitive files are now being shared electronically by employees daily, often via unsecured channels which offer far less control and protection . In addition, enterprises face strict compliance regulations such as HIPAA, PCI-DSS, FISMA and GDPR, which require them to protect sensitive data in transit.

With the amount of sensitive, business critical data that now crosses the wire on a regular basis, ensuring it falls into the right hands is more than an IT or security issue, it's a matter of business survival. With this in mind, what secure transfer techniques are most popular amongst businesses today? PGP, or Pretty Good Privacy, has been around since 1991 and is still often used today for signing, encrypting and decrypting communications, providing privacy and authentication. Secure Managed File Transfer (MFT) solutions provide robust encryption as well as threat detection to help organisations transfer files securely.

However, once this data is received, what happens to it is completely outside the organisation's control. For example, take media organisations like the BBC and HBO. Their most popular shows are often distributed around the world to international broadcasters and streaming services. Once those digital copies are sent out, if the data isn't properly protected then it's all too easy for pirates to copy it and share it illegally, or even leak spoilers for yet un-broadcast content, often with major ramifications. While solutions like Secure MFT do mitigate the problems of getting files safely and securely from point A to point B, businesses today need their files to be safe, regardless of where they go, for the lifetime of the data.

The importance of Zero Trust

So, how can businesses tackle the root of the problem? To understand this better, we must first understand Zero Trust. Zero Trust is a security framework whereby nothing is left to chance – everything must be proven, every time, and there are two main ways to do this. Businesses can either secure the transfer method, or they can secure the data itself. At the moment, most do the former but neglect the latter.

While there is no more traditional 'perimeter', most secure transfer solutions still verify users at a "gate," and once they've been authenticated, they are given carte blanche to do whatever they like with the data contained within. Of course, there are numerous issues with this approach. For a start, credential-based authentication methods are far from bulletproof. Usernames and passwords can be easily lost, stolen, or even guessed, which makes relying solely on them for data protection very risky. Remember that when it comes to data, businesses

typically need solutions that ensure three things – availability, confidentiality, and integrity. While this gatekeeping technique makes the data both confidential (at least while in transit) and available, it does very little to protect its overall integrity. Even if the file transfer successfully delivers sensitive data to the intended person, if that person then acts maliciously or carelessly with it, there are absolutely no other measures in place to keep it protected at that point.

DRM As an Essential Component of Zero Trust

To truly achieve Zero Trust across files, data, and critical information, businesses need to defend it at the source. This means placing access controls on both the method of delivery and the information itself.

For this, there is Digital Rights Management (DRM), which, when paired with secure file transfers, offers more complete data security. Rather than making the data impossible for unwanted parties to catch, it makes it impossible for them to use. DRM lets businesses control every file, email, and piece of intellectual property that crosses the wire, with rights applied or revoked at any time. They can set permissions on who's allowed to open it, limiting access to specified email or IP addresses only, and retain full control over who can print, copy, save, edit, or even screenshot files.

Protecting such files with specific permissions prior to sending ensures the information cannot be accessed by anyone other than the intended recipients, even if it goes astray at any point before, during, or after the transfer process. In short, DRM ensures that:

1. Businesses and their employees can send and receive sensitive files and data to authorised recipients only, without exposing any of it to unauthorised third-parties at any point

2. Businesses can retain full control of the files after they are sent, received, and accessed and can even prevent editing, printing and screenshots from being taken on a mobile phone.

3. Administrators can retain full DRM rights management even after data has left the organisation, revoking access so that the file can no longer be viewed.

With businesses and their employees sharing more digital information now than ever before, keeping sensitive data protected at all times is an increasingly difficult challenge. While many still rely on secure transfer services to get it from A to B, without further protections of the data itself, its integrity remains at risk. By combining DRM with secure MFTs and integrating it effectively into their data security process, businesses know that regardless of where their data goes, they are still in control of it, giving them the peace of mind they need to operate effectively in today's competitive business landscape.

Why high-performance computing and AI will revolutionise healthcare

The social value of high-performance computing (HPC) is becoming increasingly obvious. It offers the computing power needed to help humanity solve some of its greatest challenges.

