DIGITALISATION WORLD

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

ISSUE IX 2022

DIGITALISATIONWORLD.COM

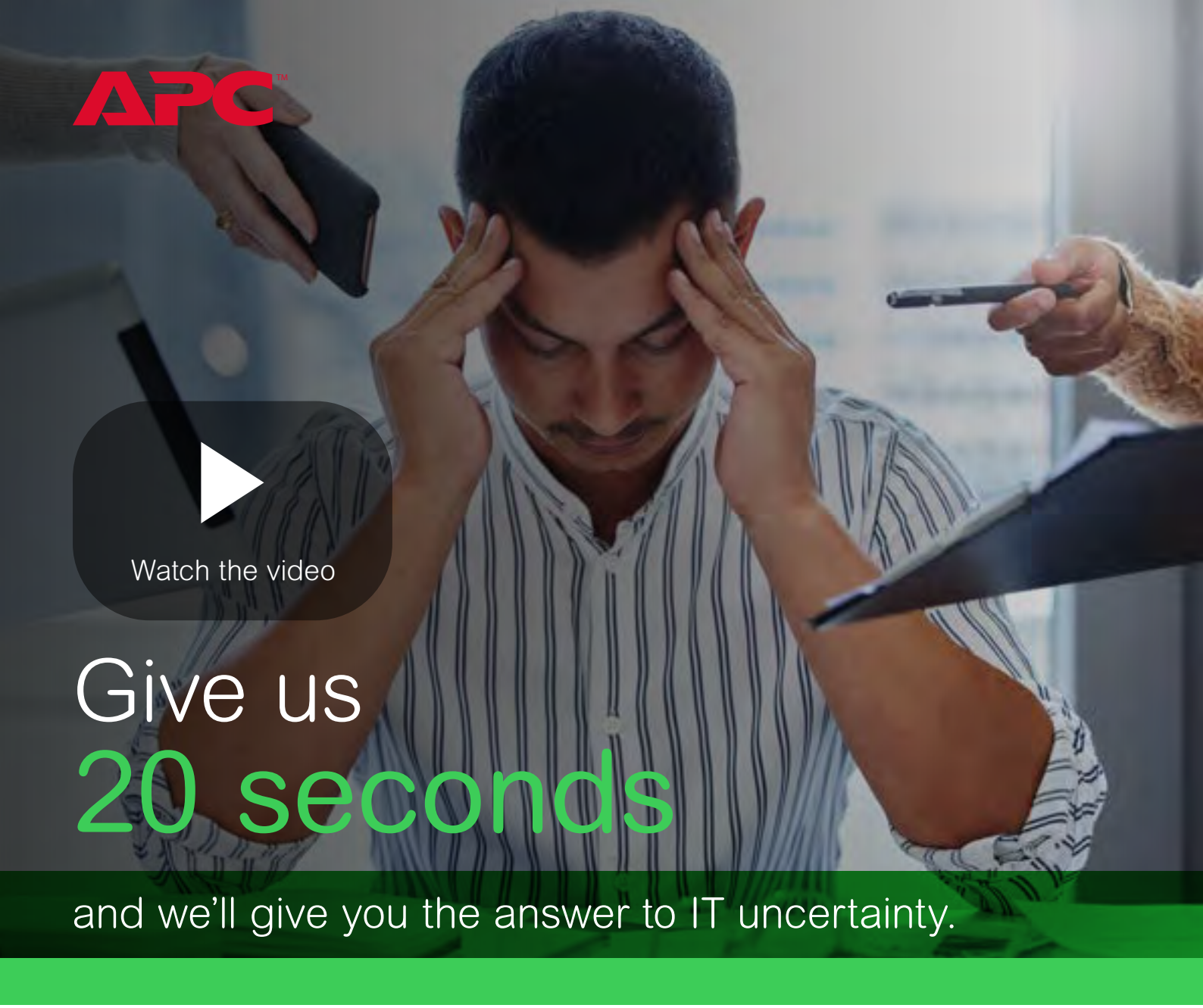
What's best for enterprise storage customers when times are tough?

DW talks to Infinidat's Richard Bradbury

INFINIDAT

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



IT is a serious matter but, let's face it, there are some strange things that people in IT face every day.

That's what **IT Happens** is all about.

It's a quick look at how nothing in IT is certain. **But it can be.**

See how Schneider Electric, through the power of APC offerings and **EcoStruxure™ IT software**, can provide the resilience, reliability, and sustainability you need. That's no joke.

www.apc.com

Life Is On Schneider Electric

Editor's View

By Phil Alsop, Editor

Uncertainty the only certainty

Despite the increase in the use of IT and automation within the workplace, human beings have never been so crucial to business success as they are now and will be into the future. Gartner's annual strategic predictions always make for interesting and enjoyable reading as they provide some valuable insights into where the world of work is heading. Some of the predictions are of the fairly obvious kind – the continuation of the re-imagining of the workplace and further consolidation of the cloud market, for example – but plenty are not.

Right now, the world is rushing towards Artificial Intelligence (AI) and Machine Learning (ML) in all their many flavours. Gartner points out that, unless this shift is done in a sustainable manner, we will shortly reach a stage where AI will consume more energy than the human workforce. Not such a great outcome for those tasked with hitting various Net Zero targets. However, we should perhaps not be surprised to see this warning, as digital consumption and sustainability are, essentially, incompatible.

Don't worry, I'm not a digital luddite or gloomster, just someone who is honest enough to see and admit that, however well we manage our natural resources, many of them are, ultimately of the finite, non-renewable kind and, therefore, will run out at some stage in the future. Until we learn to grow and harvest metals and minerals(!), the long-term future is obvious for all to see. Most striking in the Gartner predictions are the number which focus on the workforce. I've already mentioned the rapidly evolving, hybrid workplace – responding to the needs of employees, but there is also the related issue of labour volatility, encompassing 'The Great Resignation' and, for now at least, a tight labour market, where well-qualified, reliable employees are hard to find and retain. Gartner talks of 'labour resilience', and more and more organisations are realising that the people part of their organisation is no longer just the responsibility of the HR department, but requires input from all departments.

Gartner also mentions the importance of both equitable pay and the recognition that investment in the workforce can (unsurprisingly to me at least!) lead to better business outcomes and profitability. The whole CX/DX movement continues to gain momentum as, in simple terms, there is a growing recognition that people are rather more important than the machines that many would have replace them.

The volatility of the world in which we are living has served for many individuals as something of a wake-up call to decide what does and doesn't matter in life. It would seem that a similar crossroads faces many businesses, as they wrestle with the importance of continuing to make profits, but at what cost to their employees, customers and the planet?

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

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

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

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

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

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

Directors
Scott Adams: CTO
Sukhi Bhadal: CEO

Angel BUSINESS COMMUNICATIONS

Digitalisation World is published 8 times a year on a controlled circulation basis in Europe, Middle East and Africa only. Subscription rates on request. All information herein is believed to be correct at time of going to press. The publisher does not accept responsibility for any errors and omissions. The views expressed in this publication are not necessarily those of the publisher. Every effort has been made to obtain copyright permission for the material contained in this publication. Angel Business Communications Ltd will be happy to acknowledge any copyright oversights in a subsequent issue of the publication.

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

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

DW DIGITALISATION WORLD

WHAT'S BEST FOR ENTERPRISE STORAGE CUSTOMERS WHEN TIMES ARE TOUGH?

Storage is one of the areas where an IT department can deliver very substantial cost savings, without sacrificing availability, reliability, performance, or cyber resilience

THE ANALYST

CX / DX

LOW CODE / NO CODE

DCA News

NEWS

MONITORING

APPLICATIONS

STORAGE

Research identifies seven qualities of organisations delivering good digital employee experience

Employees from organisations with high-quality DEX report over 75% less downtime and are 30% less likely to leave their employers.

LAKESIDE SOFTWARE has published a new research report *Digital Experience Guide: 7 Qualities of Digital Employee Experience Leadership*, revealing the seven attributes of organisations that are delivering high-quality digital employee experience.

DEX describes the quality of a workforce's daily interactions with the technology they use for work. The goal of DEX is to drive positive change by analysing how employees interact with the organisation's computing devices, local and cloud applications, networks, and virtual desktop infrastructures (VDIs).

The new guide is the first industry report to analyze organizations at every stage of the DEX maturity curve and outline the benefits DEX leaders enjoy over less engaged organizations. Lakeside is able to pinpoint the attributes of successful DEX leadership, where organisations fall on the DEX maturity curve, the business outcomes of improving DEX, and what it takes to bring DEX to the next level.

The research shows that only 20% of organizations can be classified as DEX leaders with technology and financial services firms leading the way. Healthcare and insurance accounted for the most intermediate organizations while later adopters can be found in the manufacturing and professional services sectors. Larger concerns, with more than $10 billion revenue, represent the largest percentage of DEX leaders. Despite significant proven benefits in employee usability, customer satisfaction, and annual revenue, 58% of companies are still in the intermediate stages of adoption, and 22% are only just getting started.

As more jobs become available as remote positions, it's important to note that as remote and hybrid positions increase, so do the expectation for modern work experiences. Greg Dolphin, director of global support at LexisNexis, said, "Lakeside's proactive IT capabilities have significantly enhanced our digital employee experience. The quantity and quality of data collected has let us strategically identify and remediate issues far faster than we otherwise would have. A year after onboarding SysTrack, about 5% of the logged incidents across the local IT support teams were filed proactively. Today, we are solving 50% of issues proactively, purely because of the level of visibility that we have into endpoints."

7 Qualities of Digital Employee Experience Leadership

Proactive IT stance across the entire organization was the top trait of firms that were further along the DEX maturity curve. They shift from solving issues only after they occur to preventing problems in the first place.

Think of it like a car heading the wrong way, like a GPS system, this technology tells the driver to turn around and go in the right direction. This is why proactive IT via endpoint management is important - the endpoint in tech affects a user's ability to continue a task, causing technical difficulties and disruptions.

In a car, you would end up at the wrong house. End-point management software constantly scans to predict and repair issues before they become apparent to a user, creating real-time fixes.

Fully integrated tech suites support IT teams to monitor the full picture. Leaders have a single source of truth that provides a holistic view of the environment to all sub-teams, while DEX laggards will still be relying on disparate tools and workflows. Complete data collection enables DEX leaders to gather objective system details, device performance, and user behaviour data directly from endpoints, as well as user sentiment and other qualitative metrics. Those who are responsive to change and share data internally, reap the benefits of easier fixes, fewer problems, and enable the ability to gather a broad range of metrics which can provide data history for further analysis.

Personalized IT unlocks opportunities for optimal performance, enabling leaders to track daily engagement preferences, user ability, and offer the end-user a bespoke experience. DEX leaders have already shifted towards personalization with the help of sentiment data, pulse surveys and questionnaires with emphasis on hard supporting data about user performance, software adoption, and other classifying metrics.

Self-reliant employees are more prevalent at DEX leaders, and benefit form an environment where support is "always available." Users have access to self-help remediations, with organizations limiting the cost and time lost to technical difficulties to just thirty minutes a week, four times less than those without.

Automated fixes for common issues remediate, update, and patch across the IT estate. DEX leaders also make use of data insights to understand when certain thresholds are met rather than having IT personnel perform these tasks one by one.

Predictive analysis anticipates future failures whereby DEX leaders leverage artificial intelligence and machine learning to scan for patterns and trends that may cause disruptions and provide evidence of potential IT problems while recommending solutions.

Digital transformation delays cost organisations over £3 million per project

Research from Toca finds that spiralling cost overruns, legacy systems and a demand for speed are causing organisations significant challenges when delivering digital transformation.