BY NOAM ROSEN, EMEA DIRECTOR, HPC & AI AT LENOVO ISG

USING HPC in healthcare is relatively new: traditionally, it has been dominated by physicists, chemists, and astrophysicists. Applying this technology to healthcare, however, benefits not just individuals but society as a whole. Artificial intelligence (AI) also has an important part to play in the public health domain, the administration of healthcare, as well as the clinical setting, particularly when it comes to the automation of diagnosis processes. Combined with HPC, these technologies will transform the future of healthcare.

HPC is a perfect fit for healthcare because of the large data sets generated by public health systems, much of which is in the form of images (from scans, for example). These data sets constitute a vast body of knowledge which has been largely unexplored until now. Most of their value comes from interpretations by experts, which has been done manually and is a hugely limiting factor when it comes to getting value from this data.
This is where HPC can make a huge difference, enabling both researchers and clinicians to ask bigger and more complex questions, and get the answers much faster. It leads directly to better research results and more precise treatment decisions.

Why bioinformatics matters

HPC is particularly useful in bioinformatics, which is a multidisciplinary field that integrates the principles of mathematics, statistics, computer science and biological science. The role of bioinformatics in medical research is to extract knowledge from biomedical data. HPC systems are now evolving to meet bioinformaticians' needs, with new hardware and software products allowing more sophisticated uses of data.

In life sciences, the time it takes to answer crucial questions is incredibly important. For instance, when it comes to seeing how a cancer patient will respond to a specific treatment, time matters a great deal. Speed is also imperative when spotting the signs of a new infection in society and stopping it before it spreads widely. The urgent need to create quick

answers requires more powerful and sophisticated computing resources.

Understanding our genes

HPC enables us to not only be quick, but to also be accurate, allowing us to focus more on individual data. The life sciences industry is shifting from the development of blockbusters, which addresses the needs of the masses, to developing more niche, personalised solutions for patients. That's the promise of genomics, the study of the genome. Genomics is providing us with far more detailed understanding of what causes illness and infectious diseases and it's underpinning the development of innovations that would have been unthinkable even a decade ago.

Rapidly decreasing DNA sequencing costs, combined with increasing computing power, means that we are able to understand the human genetic code like never before. We are well placed to harness genomics to respond quickly to evolving threats, such as COVID-19, as well as potential future pandemics. Genomics has the potential to revolutionise healthcare in many ways. It's a game changer.

Through genomics, scientists can identify a drug target, often a protein that is either misbehaving or has behaviour that needs to be modulated. Once that protein is understood, it is important to think about how to make a small molecule that might actually interact with it. In order to do that, we need to understand and see the structure of the protein. When we start to think about precision medicine, which takes into account genes and lifestyle for the individual patient, all of the data collected from edge devices - wearables, medical devices, IoT devices - need to show up and be computed at the same time. This must happen at a very high speed, which is where HPC comes in.

HPC solutions deliver scientific data at a significant speed, which allows integrators of HPC to break into the genomics space faster, without having to hire vertical technical expertise. By leveraging the technology, the time needed for scientific insights by turning genomics analytics can be reduced to minutes, which was a process that previously took days. Excessive time taken to analyse data impacts profits, growth, and delays time to scientific insights.

The role of AI

Artificial intelligence will also be important in everything from drug discovery to public health to the clinical setting.

Drug manufacturers frequently apply machine learning techniques to extract chemical information from large compound data sets and use this to design new drugs for clinical trials. AI models can be trained to better select the study participants with advanced statistical methods and to assess the results of the studies.

Through genomics, scientists can identify a drug target, often a protein that is either misbehaving or has behaviour that needs to be modulated. Once that protein is understood, it is important to think about how to make a small molecule that might actually interact with it

In the clinical setting, the potential of AI is enormous, ranging from the automation of diagnosis processes to therapeutic decision making and clinical research. Among the most promising applications of AI is for the automated processing of cardiac imaging data, which is necessary for the assessment of cardiac structure and function. Generation of more accurate and automated echocardiograms with the use of AI is expected to reveal unrecognised imaging features that will facilitate the diagnosis of cardiovascular disease. It will also minimise the limitations associated with human interpretation of these scans.