AS DIGITAL transformation remains top of the agenda for many businesses, research conducted for low-code application development platform, Toca, reveals the extent of the challenges faced by IT teams in delivering these projects. Looking at the top barriers to successful transformation, IT decision makers cited budget constraints, a lack of collaboration across the wider business, legacy systems, a shortage of developers and integration challenges as the top five. Consequently, 88% of IT decision makers are facing costly project delays – with the average digitalisation delay lasting five months at a cost of £20,200 a day, totalling £3,070,400.

The survey of 200 IT decision makers reveals:

- 68% of organisations' digital transformation projects are now expected to be delivered three times faster than five years ago.
- However, 72% of IT leaders say the waiting lists for digital projects are getting longer.
- As a result, 71% of IT leaders are struggling with the pressure of innovation.
- Employee satisfaction, customer service and productivity are the top three areas being negatively affected by failure to match the speed of expected delivery for new applications or systems.
- 72% of IT leaders believe the days of large-scale projects are over, favouring smaller projects that deliver incremental business benefits faster.

"Organisations are focusing attention on digital transformation projects to drive new business opportunities and to meet the growing expectation for seamless customer journeys, which have been heightened by newer, digital-first competitors entering the market," comments Mat Rule, Founder and CEO of Toca. "This has placed IT teams under significant pressure, with issues like shorter timelines, tight budgets and legacy processes impacting the success of the projects. And with spiralling cost overruns and delays lasting months at a time, businesses are facing a growing issue as they try to deliver value with new applications and systems."

Despite organisations making progress with digital transformation, almost all (94%) IT leaders confirm that "building apps, connecting systems and automating processes faster is business imperative." To combat this, 89% of IT decision makers state they would prefer to leverage legacy systems to speed up digital projects, rather than rewrite and platform them.

Yet the pressure to deliver is forcing organisations into sacrificing best practice for quick delivery. In fact, 80% of IT leaders agree that the need for speed with digital projects is increasing technical debt at their organisation. This can impact other projects by creating a knock-on effect, with 76% of IT decision makers in agreement that technical debt holds them back from taking on new projects.

This is hampering organisations' ability to deploy digital technologies, with respondents reporting that on average they are only able to address one in four problems with digital transformation. Over three quarters (79%) of IT decision makers confirm that processes aren't automated because of time, cost, or complexity, despite the data revealing that automating manual tasks could save the average employee over five hours a week.

"Digital transformation projects are proving challenging for businesses, as they tackle delays and cost overruns," continues Mat Rule. "In order to drive quick digital wins and to solve more business problems, organisations need to empower their development teams to be more productive and to overcome the restraints of legacy technologies.

To achieve this, businesses are increasingly looking at solutions like low-code development, which can enable IT teams to deliver flexible digital services in a matter of days, drastically reducing the cost and time of traditional development. Using low-code, businesses can build digital wrappers around their legacy systems and then integrate apps and portals to drive digital journeys."

Board members 'unprepared' for cyberattacks

Proofpoint and Cybersecurity at MIT Sloan (CAMS), an interdisciplinary research consortium, have released their Cybersecurity: The 2022 Board Perspective report, which explores board of directors' perceptions about their key challenges and risks.

CYBERSECURITY is dominant on their agendas. Seventy-seven percent of participants agree cybersecurity is a top priority for their board and 76% discuss the topic at least monthly. Consequently, 75% believe their boards clearly understand the systemic risks their organisations face and 76% assert they've made adequate investments in cybersecurity.

But this optimism may be misplaced. Our report found that nearly two-thirds (65%) of board members believe their organisation is at risk of material cyber attack in the next 12 months. Almost half (47%) feel their organisation is unprepared to cope with a targeted attack. And only two-thirds of board members view human error as their biggest cyber vulnerability, despite the World Economic Forum finding that this risk leads to 95% of all cybersecurity incidents.

The Cybersecurity: The 2022 Board Perspective report examines global, third-party survey responses from 600 board members at organisations with 5,000 or more employees from different industries. In August 2022, 50 board directors were interviewed in each market across 12 countries: the U.S., Canada, the UK, France, Germany, Italy, Spain, Australia, Singapore, Japan, Brazil, and Mexico.

The report explores three key areas: the cyber threats and risks boards face, their level of preparedness to combat those threats, and their alignment with CISOs based on the CISO sentiments Proofpoint uncovered in its 2022 Voice of the CISO report. We found a disconnect between the two sides in cyber risks, consequences, and threats. "It is encouraging to see that cybersecurity is finally a focus of conversations across boardrooms. However, our report shows that boards still have a long way to go in

understanding the threat landscape and preparing their organisations for material cyberattacks," said Lucia Milică, vice president and global resident CISO at Proofpoint. "One of the ways boards can boost preparedness is by getting on the same page with their CISOs. The board-CISO relationship is instrumental in protecting people and data, and each side must strive toward more effective communication and collaborative effort to ensure organisational success."

Proofpoint and CAMS' Cybersecurity: The 2022 Board Perspective report highlights global trends, along with industry and regional differences among organisational leaders. Key global findings include:

- There is a disconnect between the boardroom and CISOs when evaluating the risk posed by today's sophisticated cybercriminals: 65% of board members believe that their organisation is at risk of material cyberattack in the next 12 months, compared to 48% of CISOs.
- Board members and CISOs have similar concerns about the threats they face: board members ranked email fraud/business email compromise (BEC) as their top concern (41%), followed by cloud account compromise (37%), and ransomware (32%). While email fraud/BEC and cloud account compromise are also among top concerns for CISOs, they view insiders as their top threat, whereas board members rate insiders as a lower concern.
- Awareness and funding do not translate into preparedness: although 75% of those surveyed feel their board understands their organisation's systemic risk, 76% hink they have invested adequately in cybersecurity, 75% believe their data is adequately protected, and 76% discuss cybersecurity at least monthly, these efforts appear insufficient – 47% still view their ganisation as unprepared to cope with a cyberattack in the next 12 months.
- Board members disagree with CISOs about the most important consequences of a cyber incident: internal data becoming public is at the top of the list of concerns for boards (37%), followed closely by reputational damage (34%) and revenue loss (33%). These concerns are in sharp contrast with those of CISOs, who are more worried about significant downtime, disruption of operations, and impact on business valuations.
- High employee awareness doesn't protect against human error: although 76% of those surveyed believe their employees understand their role in protecting the organisation against threats, 67% of board members believe human error is their biggest cyber vulnerability.
- The relationship between boards and CISOs has room for improvement: there is a sharp variance in perspective between board members and CISOs: while 69% of board members report seeing eye-to-eye with their CISO, only 51% of CISOs feel the same.
- Boards are warming up to regulatory oversight: 80% of respondents to the survey agree that organisations should be required to report a material cyber attack to regulators within a reasonable timeframe and only 6% disagree.

Quality Engineering has a role in sustainable IT

New report also highlights 85% of organizations consider Quality Engineering to be pivotal in the implementation of emerging technologies into real-world use cases.

THE 14th EDITION of the World Quality Report, published recently by Capgemini, Sogeti, and Micro Focus, examines the key trends and developments in Quality Engineering and Testing (QE&T) and highlights sustainable IT and Value Stream Management as new interest areas for quality teams. According to the report, there is also significant optimism around the future impact of emerging technology such as blockchain, the metaverse, and other Web 3.0 applications.

Sustainability was one of the new areas explored by this year's edition of the report. Research revealed that while the role of quality within sustainable IT is still evolving, 72% of organizations think that QE&T could contribute to the environmental aspect of sustainable IT.

Respondents are also optimistic about the benefits of green engineering as part of their sustainable IT strategies, with 47% of respondents citing improved brand value ranking as the most important benefit, followed closely by improved customer loyalty (46%). The report also finds that organizations are increasingly looking at Quality Engineering and Testing (QE&T) to support the deployment and success of new technologies such as blockchain and Web 3.0 and to address associated business challenges in the fields of customer experience, time to market, security, and cost. To ensure seamless experiences for end-users, new technology needs to be tested in a different way than before, with a different approach and types of testing and quality validation.

Also, 96% of respondents believe they would face medium or high risks of cyber-attacks without a quality strategy in place for emerging technologies. As the pace of technological change is exponential, importance of adapting cybersecurity strategies to counter the risk of cyber-attacks also emerged in the research.

Quality assurance function is accelerating its transformation to quality engineering practices

While awareness is growing on how quality strategy can offset various risks associated with deploying new technology, the quality assurance function is transforming at speed from pure testing to actual quality engineering practices. For example, 88% of respondents agreed they were at medium to high risk of losing market share to a competitor and 90% agreed that they face risk of increased costs for the deployment of new technology solutions without a QE&T strategy.

Focus on data continues to grow

There is unanimous agreement (89%) that robust data validation capabilities can improve decision making, efficiency, and improve bottom line profits. Test Data Management (TDM) is an integral part of the software testing lifecycle, however, only 20% of respondents have a fully implemented enterprise-wide test data provisioning strategy. Many organizations have serious challenges with the implementation of an effective data validation strategy; 42% see implementing data validation as a time-consuming exercise, while 47% of respondents said that having multiple complex databases itself acts as a challenge.

More integration across business teams needed to realize the potential of Agile

There is a growing recognition of Agile development and digital transformation as key enablers of further IT investment: To accompany the fast DevOps transformation, there is a recognition that integrating QE&T at every stage of product development is critical to leveraging the full potential of this function.

The research found that organizations are reporting significant improvements by adopting Agile development: 64% of respondents cited on-time delivery as the biggest improvement. Reduced cost of quality was another key improvement (62%), followed closely by improved customer experience (61%).

However, organizations continue to struggle to implement Agile development across packaged applications and enterprise systems due to the complex practicalities involved in breaking down Enterprise Resource Planning (ERP) workflows and end-to-end business practices into a single backlog.

Mark Buenen, Global Leader, Quality Engineering and Testing at Capgemini Group, commented, "Recent years have seen unprecedented acceleration for digital platforms and an overall modernization of applications. At the same time, supply chain challenges, cyber security threats, and the ongoing skills shortage mean the landscape for enterprises has never been more complex. In turn, investment in robust quality assurance and engineering are the foundation of an organization's ability to remain flexible, responsive, and adaptable. By looking deeper, we can see that this vital function can have a tangible impact on broader business performance, including profitability and even sustainability".

"The World Quality Report provides great insight into the current state and the future of IT, with an in-depth look at how emerging technologies are changing the quality needs and practices of organizations," said Rohit de Souza, Senior Vice President, General Manager - ITOM Product Group & ADM Product Group, Leader of the CTO office and Product Security, Micro Focus.

Record business expansion sees London as the largest EMEA digital hub

Forecast to exceed pre-pandemic interconnection growth despite uncertain macro environment.

CURRENT SUPPLY CHAIN constraints and geopolitical and economic instabilities are not slowing the pace of digital infrastructure investment for the most connected companies, according to a new report.

The latest Global Interconnection Index (GXI) 2023, an annual market study published by Equinix, found that globally the most ecosystem-connected businesses – those directly interconnecting with partners to provide their own digital services – have expanded their digital operations more in the past five quarters than in the previous five years. On average, organisations around the world are connecting to three times as many business ecosystem partners and metros, consuming more than twice the amount of interconnection bandwidth.

As businesses reinvent themselves in the aftermath of the global pandemic, ecosystem density has become a catalyst for digital innovation, which continues to fuel the growth of interconnection bandwidth. According to GXI 2023, global interconnection bandwidth is forecast to reach 27,762+ terabits per second (Tbps) by 2025, representing a five-year compound annual growth rate (CAGR) of 40%.

This is equivalent to 110 zettabytes of data exchanged annually, or enough bandwidth to support over 50 million autonomous cars each exchanging over 2,000 terabytes (TB) of data per year. This forecasted global growth shows how organisations are rethinking their business to implement future-proof infrastructure on technology platforms. EMEA contributes 25% of the global interconnection bandwidth forecast, predicted to grow at a rate (CAGR) of 40% by 2025, reaching 6,972+ Tbps, equivalent to 28 zettabytes of data exchanged annually. EMEA is leading the way in digital infrastructure deployment at 20-30% larger than any other region globally.

Within EMEA, London is the fastest growing core interconnection hub, with more than two times the capacity of any other location in the region. Led by financial services and network provisions, the city's digital capacity is expected to increase by (CAGR) 43% by 2025 (Amsterdam 39%, Frankfurt 38%, and Paris 37%).

"In today's dynamic setting, every business is becoming a digital provider, which requires a new type of digital infrastructure built sustainably around leveraging ecosystems to deliver seamless digital experiences. Those with a digital-first strategy in place, investing in a robust, future-looking business model and interconnecting to rich ecosystems, are prepared to scale, adapt and thrive," said Steve Madden, Vice President of Digital Transformation & Segmentation at Equinix.

Additional Insights from GXI 2023
Digital growth continues: While the overall global growth rate is predicted to be (CAGR) 40% by 2025, every region and major metro worldwide is expected to increase its Interconnection bandwidth by at least (CAGR) 35% within the same period.

London leads EMEA: The UK capital is the biggest metro interconnection hub in EMEA for Cloud & IT Services, Wholesale & Retail, and Healthcare & Life Sciences. The city also leads the region in Banking & Insurance, Securities & Trading, Business & Professional Services, Energy & Utilities, Industrial Services, and Consumer Services.

The move to the edge is accelerating: Both enterprises and service providers are forecast to interconnect to edge infrastructure 20% faster than the core globally. The expansion of multicloud: 85% of global companies are expected to expand multicloud access across several regions by 2025.

Businesses are becoming digital providers: GXI 2023 predicts that 90% of Fortune 500 companies will become digital providers, both selling and consuming digital services, by 2025.
· The sustainable road to digitally thrive: All industries are harnessing digital to accelerate ESG objectives, with 65% of global IT decision-makers (78% in the UK) saying they will only work with IT partners who meet key carbon reduction targets.[2] GXI 2023 forecasts the Energy & Utility sector will lead the digital growth rate by 2025 as all organisations explore a sustainable approach to build and expand their digital presence.

Russell Poole, Managing Director, UK at Equinix, said, "The latest GXI reveals that despite supply chain constraints, and ongoing geopolitical and economic instabilities, organisations continue to prioritise a digital-first strategy. Digital leaders in the UK recognise the value in creating agile IT infrastructures interconnected to their entire digital ecosystems to ensure prime performance, accelerate their Environmental, Social and Governance objectives, and develop business opportunities on a global scale.

"London maintains its position as a leading strategic digital business hub for enterprises looking to compete across international markets. The city is a long-established financial centre of the world and also leads EMEA in other critical growth sectors, including Cloud & IT Services, Banking & Insurance, and Healthcare & Life Sciences. Despite ongoing market uncertainties, there are many reasons to be optimistic about digital transformation and technology investment in the UK."

‘Perfect storm’ in cybersecurity demands new generation of cyber leaders

A new report published by Savanti, argues that cybersecurity leadership is broken and failing to deliver cyber success for businesses.

THE REPORT ARGUES that the combination of home working (which now means there are far more entry points into company networks than before), ballooning threats from rogue states and criminal groups, and low understanding of what companies actually need to defend themselves has created a ‘perfect storm’ in cybersecurity.

The report lays bare the rapidly growing threat environment in which attacks from nation-state actors have increased and are now more likely to target private companies than government agencies. 90 per cent of organisations believe they have been targeted by a nation state threat actor, with 39 per cent citing Russia and 44 per cent China.

Globally, cybercrime is predicted to increase by 15 percent per year, reaching more than £12 trillion annually by 2025 – which would make it the world’s third-largest economy behind China and the US.

Savanti’s report outlines how low levels of understanding about cybersecurity amongst company leaders results in isolated, technically-focused approaches that fail to deliver holistic security and risk management.

The report finds that, most crucially, Chief Information Security Officers (CISOs) are hired, managed and evaluated as technical experts rather than business leaders – a skills gap that is leaving companies increasingly vulnerable to cyber threats.

The skills gap is also creating unsustainable job churn. The average tenure is of a CISO is 2.3 years – compared to 6.9 years for a CEO, 4.7 years for a CFO, 4.6 years for a CIO – and the average CEO will cycle through

three CISOs in their tenure, stunting the company’s ability to build a long-term strategy. Analysis of recruitment and cyber investments by Savanti estimates the cost of a bad CISO hire to be at least £7.6 million.

The report recommends a number of recommendations, including:

- CISOs should be hired, managed and measured as business leaders rather than technical experts;
- Recruitment should priotise communication skills for CISOs;
- Cyber risk should be owned by the board, embedded in organisational processes and led with sufficient budget and staffing to drive organisation-wide change;
- Cyber leaders need to achieve change through influence rather than control;
- Boards need independent trusted cyber advisors, including ex-CISOs, to help them effectively interrogate all aspects of cyber leadership and strategy;
- CISOs should be integrated into all forward-looking aspects of business growth.

Richard Brinson, CEO of Savanti, said: “Our report is a wake-up call for business leaders to stop treating cybersecurity as a compliance exercise – those days are gone.

“Businesses simply cannot ‘farm out’ cybersecurity to technical experts without fundamentally changing the way they operate.

“We need a new model of leadership for the cyber age that unites security and business goals and utilises cybersecurity to enable and grow businesses as well as protect them.” Recent attacks on NHS supplier software, the Russian attack on Ukrainian military through ViaSat and the historically devastating NotPetya attack that nearly folded the global giant Maersk are just some examples of the damage wrought by cyberattacks.

Employees 'dodge' cybersecurity responsibility

New research shows that when it comes to company's cyber security, the majority of employees (81%) believe it's the IT department's responsibility to ensure it.

TERRANOVA SECURITY by HelpSystems, a global leader in security awareness training, has published the results of a study that showcases the level of cyber security awareness among workers in the UK, France, U.S., Australia and Canada.

The study, conducted in partnership with research company Ipsos, surveyed 500 UK employees. It concluded there is confusion among employees over who is responsible for protecting company data. Despite the fact that human error causes 95% of cyber issues, 81% of UK employees believe it's the IT department's responsibility.

In addition, 1 in 4 employees do not think cyber security is necessary for them, and 18% believe they can't be targeted at all by cybercriminals. The findings come at a time when the danger from a data breach is at an all-time high – businesses suffered 50% more ransomware attacks in 2021 compared to 2020. As of 2022, the average cost of a data breach to a large organisation increased to $4.35 million.

The research also highlighted that UK businesses aren't doing enough to support their employees when it comes to providing education on common cyber threats and security best practices. Only 42% of employees say they work in a company where cyber security awareness training is mandatory.

Of the 44% who haven't participated in any cyber security training, nearly a third (31%) indicated that their company doesn't offer any relevant training.

These low training rates aren't due to a lack of interest from employees, as 76% believe cyber security training is interesting, and 56% have started or completed the training when it's offered to them.

"It's concerning to see such a high percentage of employees who believe a company's cyber security is not their responsibility – especially in larger organisations," said Theo Zafirakos, Chief Information Security Officer, Terranova Security.

"It's clear that many British businesses have room to grow security awareness training strategies, especially in the face of rising cybercrime. Our research also shows there's still quite some work to do on educating people about the important role they play in protecting data at work. These people are the first line of defence against any cyber-attack, and on a positive note, our research demonstrates a strong appetite for learning more about it. By taking responsibility to invest more in education and build a security-aware culture around data protection within the business, companies will set up a powerful barrier against any cyber threats."

75% of workers say leadership has prioritised structure over collaboration

TRANSFORMATION during the pandemic did not focus on how people collaborate, leading to a new contributing factor to the great resignation and quiet quitting.

New research has found that despite 75% of businesses reviewing their structure to adapt to new ways of working, less than half of workers believe their organisation will change its approach to collaboration. A further, 28% feel their organisation should change the way it collaborates but do not believe change will come.

This new research was conducted by the leading AI-powered collaboration platform, Howspace. The research asked 3000 employees across 15 industries and seven countries about their experiences and attitudes to workplace collaboration. While other studies have focused on employee engagement, this honed in on the state and impact of collaboration. More than three-quarters of workers said they enjoyed collaboration in the workplace and almost half of workers believed they needed to collaborate more to be good at their job. However, nearly a third of employees feel their organisation should change the way it collaborates, but don't believe it will.

Against the backdrop of plummeting employee engagement, recognising employee needs is critical. Organisations must take action to improve collaboration across the board. Ilkka Mäkitalo, CEO of Howspace, said: "Many of today's work and management practices are counterproductive and destructive for collaboration.

While it is natural that leaders were seeking more control during the pandemic, the fact remains that people come to work to work together. Leadership needs to shift mindset from structure and control to one of designed collaboration that embraces both synchronous and asynchronous work. This requires inherently different management practices and working systems from where we are today."

Making moves on the metaverse

Ciena global study explored business professionals' views on utilizing more immersive and connected digital applications in the workplace.

A NEW GLOBAL STUDY commissioned by Ciena has uncovered just how ready business professionals are to collaborate in the virtual world.

Ninety-six percent of the 15,000 business professionals surveyed across the globe recognize the value of virtual meetings, and more than three-quarters (78%) say they would participate in more immersive experiences like the metaverse versus current tools, such as video conferencing. Additionally, while appetites grow for the new digital world, unreliable network performance was cited (by 38% globally) as the top concern holding organizations back. While the data reveals a significant push toward more digital and immersive platforms on a global scale, there are regional differences.

On a global level, 87% of business professionals confirmed they would feel comfortable conducting HR meetings in a virtual space. At a country level, this was as high as 97% in India and 94% in the Philippines, and as low as 57% in Japan.

According to the respondents, the top two benefits of virtual meetings are: improved collaboration and convenience. And, when it comes to selecting their avatar for the virtual world, 35% of business professionals would choose an avatar that reflects their real-world self, 22% would choose an idealistic version and only 10% would pick a pop culture figure.

Globally, 71% of professionals can see the metaverse becoming part of existing work practices, and 40% think their business will move away from traditional/static collaboration environments to more immersive and virtual reality-based environments in the next two years.

Despite growing interest among working professionals, barriers to widespread business adoption of immersive technologies still exist. According to survey participants, network reliability is a higher concern than the belief that immersive applications/tools are not yet widely available.

"Clearly, the business world is ready to move to the metaverse and start using enhanced reality tools for collaboration and innovation," commented Steve Alexander, Senior Vice President and Chief Technology Officer of Ciena.

"Network reliability may be seen as a barrier to making this possible today, but service providers know the demand is there and are already investing and testing to make networks faster, smarter and bring them closer to the user."

Gartner unveils top predictions for IT organisations and users

GARTNER, INC. has revealed its top strategic predictions for 2023 and beyond. Gartner's top predictions explore how business and technology leaders can reimagine assumptions and seize the moment to turn uncertainty to certainty.

"UNCERTAINTY carries as much opportunity as it does risk," said Daryl Plummer, Distinguished VP Analyst and Gartner Fellow. "The key to unlocking those opportunities is to reimagine assumptions – especially those rooted in a pre-digital past – around how work is done, how relationships between customers and providers will evolve and how current trends will unfold.

"The comforts of consistency are a detriment to the growth of any company seeking to lead in a modern digital world filled with unknowns. This year's predictions provide a foundation for executive leaders to seize uncertainty, challenge thinking and change expectations while maintaining forward movement."

Gartner analysts presented the top 10 strategic predictions during the recent Gartner IT Symposium/Xpo™.