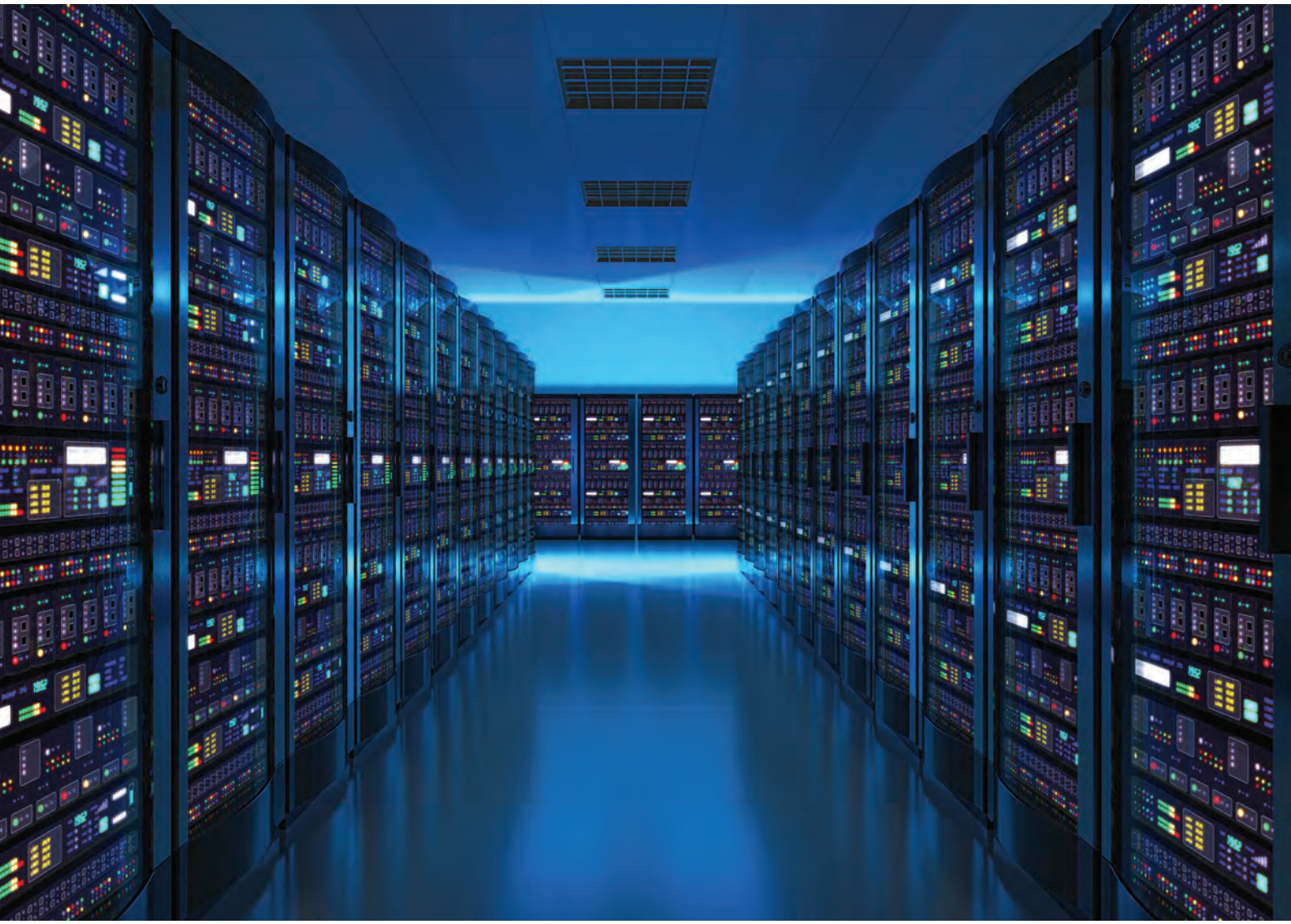
AI can assist in the public health domain as well, in preventing disease, prolonging life and promoting health. It can help identify specific demographics or locations where the prevalence of disease or high-risk behaviours exist, allowing doctors to intensify contact with patients as well as to target services to specific individuals.