Through 2027, fully virtual workspaces will account for 30% of the investment growth by enterprises in metaverse technologies and will "reimagine" the office experience.

As employees continue to desire more flexible work scenarios, virtual workspaces in metaverses will emerge to support new immersive experiences. Fully virtual workspaces are computer-generated environments where groups of employees can come together using personal avatars or holograms.

"Existing meeting solution vendors will need to offer metaverse and virtual workspace technologies or risk being replaced," said Plummer. "Virtual workspaces deliver the same cost and time savings as videoconferencing, with the added benefits of better engagement, collaboration and connection." By 2025, without sustainable artificial intelligence (AI) practices, AI will consume more energy than the human workforce, significantly offsetting carbon zero gains.

As AI becomes increasingly pervasive and requires more complex machine learning (ML) models, it consumes more data, compute resources and power. If current AI practices remain unchanged, the energy needed for ML training and associated data storage and processing may account for up to 3.5% of global electricity consumption by 2030.

Yet as AI practitioners become more aware of their growing energy footprint, sustainable AI practices are emerging, such as the use of specialized hardware to reduce energy consumption, energy efficient coding, transfer learning, small data techniques, federated learning and more.

"AI offers huge potential benefits to optimize operational efficiency and sustainability, far outweighing its own footprint," said Plummer. "Provided it is applied more pervasively and

effectively than today, AI could reduce global carbon dioxide emissions by five to ten percent."

By 2026, citizen-led denial of service (cDOS) attacks, using virtual assistants to shut down operations, will become the fastest growing form of protest.

Protests against businesses and government organizations are increasingly digital. Citizen-led denial-of-service attacks (cDOS) are led by average people rather than hackers, performed through virtual assistants.

Gartner predicts that by 2025, 37% of customers will try using a virtual assistant to interact with customer service on their behalf; for example, by waiting on hold for them. These legitimate interactions using virtual assistants will pave the way for protests. By 2024, citizens will shut down a Fortune 500 company's contact center through denial-of-service attacks launched by virtual assistants.

Through 2025, powerhouse cloud ecosystems will consolidate the vendor landscape by 30% leaving customers with fewer choices and less control of their software destiny.

The largest cloud service providers (CSPs) are creating ecosystems whereby they and preferred independent software vendors (ISVs) offer a range of pre-integrated and composable services. CSP ecosystems offer the potential for significant productivity gains from simplified sourcing, integration and composability of software components. As CSP ecosystems mature, there will be diminishing need for third-party ISV tools because CSPs can quickly release new features and become fast followers of innovation due to the speed and agility of cloud development.

Through 2024, jointly owned sovereignty partnerships sanctioned by regulators will increase stakeholder trust in global cloud brands and facilitate continued IT globalization.

As societies become increasingly globally interconnected and dependent upon digital information, more regulations and legislation are emerging from a desire to control and protect citizens and ensure continued availability of critical services. Specifically, governments and commercial regulators are tightening policies regarding the use of non-regional cloud providers for critical or sensitive workloads.

"Due to recent geopolitical events and seeing the direct impact that de-platforming sanctions can have, demand for sovereign cloud solutions is evolving," said Plummer. "Governments and regulators that sanction specific jointly owned approaches of cloud providers with local partners can meet tightened sovereignty requirements while facilitating continued technical globalization."

Gartner predicts that by 2025, 37% of customers will try using a virtual assistant to interact with customer service on their behalf; for example, by waiting on hold for them. These legitimate interactions using virtual assistants will pave the way for protests

By 2025, "labor volatility" will cause 40% of organizations to report a material business loss, forcing a shift in talent strategy from acquisition to resilience.

Challenges such as the Great Resignation, burnout and quiet quitting continue to challenge business leaders to find, attract, hire and retain talent. Within corporate announcements and financial disclosures, organizations will increasingly highlight material strategic shifts due to the inability to support existing products or services or launch new opportunities because of workforce challenges.

"Labor volatility has a direct correlation to enterprise execution and delivery models that impacts financial performance," said Plummer. "The resiliency dialogue must become a CEO and boardroom conversation, rather than one siloed to HR." By 2025, shareholder acceptance of moonshot speculative investments will double, making them a viable alternative to traditional R&D spend to accelerate growth.

To find advantages amidst uncertainty and volatility, industry leaders are increasingly accepting high-risk technology investments with little-known returns and potential failure, known as "moonshots."

"Winning enterprises have learned the real risk they face is doing too little too late. Adopting antifragile approaches, such as moonshots, allows enterprises to maximize their advantage from disruption by adjusting their risk appetite and raising their tolerance for failure," said Plummer.

By 2027, social media platform models will shift from "customer as product" to "platform as customer" of decentralized identity, sold through data markets. The current paradigm of users having to prove their identity repeatedly across online services is not efficient, scalable or secure. Web3 enables new

decentralized identity standards which introduce several disruptive benefits, including giving users more control over which data they share, removing the need for repeated identity proofing across services and supporting common authentication services.

By 2025, organizations that remediate documented gender pay gaps will decrease women's attrition by 30%, reducing pressure on talent shortages. Gartner data consistently shows that compensation is a top driver for talent attraction and retention, yet only 34% of employees believe their pay is equitable. There is no generally accepted methodology for calculating pay equity, challenging organizations to identify and account for gender pay gaps. A nascent market is forming for software tools that offer pay equity assessments, with specialist vendors emerging that provide more ways to analyze and model data related to equitable pay.

Through 2025, employee value metrics like well-being, burnout, and brand satisfaction will override return on investment (ROI) evaluations in 30% of successful growth investment decisions.

Investments in efforts such as employee well-being and customer experience can yield direct financial returns through revenue growth and cost reduction.

However, their more significant impacts are often on brand value, reputation and employee and customer acquisition and retention. Such metrics are difficult to quantify in terms of short-term financial gains, but they influence longer-term financial outcomes that drive enterprise value.

"Use of traditional ROI models to make investment decisions can discount or completely exclude non-financial benefits. Organizations that use more expansive valuation approaches will shift their investment focus to long-term growth, disruption and innovation," said Plummer.

Worldwide digital transformation investments to reach $3.4 trillion in 2026

Forward-looking organizations have been pursuing digital transformation (DX) with the goal of creating new sources of value through digital products, services, and experiences. As an added benefit, the pandemic revealed that digital transformation efforts improve an organization's resilience against market disruptions. Given its importance to future success, global DX spending is forecast to reach $3.4 trillion in 2026 with a five-year compound annual growth rate (CAGR) of 16.3%, according to the INTERNATIONAL DATA CORPORATION (IDC) WORLDWIDE DIGITAL TRANSFORMATION SPENDING GUIDE.

"DESPITE STRONG HEADWINDS from global supply chain constraints, soaring inflation, political uncertainty, and an impending recession, investment in digital transformation is expected to remain robust," said Craig Simpson, senior research manager with IDC's Data & Analytics Group.

"The benefits of investing in DX technology, including automation, strong intelligence, operational transparency, and direct support around customer experience, all support targeted areas of business focus to weather the current environment of uncertainty and to make the most of any opportunities in the recovery."

The DX use case that will see the largest investments over the forecast period is Innovate, Scale, and Operate, a broad area covering large-scale operations, including making, building, and designing activities. Core business functions that make up this area include supply chain management, engineering, design and research, operations, and manufacturing plant floor operations. Innovate, Scale, and Operate will account for more than 20% of all DX investments throughout the forecast.

The next largest use cases are Back-Office Support and Infrastructure at more than 15% of all DX

spending and Customer Experience at more than 8%. The fastest growing among the more than 300 DX use cases identified by IDC include Digital Twins and Robotic Process Automation-Based Claims Processing with five-year CAGRs of 35.2% and 31.0% respectively.

Nearly 30% of worldwide DX spending throughout the forecast period will come from the Discrete and Process Manufacturing industries, where Robotic Manufacturing, Autonomic Operations, and Self-Healing Assets and Augmented Maintenance are among the leading use cases. The next largest industries for DX spending are Professional Services and Retail where Back-Office Support and Infrastructure is the leading DX use case. The Securities and Investment Services industry will experience the fastest growth in DX spending with a five-year CAGR of 20.6%, followed closely by Banking and Healthcare Providers with CAGRs of 19.4% and 19.3% respectively.

The United States will be the largest geographic market for DX spending throughout the forecast, accounting for nearly 35% of the worldwide total and surpassing the $1 trillion mark in 2025. Western Europe will be the second largest region with nearly a quarter of all DX spending. China will see the strongest growth in DX spending with a five-year CAGR of 18.6%, followed closely by Latin America with a CAGR of 18.2%.

"Consumers and enterprises within the Asia/Pacific (excluding Japan and China) (APeJC) region are growing in connected technology and they tend to show higher consumption of digital products and services," said Mario Allen Clement, associate research manager for the Asia/Pacific IT Spending Team. "Amidst the pandemic and recovery, organizations have accelerated their digital engagements, products, and services, which have been predominantly improved by deploying digital technology faster. More and more businesses have started to go digital as a source of resiliency and innovation, which is shown across the region as new offerings and solutions are widely available. The APeJC region is expected to grow in double digits across the forecast period where use cases from IoT and Robotics are showing a high potential within the Manufacturing sector. Customer experience, engagements, and personalized customer journey will be the highlight of pushing a stable growth in digital transformation." The IDC Worldwide Digital Transformation Spending Guide (V2 2022) examines the digital transformation opportunity from a use case — technology, industry, and geography — perspective. The Spending Guide quantifies enterprise spending for more than 300 DX use cases and 12 technology markets across 19 industries and 14 geographic regions. The Guide provides spending data for 51 DX strategic priorities and 99 programs as well as technology spending by deployment type (cloud, non-cloud/other).

IDC maintains worldwide IT and business services forecast

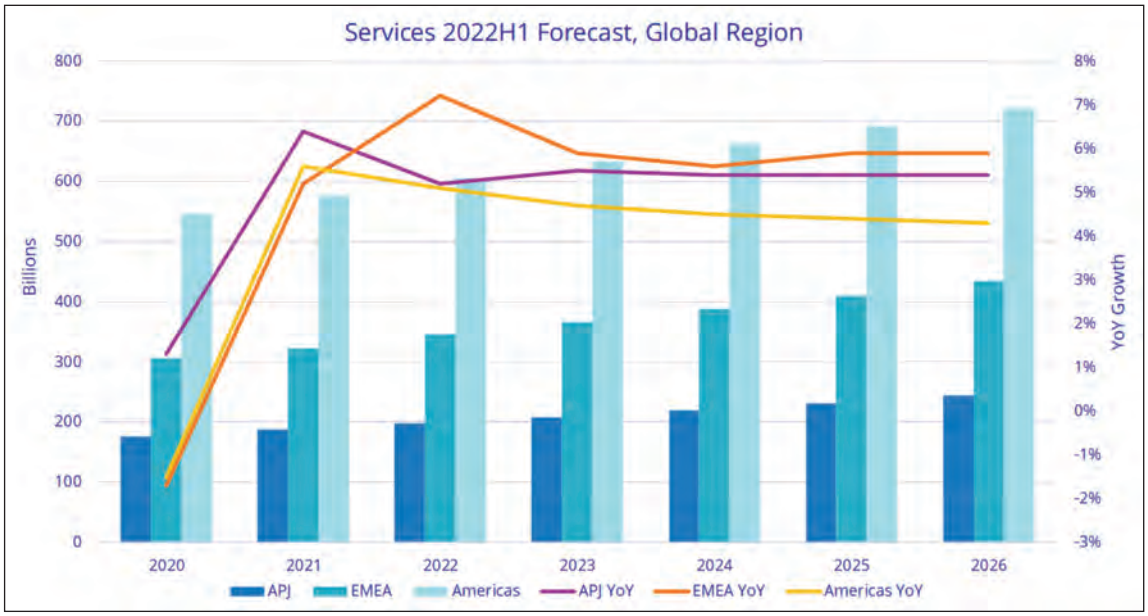
Worldwide IT and business services revenue is expected to grow (in constant currency) 5.7% this year and 5.2% in 2023, according to the INTERNATIONAL DATA CORPORATION (IDC) Worldwide Semiannual Services Tracker. In nominal dollar denominated revenue based on today's exchange rate, the market will grow by 2% this year, due to currency headwinds.

The 2022 market growth represents a slight increase of 12 basis points from IDC's April 2022 forecast. The five-year compound annual growth rate (CAGR) is now projected to be 5.2%, compared to the previous forecast of 4.9%.

IDC has maintained its outlook for the worldwide services market even against the backdrop of a global recession. Worldwide GDP growth has worsened since March/April and is now expected to grow by only 2.7% this year and 2.4% in 2023, based on August's figures. After adjusting certain geographic and market segments accordingly, IDC remains cautiously optimistic based on stronger than expected reported results from vendors in the first two quarters of this year (including revenues, bookings, and pipelines) and larger residual effects from the pandemic on the IT industry (i.e., hybrid workplace, cloud adoption, etc.).

For example, in the first half of 2022, the median year-over-year growth in constant currency for the top 20 IT and business services vendors was more than 9% (excluding product and other services revenues, such as engineering services). This was coupled with healthy bookings and pipelines. In addition, services firms have not yet lowered their revenue guidance significantly.

"While economic conditions for major economies around the world worsened in the last few months, given the services vendors' strong revenues, bookings, and other leading indicators, the worldwide services market will likely continue on



its current growth trajectory," said Xiao-Fei Zhang, program director, IDC Worldwide Services Tracker program. "Also, the real threat to vendors may be from the supply side: with book-to-bill ratios above 1.1 or 1.15, attrition 25% plus, and utilization rate pushing close to 90%, something has to give. A cooler economy may actually help vendors to convert bookings to revenue faster by easing the labor market."

IDC has adjusted its short-term growth rate for professional services slightly downward: during an economic downturn, discretionary spending will suffer more as some projects will be delayed or put off indefinitely. But this will be partially offset by the potential upside on the supply side. The negative impact will be felt mostly in business consulting: IDC lowered its business consulting market growth rates by 100 and 40 basis points in 2022 and 2023, respectively. Poised to grow between 6% and 8% in the coming years, business consulting will outperform the overall economy by a long stretch. The recessionary impact on recurring revenues is also expected be minimum to marginal. IDC has raised the growth rate for managed services by 40 to 60 basis points each year as managed services will be more shielded from economic downturns because these are mission critical to buyers. Pricing also helps as providers are increasingly able to pass on wage increases to customers in large outsourcing contracts.

Within managed services, apps remain the key growth driver, as the pandemic added billions of digital users across the globe almost overnight, exhausting the available software development talent pool worldwide. Therefore, IDC has increased its five-year CAGR (in constant currency) for application management from 4.5% to 5.2%. The workplace and infrastructure-related outsourcing

market outlooks have also been adjusted moderately upward as cloud and hybrid workplace continue to drive strong growth, albeit that these are relatively slow growth markets to begin with. Similarly, the growth rate for support services was adjusted upward only slightly in the short term as support services revenues depend on multi-year contracts and are much more insulated from sharp hardware shipment declines.

On a geographic basis, IDC has largely maintained its outlook for the Americas. Canada's long-term forecast remains intact, and the short-term growth rate was adjusted to reflect the speed of recovery among Canada's major vendors. Latin America's near-and-mid-term market outlook improved markedly this cycle: while still challenged by economic uncertainties and soaring inflation, major Latin American markets' economic conditions improved, thanks to rising commodity and energy prices. This is offset by a slightly weaker outlook for the U.S. market, where a recession will primarily impact business consulting – its five-year CAGR was adjusted down by almost 110 basepoints (from 6.2% to 5.1%). Overall, the US market is still expected to grow 4% to 5% year over year in the coming years.

The growth outlook for Asia/Pacific was adjusted downward by roughly 10 basis points each year for the next four years. The region is forecast to grow at around 5.5% each year. Within the region, the growth rates for both China and India have been lowered. As China's economy decelerated this year, the services market saw its 2022 growth rate adjusted downward by 130 basis points to just 5.2%, and the five-year CAGR declined by more than 90 basis points to 6.4%. India's services market growth was also lowered marginally under recessionary threats with the five-year CAGR reduced from 8.9% to 8.2%. The outlook is more favorable for the rest of the region, with faster than expected recoveries in mature markets like Australia and New Zealand, and more vibrant emerging economies in Southeast Asia. The 2022 forecast for Europe, the Middle East, and Africa (EMEA) was raised moderately. The outlook for the Middle East & Africa (MEA) remains unchanged with year-over-year growth between 6% and 8%. Recessionary threats have marginally lowered the outlook for non-petroleum producing countries, but this is offset by stronger forecasts for petroleum producing markets, as well as improved conditions in Turkey. For Europe, the outlook is mixed. IDC has lowered the short-term outlook for Central and Eastern Europe (CEE) with 2022 growth of just 3.6% as economic conditions have worsened in the region. However, Western Europe's growth rate has been raised by 100 to 200 basis points each year to more than 7% for this year (in constant currency) and 5.5% to 6% growth per year for the next four years despite economic and geopolitical headwinds.

While the dynamics within each market differ, the outlook for all major Western European markets have improved compared to March/April, including France, Germany, the Nordics, and the UK. Overall, IT services will be much more resilient, as large European enterprise buyers need them to close the digital gap. Additionally, governments will also fund digital initiatives through big recovery programs and boosted military spending.

"So far, the European services market has weathered the storms of disruption exceptionally well, resulting in a solid market performance in the first half of 2022," said Milan Kalal, senior research manager, IDC European Services Group. "The demand has been fueled by the acceleration of digitization efforts in European organizations as well as their ongoing appetite to transition to the cloud. But now it's time to go even further. Thanks to the wide deployment of technologies to change the business model, organizations are now entering the digital business era, where acting as a digital-first business is a mandate and a strategic differentiator to ensure future resilience."

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

Identifying a new framework for the fragmented workplace

To achieve better talent and business outcomes, organizations must adopt a new framework that centres around proactive rest, intentional interactions and patient growth, according to GARTNER, INC. The latest research was showcased during the recent Gartner ReimagineHR Conference.

GARTNER ANALYSIS reveals that several trends are causing workplaces – and employees – to disconnect from each other:

- Turnover will be 20% higher in the foreseeable future
- Up to 81% of employees who can work remotely or in a hybrid scenario will choose to do so
- Only 43% of employees trust their organization's leaders to act in their best interest
- Employees spend almost 10% of their time pening, closing and switching between different technology applications

"As a result of these factors, employees feel increasingly isolated and less connected to their coworkers," said Kimberly Shells, director of advisory in the Gartner HR practice. "A July 2022 Gartner survey of more than 3,400 employees found that those who are pulled apart from their organizations, their colleagues and their work are 57% less likely to be high performers and 68% less likely to stay at their organization."

Gartner has identified three areas that HR leaders need to focus on to build a more human organization:

Proactive Rest

The fragmentation in today's workplace is causing stress, exhaustion and burnout among employees. The average employee is working more than nine extra, unpaid, hours of overtime per week. Despite increasing employee burnout, a July 2022 Gartner survey of 243 HR leaders found that 77% believe that high performing employees work longer hours than average employees.

However, Gartner analysis found there is no consistent correlation, across employees, between performance and the number of hours worked. "Simply put: More hours worked does not equal more results," said Brent Cassell, vice president of advisory in the Gartner HR practice. "Instead, organizations must rethink how they approach rest – rest should be embedded into the workflow to prevent burnout rather than being used to recover from it."

Proactive rest encompasses three facets:

1. **Available:** There are a robust set of options for employees to use to rest and stay charged.
2. **Accessible:** Employees are encouraged to take advantage of the tools and resources available and to rest guilt-free.
3. **Appropriate:** Rest tools meet the individual needs of employees.

When rest is available, accessible and effective, employees perform at a level that is 26% higher. Additionally, Gartner's July 2022 employee survey found that at the average organization, 22% of employees are burnt out; at organizations with proactive rest strategies in place, just 2% of employees are burnt out.

Intentional Interactions

Human-to-human connections boost successful collaboration by 23%, but they are harder to come by now. Historically, employee connections were the by-product of working in the same location every day. The July 2022 Gartner employee survey found that only 31% of employees have human-to-human connections.

Yet, forcing connections among coworkers who work virtually or hybrid doesn't work – employees who spend more than half of their time collaborating with colleagues are only 4% more connected.

Facilitating successful connections among employees relies upon three factors:

- **Choice:** Human organizations offer employees the choice to participate in interactions with each other, but they don't mandate it.
- **Structure:** Everyone must understand the rules of participation via clear norms.
- **Levity:** The interactions must be fun for employees.

"When organizations help employees build connections intentionally, their employees are 12 times as likely to feel connected with colleagues," said Cassell. "Furthermore, their employees are five times more likely to be on a high performing team."

Patient Growth

More than half of the HR leaders Gartner surveyed in July think that their employees are less connected to their organizations now compared to before the pandemic. A separate March 2022 Gartner survey of more than 3,500 employees found that employees are half as likely, now, to be willing to change their behavior to support their organization through changes versus in 2016.

"What this means is that employees are both less loyal to their employer and also less willing to change for them," said Shells. "One critical strategy to improve loyalty and connection of employees to their organization is to invest in their development."

The best organizations have expanded the development and growth that they provide to employees beyond role-focused development and to the entire person. Providing opportunities for broader growth requires organizations to be willing to experiment and to allow time for employees to reflect and apply. When employers give their workforce time to grow as human beings, those employees are twice as likely to stay at the organization.

"When organizations strive to be more human, they can overcome the fragmentation that they have been experiencing and are four times more likely to exceed revenue and profit goals," added Shells.

What's best for enterprise storage customers when times are tough?

Storage is one of the areas where an IT department can deliver very substantial cost savings, without sacrificing availability, reliability, performance, or cyber resilience.

BY RICHARD BRADBURY – SVP EMEA & APJ AT INFINIDAT

WHEN INFINIDAT first began highlighting its low cost of ownership benefits compared to other enterprise storage platforms, executives at our award-winning company could not have conceived that this message would become so significant to users.

Cost efficiency is always essential, but fast forward to winter 2022 and its relevance is greater than ever. IT costs are soaring, and business leaders continue to scramble to find ways to lower costs. We are in the midst of a cost-of-living crisis, with economic uncertainty unseen since the 1970s set against a global backdrop of geopolitical uncertainty. Added to this, business energy costs are rocketing and earlier attempts by the government to control expenditure have floundered. There are ways to contain some of these costs,

by taking a more strategic approach to storage infrastructure. Making this change will make a huge difference to the bottom line.

For organisations that that require low-latency, high-throughput access to consolidated data of more than a petabyte, there are multiple ways that Infinidat helps companies to control their storage costs. The potential savings are so significant, we believe Infinidat's products should be the de facto enterprise storage platform of choice for any organisation wanting to minimise the current economic and energy crisis.