The last application of AI is in the administration of healthcare. Healthcare systems are characterised by heavy administrative workflow. AI can perform different types of routines related to that administrative effort in a more efficient, accurate and unbiased fashion. A lack of bed availability in hospitals is an important cause of surgical cancellations and applying AI to optimise the availability of beds can help to decrease these.

HPC and AI in healthcare - the future

Looking ahead to the future, society must make it easier for healthcare organisations to use these important tools. Rather than research institutions taking the components and starting from scratch, we need to integrate these tools in a way that makes it easier for organisations in the healthcare space to make the most of them.

HPC can offer answers to many of the greatest problems we face, and combined with AI, can herald a new era of personalised medicine. It is therefore crucial that medical experts have the access they need to these game-changing technologies.



Going green: how data centre sustainability is changing the IT industry

As the world increases its dependence on energy-hungry technologies, the IT industry faces a major challenge: how to more efficiently power the devices and networks that drive our daily lives while also playing a full role in getting to net zero.

BY TERRY STORRAR, MANAGING DIRECTOR, LEASEWEB UK

DATA CENTRES, for instance, are a major source of greenhouse gases, with estimates suggesting that they account for nearly 1% of all energy-related emissions. This means that finding sustainable ways of operating in the IT industry is increasingly urgent, and many experts agree that this will require a radical rethink of the infrastructure used to support current and future technologies.

Despite the challenges, there are a range of proven approaches that can help organisations improve the environmental performance of their tech infrastructure. High on the list is moving hardware, software and services to the cloud, not least because it can play a major role in improving the energy efficiency of the underlying systems.

For instance, on-premises servers and data centres typically consume power even when applications and platforms aren't running and sitting idle, primarily because infrastructure is often configured to handle peak traffic requirements. Clearly, this is inefficient from an energy consumption and financial perspective.

Cloud-based services can be built to share the compute and storage requirements of multiple servers within a single platform. This means less hardware is required overall, and as a result, fewer emissions are produced to build infrastructure technologies in the first place, while there is also less to recycle at the other end of its lifecycle

In fact, on-premises servers are by far the least sustainable way of running infrastructure as they are incredibly energy inefficient. Put simply, instead of one big data centre with shared cooling and power systems running thousands of servers, on-premises servers require a separate cooling and power supply for each individual server. This is not only less energy-efficient, but it also takes up more physical space and produces higher emissions.

Sharing is caring

In contrast, cloud-based services can be built to share the compute and storage requirements of multiple servers within a single platform. This means less hardware is required overall, and as a result, fewer emissions are produced to build infrastructure technologies in the first place, while there is also less to recycle at the other end of its lifecycle. Similarly, a general reliance on fewer servers means data centre operators and their customers can spend less on the power needed to cool and run their equipment. The impact can be significant, with one study finding that the energy footprint of moving applications to the cloud could be reduced by nearly 90%.

Indeed, data centre energy efficiency has become a major focal point for the entire industry and its customers the world over. For example, the Power Usage Effectiveness (PUE) of each data centre has become an important benchmark of environmental performance and impact – the lower the PUE, the better.

Whether it's cooling systems, networking infrastructure or storage, there are a range of other factors that contribute to PUE (or the lack of it) in each data centre. Increasingly, data centre providers are investing in greener infrastructure as it gives them a competitive edge over less efficient rivals. Ultimately, access to this performance data gives data centre users a useful way to compare providers, especially when sustainability is becoming an important part of the decision-making process when choosing one provider over another.

As well as offering the potential for reducing energy consumption, a cloud-centric IT strategy that optimises the use of hardware also means that data centres need less physical space than might otherwise be the case. This also helps ensure that cooling systems can be run with greater efficiency, helping to further improve overall environmental performance.

While the cloud is a great solution for organisations everywhere and moving to the cloud is generally greener than traditional servers, it's not right for everyone. For example, in situations where applications or functions are used continuously, a hybrid infrastructure strategy might be better than a complete cloud migration. When most or all of the capacity of a single server is being used 24/7, it isn't automatically going to be cheaper or better for the environment by moving to the cloud.

In an era where the global push for net zero is a huge driver of everything from government policy to business strategy, cloud has a major role to play in getting there. From improving the environmental performance of the IT industry in general and data centres in particular, putting these considerations at the forefront of infrastructure planning and investment should be high on the agenda of every responsible business.