Hyper consolidation opportunity

An organization knows it's experiencing storage proliferation when the number of storage arrays has amassed 10, 12, 15, 20, 40 or more. Implemented gradually over time, array numbers increase in proportion to increased need for data storage capacity and additional workloads. With the explosion of data volumes in recent years, this is no surprise, but such a high number of storage units inevitably causes problems. Inefficiency, excessive costs, overly complex data centres, poor storage management, negative environmental impact, a larger cyberattack vector and waste, being the prime offenders

Storage consolidation is an ideal way to solve this issue and Infinidat goes a step further, leading the way in hyper consolidation. For example, without interrupting an organisation's operations we can convert 20+ storage arrays into a few InfiniBox solutions, providing easier management, cost savings, greater efficiency, cyber resilience, and sustainability aligned with green IT goals. Thanks to advancements in enterprise software-defined storage technology, there is no longer any need for 25 or 50 different older arrays, each running one application or workload, all applications and workloads can reside on just a few modern enterprise storage platforms.

Data centre simplification through the strategic consolidation of storage systems saves on power and cooling expenditure, minimises operational manpower, shrinks the need for rack space and floor space, and substantially reduces the CAPEX and OPEX of data centre storage. It's also possible to consolidate storage whilst simultaneously improving real-world application and workload performance across a hybrid cloud and a container-native environment. Beyond cost management, this offers the additional benefits of greater cyber resilience and higher availability.

Triple redundancy protection

To allay any concerns about becoming vulnerable to downtime after consolidating, it's important to mention the advantage of Infinidat's triple redundancy approach. Any business reliant upon on a dual-redundancy storage architecture is using an outdated architecture, one that does not deliver the level of reliability needed in our digitised world. Best practice in storage has moved on - to a triple-redundancy architecture - because it offers high reliability, availability, and durability.

Infinidat does this by offering three layers of controller redundancy, coupled with a self-healing architecture based on Infinidat's patented InfiniRAID data layout and predictive failure analytics. In addition, Infinidat goes a step further and provides a 100% availability guarantee for its InfiniBox solutions. The reassurance that comes with this means a hyper consolidation strategy can become a reality for every organisation, regardless of industry sector.

Minimise human resource overheads

Talent shortages continue to trouble the IT sector and finding qualified technical resources to manage storage environments is no exception. By deploying Artificial Intelligence for IT Operations (AIOps) within data storage, enterprises can simultaneously overcome talent shortages, centralize their operations and improve cost management. AIOps is essentially a dynamic way to simplify IT operations, reduce administrative overheads and add a predictive layer onto the data infrastructure. Through AIOps, the resources required to manage data centre operations can be permanently reduced and any engineers that are still required can be trained and fully efficient very quickly.

AIOps achieves this by combining automation with analytics and deep machine learning on a multi-layered technology platform, Infinidat's Neural Cache. Its deep learning capabilities deliver a zero-touch, "set-it-and-forget-it" experience that continues to optimize application environments and performance over time. Very significantly for today's economic environment, it dynamically adapts to changing application, user and performance demands without excessive administrative overhead

– using advanced predictive analytics and early issue detection, combined with proactive support.

Flexible consumption models

All these benefits are important, but they are not enough in isolation to satisfy today's enterprise challenges when it comes to cost cutting. It is also critical to flex how a business can consume their storage technology needs. While some organizations still prefer to buy equipment outright for their on-prem data centres, others prefer more flexible, cloud-like procurement models that allow for budget-friendly capacity- or usage-based payment approaches.

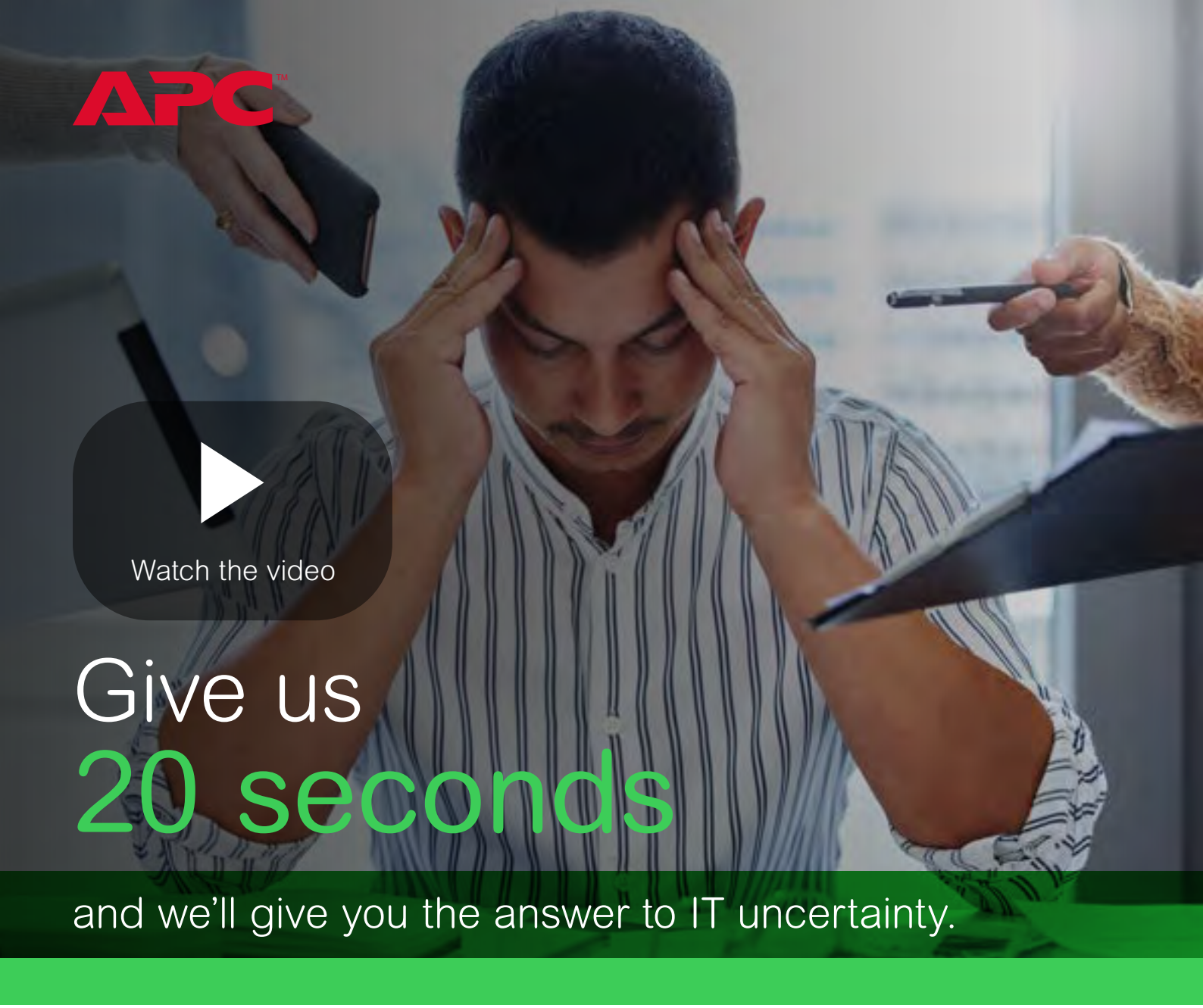
Flexible consumption is perhaps the most disruptive trend to impact enterprise IT over the past half-decade. Infinidat's flexible approach makes it particularly easy for organisations to work with us, with a choice of three distinct consumption approaches. The simplest and most traditional model is the standard up-front purchase, but even this offers some important cost saving advantages for customers thanks to the AIOps and deep machine learning capabilities. Uniquely, Infinidat's solutions are all-inclusive, spanning current and future feature upgrades, installation and 3 years of premium support. They also include a further cost benefit, a dedicated technical advisor (TA) to assist your in-house team and reduce any need for external technical consultants.

In tandem we offer Elastic Pricing, combining Infinidat's Capacity on Demand model with OPEX burst capability. Customers who are scaling their business rapidly and expect to grow further in the short term adopt this model. It's beneficial because Infinidat will deliver a full system to the customer, but only charge them for what they need. No license keys, buffer capacity or migrations are needed. The final addition to consumption-based pricing options is FLX, whereby customers pay according to what they use and need. It's very simple.

The more they need, the more they pay. And the less they need, the less they pay. If customers know they have large storage requirements for their mission-critical applications, we have the solution with our standard, up-front purchase model. If customers know they're going to grow, we have Elastic. If customers really aren't sure and want to remain flexible, we have FLX.

Almost all businesses are facing unique challenges and due to continuing economic uncertainties, a considerable amount of turbulence lies ahead.

Whilst we can never fully predict the future, enterprises can always model for best-case outcomes. This same logic applies to storage ad one thing every enterprise user can always be sure of, it's that Infinidat's technical teams have their best interests at heart.



IT is a serious matter but, let's face it, there are some strange things that people in IT face every day.

That's what **IT Happens** is all about.

It's a quick look at how nothing in IT is certain. **But it can be.**

See how Schneider Electric, through the power of APC offerings and **EcoStruxure™ IT software**, can provide the resilience, reliability, and sustainability you need. That's no joke.

www.apc.com

Life Is On Schneider Electric

Enterprise architecture must evolve for digital transformation

Why would we restrict our businesses to an architectural framework developed before the internet, mobile computing, and cybersecurity?

BY TABITHA POWELL, SENIOR SPECIALIST, OFFICE OF THE CTO AT F5

ON THE ROAD to innovation, it's not uncommon for fundamental architectures – the guiding frameworks and standards – to be modernized in order to enable continued progress.

Take for instance the telescope. We'll skip over optics and light theory and jump to the function that prompted a telescope's architectural framework. People wanted to be able to see "faraway things as though nearby". Working with the available technology they created a framework, which included optic lenses and a cylindrical tube. That was more than 400 years ago.

While early telescopes were confined to something people could physically peer through, scientists realized that with new technology capable of transmitting images over waves and launching things outside of Earth's atmosphere, the architectural framework should be updated. This eventually enabled the development of the Hubble telescope. It still called for lenses and a cylindrical

tube, but the framework no longer required it to be physically within reach – telescopes could be mobile and operated from afar – allowing for continued innovations.

By contrast, today's enterprise architecture has not been modernized; it's like we're working with the initial outline of the telescope. By circumventing this important evolution organizations create more friction down the line. Why? Because it's generally harder to alter the foundation when it's already holding up a three-story home (not to mix metaphors). The digital transformation journey businesses are on is also a continuous road of innovation, and no one wants to arrive at a dead end then be forced to backtrack, but that's what digital businesses can expect if they don't modernize their enterprise architecture.

Outdated frameworks impede innovation

Current enterprise architectures (EAs) were being developed in the 1980s, and while there have been iterations of them since, widely adopted EAs are still utilizing the same architectural foundations as when they were established. Take for example The Open Group Architecture Framework (TOGAF), which had its first version published in 1995. The foundation still consists of the same four architectural domains: business, application, data, and technical.

That foundation was laid before the internet existed. And this is part of the problem. Today it is not uncommon to equate technology with the worldwide connection that is so ingrained in our everyday lives. While TOGAF has managed to support businesses up to now by versioning, including integrating the internet and new capabilities into its architecture, it wasn't purpose-built for today's possibilities – digital business. Our understanding of what's possible drives the need for modernizing enterprise architecture.

Modernize for mobility

As technological advances create new possibilities the enterprise architecture needs to adapt to new constraints – or lack thereof – to sustain continued innovation. Advancements like Wi-Fi and 5G have changed the landscape. Computer applications can leave the data center and users are no longer static, they're mobile. The pressure has been building for a modern architectural framework intentionally designed to account for these and other advances. Without this modernized enterprise architecture innovation will stagnate, hindering the transformation businesses need to truly launch themselves into the digital space.

Protecting what's possible

In 2022 the US and collaborating countries completed and launched into space a new telescope, the James Webb Space Telescope (JWST). It was designed using a modernized architecture. With an updated understanding of what's possible—including the ability to detect and "see" infrared light instead of just visible light, the ability to transmit images back to earth from over one million miles away, and more – scientists believed there could be greater functions and capabilities of telescopes. With these increased possibilities came new challenges and therefore the architectural framework was yet again reimagined.

The James Webb Space Telescope still utilizes lenses and needs to collect light through a path, but instead of requiring a cylindrical tube to focus the incoming light, the architecture evolved for its new purpose – to collect the increased range of light that is infrared waves. This new purpose also presented a unique challenge. Everything above absolute zero registers as infrared light, so it was essential to mitigate interference from heat sources like the sun. The result was a modernized architectural framework to serve the evolved needs, which included the sunshield, spacecraft bus, optical telescope elements (OTE), and an Integrated Science Instrument Module (ISIM).

Similarly, while modernized EAs must be purpose-built to support new capabilities available to organizations following the establishment of the internet, they must also address emerging challenges. For example, mobility threatens security and ubiquitous access and connection increases users and demand on the resources. These are just some of the points of friction introduced in the path to digital business by the traditional architecture domains, indicating a need for new domains and concepts in the framework to remove that friction – like security, automation, and digital services.

Advancements like Wi-Fi and 5G have changed the landscape. Computer applications can leave the data center and users are no longer static, they're mobile

Like the evolution and modernization of the telescope, we have increased capabilities with today's technology compared with 30 years ago. The hardware is smaller, the communication languages are streamlined, and in general science has advanced providing for even more innovation.

For businesses, this means the ability to connect with their customers in a new way – digitally. But the enterprise architecture on which they build needs to be purposefully designed with today's understanding of what's possible. We wouldn't imagine trying to restrict today's astronomical study to a tool we can hold in our hands, so why would we restrict our businesses to an architectural framework developed before the internet, mobile computing, and cybersecurity?

Democratisation of enterprise-grade technology to fuel innovation

Democratisation of technology, where access to technology rapidly continues to become more accessible to more people, has risen to be a huge trend. With the potential to introduce innovation and long-term resiliency within organisations, executives now see tech democratisation as critical to their ability to scale.

BY SIMON JOHNSON, GENERAL MANAGER OF UK&I, FRESHWORKS

AS NEW TECHNOLOGIES EMERGE, and pressure on business leaders increases, there is no better time to take a deeper look at this topic. Whether it's moving from paper to spreadsheets, or turning to modern SaaS solutions to manage our business, we now have the chance to reimagine how we work, and how we engage our employees and customers – with digital technology on our side.

Why democratisation of enterprise-grade tech matters

As technology advances and permeates every aspect of the workplace, more and more employees are able to use technology to perform their job.

Despite organisation's recognising the positive impact that technology can have on business success, enterprise IT such as cloud-based ITSM (Information Technology Service Management), CMS (Content Management Systems) and business intelligence systems can often be overlooked, especially by SMEs.

Yet, by implementing the right enterprise technology at the right scale, companies can vastly improve their overall efficiency and performance in the market as well as improve employee productivity, communication, collaboration and satisfaction company-wide.

Democratising the right way

There are some defining steps companies should consider in their efforts to achieve technology democratisation. The first is accessibility; ensuring tech is accessible to your entire workforce is the most important step to democratising technology. Companies must assess how easily, with optimal training, a particular technology can be made available to their staff.

There is often a false assumption that in order to effectively implement enterprise IT, businesses will require an in-house expert or a tech-savvy team to deploy and use the technology. But in fact, the democratisation of technology is to a degree, a self-sustaining cycle. Modern ITSM tools to manage workflows are themselves not only easy to use – which is essential for driving access, but are also now easy to deploy and manage with a few specialised skills.

This is a key reason why modern ITSM solutions are finding more and more uses across businesses in all industries, automating repetitive tasks to free staff up for more value-creating work, driving efficiencies, and improving overall employee and customer experience. By searching for solutions that include out-of-the-box features based on pragmatic best-practice, your business will be able to deploy an ITSM solution quickly, enabling easier adoption, at scale.

Driving adoption is also important to getting full value from democratising technology. The measure of adoption is how widely a particular technology is used by the work force – having employees ask for access to a tool they see is saving a colleague time, is a great measure of success. Naturally, the rates of adoption will depend on a variety of factors like ease of use, whether the individuals are digitally adept, and the level of engagement required. While digitally adept employees will likely act as the change agents, it is important that the change is seen through the overall business and processes of an organisation – i.e. through HR, Sales, as well as IT. Therefore, ensuring this technology can be, and is engrained into all departments will enable greater collaboration across the company, and therefore greater efficiencies.

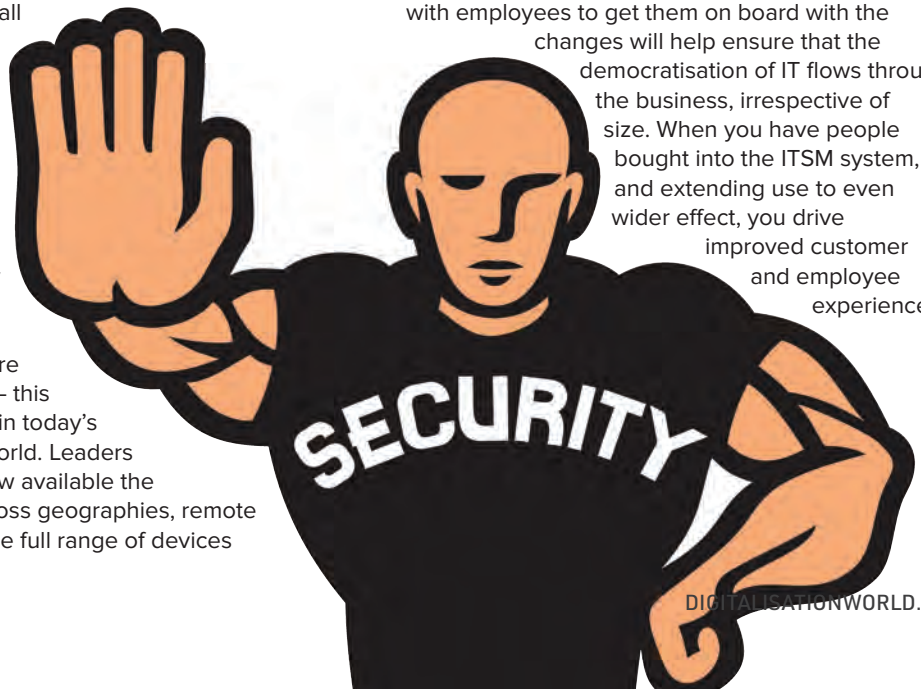
Lastly, to properly democratise tech, it must be available anywhere and everywhere – this is especially true in today's hybrid working world. Leaders must consider how available the technology is across geographies, remote work locations, the full range of devices etc. Fortunately, with modern ITSM solutions, you can deliver fast, scalable and secure services to your employees across all teams, office locations and time zones. If the answer is that any employee can access the platform at any given moment, then it's likely you are on the right track to democratising your IT.

The core benefits of democratising enterprise tech
It can be said that when all the above steps have been considered, democratisation of enterprise tech like ITMS is easy to achieve. It is therefore a no-brainer, especially when you consider the myriad of benefits that unified service management solutions can bring to your business – namely delivering delight to employees by increasing efficiency, productivity and satisfaction, but also by helping you realise greater ROI.

With robust automations, employees can eliminate repetitive tasks and manual processes, and drive service efficiency using no-code workflows. Not only will this liberate your employees of mundane processes that lead to productivity hurdles for your IT team, it will also drive service efficiency using no-code workflows and powerful automations. Having a single integrated service management platform can bridge silos, improve time to resolution, reduce costs, and improve visibility. Having a single integrated system also enables you to leverage the power of enterprise AI engines that sit at the heart of many modern ITSM solutions, so your employees can make smarter service desk decisions, increasing agent productivity, and elevating employee experiences.

Looking ahead to the future

The future looks bright for companies successfully implementing enterprise technology, especially for those achieving democratisation. The demand for increased agility and flexibility by today's workforce means that the IT team are no longer the sole 'gatekeepers' to this kind of technology, and departments company-wide have a lot to gain. For business leaders, choosing technology that is easily accessible is key, and consulting with employees to get them on board with the changes will help ensure that the democratisation of IT flows through the business, irrespective of size. When you have people bought into the ITSM system, and extending use to even wider effect, you drive improved customer and employee experience.



How enterprises are prioritising digital resiliency

Today's enterprises have faced a higher pace of change over the last few years, as existing digital transformation strategies were catalysed by the disruption of a global pandemic that restricted in-person working.

BY ADRIAN TAYLOR, REGIONAL VP AT A10 NETWORKS

THE PRESSURES on enterprises to fast-track IT strategies whilst reckoning with increased cyber risk and the competitive need to match other enterprises' digital transformation has created many challenges for enterprises in maintaining an IT infrastructure that is both resilient and secure. Overall, this has been a successful endeavour, and many enterprises transformation strategies are well underway.

Massive global macro-economic shifts have fundamentally changed the way companies operate, from the rise of remotely working employees to the adjustments of customer engagement strategies. Remote work was fairly common before the pandemic and already had an impact on IT strategy and the shift to cloud, including hybrid cloud. This trend has only accelerated due to the ease of remote deployment and accessibility for software, SaaS, and cloud options.

With all these changes, the spectre of security breaches is high. This explains the rise and popularity of Zero Trust as a framework for securing networks in these new realities, and as an effective tool to drive cybersecurity initiatives within the entire enterprise.

All this means that, in a post-pandemic era, digital resilience is a top priority for enterprises across all sectors, especially as cyber threats continue to accelerate. As a result, enterprise organisations have a broad spectrum of concerns as they look to shore up their defences.

Reflecting on and analysing the events of the last two years, 2022 is an ideal time to explore enterprise perceptions about the future. To gain these insights, A10 Networks surveyed 2,425 senior application and network professionals from across ten regions around the globe. Not surprisingly, we found high levels of concern around all aspects of digital transformation solutions and resilience, with a strong focus on business continuity.

The key features of the Enterprise IT landscape that we uncovered included:

Private Clouds are the Preferred Enterprise IT Environment

Even though the industry witnessed a rapid pivot to cloud in the last couple of years, plenty of on-premises environments remain. Twenty-three percent of respondents have retained an on-premises environment, and this is unlikely to change in the future. Private clouds were the preferred environment for 30 percent of respondents, while just under one quarter said their environment was in a public cloud with a similar percent in SaaS environments.

New Working Patterns and Digitalisation Prompt Strategy Reassessment

Resilience is certainly a board-level discussion in 2022, as senior leaders look to ensure that the business can cope with any future disruption. Our enterprise respondents said that digital transformation solutions, business continuity (both technically and organisationally), and stronger security requirements have all become paramount. This puts tremendous pressure on IT professionals to rethink their architectures and IT strategies to meet the challenge.

Asked to rate their concern about 11 different aspects of business resilience, nine out of 10 respondents expressed some level of concern about every issue. The top concerns were around the challenge of optimising security tools to ensure competitive advantage, utilising IT resources in the cloud, and enabling remote access and hybrid working while ensuring that staff feel supported in whatever work style they wish to adopt.

Top Cyber Threat Concerns for Enterprise IT

Without a doubt, the escalating threat landscape is causing a broad array of concerns from respondents. Chief among them is the loss of sensitive assets and data, followed by the disruptive impact of downtime or network lockdown. In response, there was an evident shift to a Zero Trust security approach. One-third (30%) of enterprise organisations surveyed said that they had already adopted a Zero Trust model.

Looking to the future, the adoption of cybersecurity initiatives is likely to remain high and continue to grow. The increasingly porous networks developed under COVID-19 will require a more pervasive adoption of the Zero Trust model within enterprises as all employees become more aware of the benefits of such a strategy and approach.

Although the urgent demands of the pandemic have lessened, it is clear that there is unlikely to be any relief from the pressures for enterprises and their IT practitioners, whether in infrastructure or security domains

Although the urgent demands of the pandemic have lessened, it is clear that there is unlikely to be any relief from the pressures for enterprises and their IT practitioners, whether in infrastructure or security domains. Enterprises will be dealing with the impact of these pandemic-related changes for years to come, alongside the continued integration of newer technologies, strategies, and evolving standards.

Therefore, organisations must meet their multifaceted digital resiliency needs by continuing to invest in modern technologies that will support ongoing digital transformation initiatives while striking the balance between strong Zero Trust defence and operational agility.

Understanding the Metaverse and its applications

Even though the Metaverse has been the buzz word for quite some time, most people still ask the question 'what exactly is metaverse?'.

BY MAHESH RANGABHAT, HEAD OF GLOBAL DIGITAL MARKETING AND AUTOMATION AT TECNOTREE

THE METAVERSE is a virtual reality space in which users can interact with a computer generated environment and other users. It's been called the future of the internet, and many industries are planning to incorporate it into their long-term plan. Although the meaning of metaverse is expanding daily and it's still difficult to define exactly what it means, here we will give an overview of the Metaverse, it's use-cases and how it can be used as a tool for brands.

So, what exactly is the Metaverse?

Our lives are already intersected virtually – through surfing on web, social media or giving commands to Alexa. Through the Metaverse there are more layers added to the mix with the help of augmented reality (AR), virtual reality (VR) and mixed reality (MR), which have the capability of immersing you in a more virtual environment using avatars and holograms. The Metaverse has the capacity to provide information in the real world. For example, there may be smart glasses that will remind you of someone's birthday when you meet them, and VR gloves may allow you to feel objects that are not present. You may also be able to visit popular destinations or have a preview of your new house even before it is built.

The Metaverse refers to a shared virtual world that offers 3D virtual spaces, solutions and environments created by users – a virtual shared area open to everyone. There are digital twins created for the

physical world we live in, and metaverse through the network, provides an access to this digital world. The Metaverse offers a unique opportunity for growth within the immersive world of virtual reality, with the potential to completely transform industry verticals.

There have been precursors to the Metaverse in the form of Linden Lab's multimedia platform, Second Life, launched in 2003, and other 3D interactive platforms such as Roblox and Fortnite, that allow users to create avatars and interact with other gamers. Even though the Metaverse is not yet controlled by anyone, it comes with growing sets of ethical codes, government policies and standards. The Metaverse is the natural evolution of the internet and is expected to be open just like the internet.

Metaverse as a tool and a target

In terms of usage metaverse can be utilised as a tool or as a target. As a tool metaverse can solve problems in the real world. It can be used to perform tasks such as psychological treatments, explore remote areas, and train workforce. Familiar environments can be created making it possible to perform tasks that are difficult, avoiding hindrances such as costs or physical travel. It can simplify difficult tasks such as engineering using different modes, optics, computing, and statistics as tools. User behaviour in the Metaverse is recorded through quantified data and can be analysed better enabling accurate research - making it useful for business, marketing, and policy related tasks.

The Metaverse as a target can be used to perform services and therefore generate profit. It is not just a reflection of the real world, rather it can be used for social communication including games, entertainment as well as academic problem solving. Companies can use the Metaverse as a potential new market to gain income and advertise. The Metaverse makes it possible to have role playing through interactions and avatars and facilitate commercial activities such as real estate.

How can the Metaverse be used in various applications?

The Metaverse can be a fantastic experience enabling users to explore other worlds. With this understanding, companies are now spending billions to create immersive experiences. Here are some of the most useful applications for metaverse:

AR/VR games - Developers will be able to use the Metaverse SDK to build games and applications that take full advantage of Virtual Reality. It will enable developers to create web3 games and metaverse experiences across various value chains. VR headsets have the capability of exposing the user to high-quality representations, leading to an extremely engaging experience. The Metaverse use cases also include AR/VR games with digital assets that can be exchanged for cryptocurrencies such as ETP and NFTs (Non-Fungible Tokens).

Gamers are going to be at the front lines of this evolution. But for them to hop on to the metaverse journey, the hurdles around poor internet connectivity and expensive hardware need to be addressed. Gamers wouldn't mind paying more if the cloud gaming subscription is bundled with dedicated 5G connectivity.

Healthcare

Metaverse has the best application in healthcare using augmented reality (AR), with potential to improve all aspects from mental health to complicated surgeries. With the use of AR, AI, and virtual reality, the knowledge base and skills of medical students can be enhanced. Surgical procedures can further be improved with the usage of surgical assistive tools by using technology such as HoloLens.

> The Metaverse refers to a shared virtual world that offers 3D virtual spaces, solutions and environments created by users – a virtual shared area open to everyone. There are digital twins created for the physical world we live in, and metaverse through the network, provides an access to this digital world

Manufacturing

Manufacturing use cases for metaverse include 3D design validation, remote inspection, and virtual operation. VR applications in the Metaverse can help with employee training with safety and real-life simulations of risky situations. This results in reduced accidents and efficient production process resulting in better products.

Education

Traditional teaching methods can never compare to the high level of effectiveness offered by virtual reality in terms of highlighting learning concepts through attractive visuals. Students are more motivated to learn since they can experience learning in a more real-life scenario.

Military

AR and VR has a big role to play in military applications. Tactical Augmented Reality (TAR) is a technology like night vision goggles, that can help with providing precise locations during military combats.

Sports

Potential use cases for the Metaverse in sports will enable an even better sports-viewing experience. Imagine stepping into an arena where everyone is in their own unique avatar. Here players will be able to create their own avatars, socialise, co-watch, train, work, purchase equipment, and participate in sports league. Some sports use cases for the Metaverse could include VR player training programmes and VR replay analysis applications. Matches could have a panoramic view of the entire game, and the audience could zoom into any aspect of the game.

Enterprises

Enterprises have the opportunity to develop new application types using augmented or virtual reality experiences in areas such as training, field service, remote maintenance, or product visualisation. Through the Metaverse, companies can create more human interactions and experiences. Interviews, meetings or walkthroughs can take place even before someone starts working at a company. Similarly, live product demos and interactive training could take place.

Metaverse and the role of connectivity providers

Connectivity is what ties the Metaverse development and broadening of the virtual worlds. Consumers and businesses will be able to enter metaverse with the help of 5G – with its peak data speeds of multi-gigabits per second, ultra-low latency, and great reliability. Telecom operators can play a more important role in the metaverse value chain. They can be cocreators in the metaverse universe by leveraging technologies such as 5G, Edge Computing, and AI. Telecom operators can look at utilizing the Metaverse for monetising new opportunities and enhancing customer experience.

For this to happen, the industry will require in-home connectivity packages that guarantees bandwidth, functionality, and security to allow Metaverse use cases to thrive. This can be achieved through the collaboration of many partners, including Communication Service Providers (CSPs), private enterprise networks, and IoT developers to ensure a consistent experience. With network advancement to 6G, further development in the Metaverse is expected to take place by 2030. This shift will improve the Metaverse with the higher bandwidth speed and lower latency of 6G network.

That being said, similar to the internet, it needs a close watch for safety and privacy, along with the competition and open access that enables the Metaverse to evolve. So, creating public policies for Metaverse needs to be a collaborative effort where industry leaders and policy makers along with potential users in various communities are involved. The societal effects of metaverse also needs to be considered, in terms of social interactions, psychological aspects related to addiction, application of law, trust, privacy, bias, and disinformation. The Metaverse itself will see the emergence of new technologies that will exploit the changes. It's an exciting time for technology, and we look forward to watching it play out.

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

Two technology principles to help offset the economic uncertainty

As businesses grapple with an increasingly uncertain economic environment, technologists must play their part in protecting their organisations. Building resilience starts with making sure your organisation is well-positioned, including being flexible and agile to adapt in a shifting macro-economic environment.

BY TIM CHINCHEN, SENIOR DIRECTOR, SOLUTIONS CONSULTING, PAGERDUTY

THE BEST TIME to plant a tree is twenty years ago, and the second best time is now. Preparation can help ease the blows that will land if budgets shrink and customers lighten their spending. Even as technology budgets come under pressure teams will be expected to not only keep the lights on but maintain quality of services to keep their customers. Anything that threatens IT operations can have a direct impact on customer experience. Without business resilience measures taken now, incidents and outages will risk customer happiness, halt business innovation, and very likely impact the operational staff who must work daily miracles, causing talent flight.

Back to first principles: Staying agile and flexible
Staying adaptable to circumstances is key for resilience in tough times. Technology will glitch and software will occasionally fail. Vital operations are complex and dependent on many factors, often outside of the organisation's control. Yet doing business relies on digital operations continuing to perform under all conditions or recovering well in the event of an incident.

Operational complexity tends to encourage bloat when times are easy. Trimming the excess and focusing digital operations on efficiency is key in difficult times. Business resilience rests on multiple foundations, but foundational to the ability of the firm to keep revenue coming in, sits its digital operations. Forecasting the impact of changes on service levels and staff productivity and welfare will be a key provision in ensuring infrastructure and operational resilience over the next one to three years.

Using operational data to forecast maintenance or replacement, and to plan staffing supports flexibility. A larger business with higher DevOps maturity might start by improving business processes and will channel resources towards optimising workflows. Smaller or less digitally mature organisations might start with ensuring that they know their most likely incident scenarios and what supplier or support staff needs to be given access to which systems to ensure that break-fix remediations happen smoothly. In any situation, organisations improve their resiliency when they mature their digital operations to become proactive in solving incidents before they create a cascading impact.

The blockers of flexibility and agility

Smooth operations are foiled by staff engaging in 'manual toil' and outdated processes and technologies. It can add up. PagerDuty's 2022 State of Digital Operations report found that operational teams are afflicted by overwork and burnout. 64% of respondents expected increased turnover this year because of these factors. The overall cause of

To halt this negative cycle, organisations must take a beat and consider how they shift to greater levels of operational performance as they move into economic firefighting. Complexity is here to stay, but resilient digital operations are achievable

all these factors stems from the increase in digital complexity. Particularly for those less operationally mature organisations, this causes chaos from increasingly frequent incidents. The more operationally mature – particularly in DevOps – the organisation, the greater flexibility and agility they tend to bring to all situations, resulting in greater resilience. With highly complex digital operations central to all business, inefficiency can compound when any element wobbles, leading to ever greater increases in all those factors: Manual toil, creaking processes, and dependent technologies all creating a perfect storm.

To halt this negative cycle, organisations must take a beat and consider how they shift to greater levels of operational performance as they move into economic firefighting. Complexity is here to stay, but resilient digital operations are achievable. Key principles include simplification of the tech stack, tracing dependencies and owners, and breaking down silos of communication and ownership. Making sense of infrastructure data so that signals can be brought out of noise and a proactive stance taken on incident management is a very effective measure to improve digital resilience and impact overall business resilience. Back to that mantra: Flexible and agile will win the day.

Full speed to operational maturity

Proper operational maturity immediately puts the business on a strong footing and also gives teams a more manageable workload where they are able to manage incidents predictably and effectively. What's more, they will be able to schedule maintenance with greater regularity in order to prevent incidents from ever arising.

Our report outlines the five stages of operational maturity:

- **Manual:** No inbound integrations
- **Reactive:** Has some inbound integrations but not other configurations
- **Responsive:** Has schedules and multiple escalation levels
- **Proactive:** Uses outbound integrations, service dependencies, change events, or response plays
- **Preventative:** Adopts event intelligence features or consumes analytics

14% classified their teams as manual or reactive, 50% as responsive, and 8% as proactive. We saw that those who were reactive had a noticeably higher turnover than the preventative maturity cohort.

Three steps

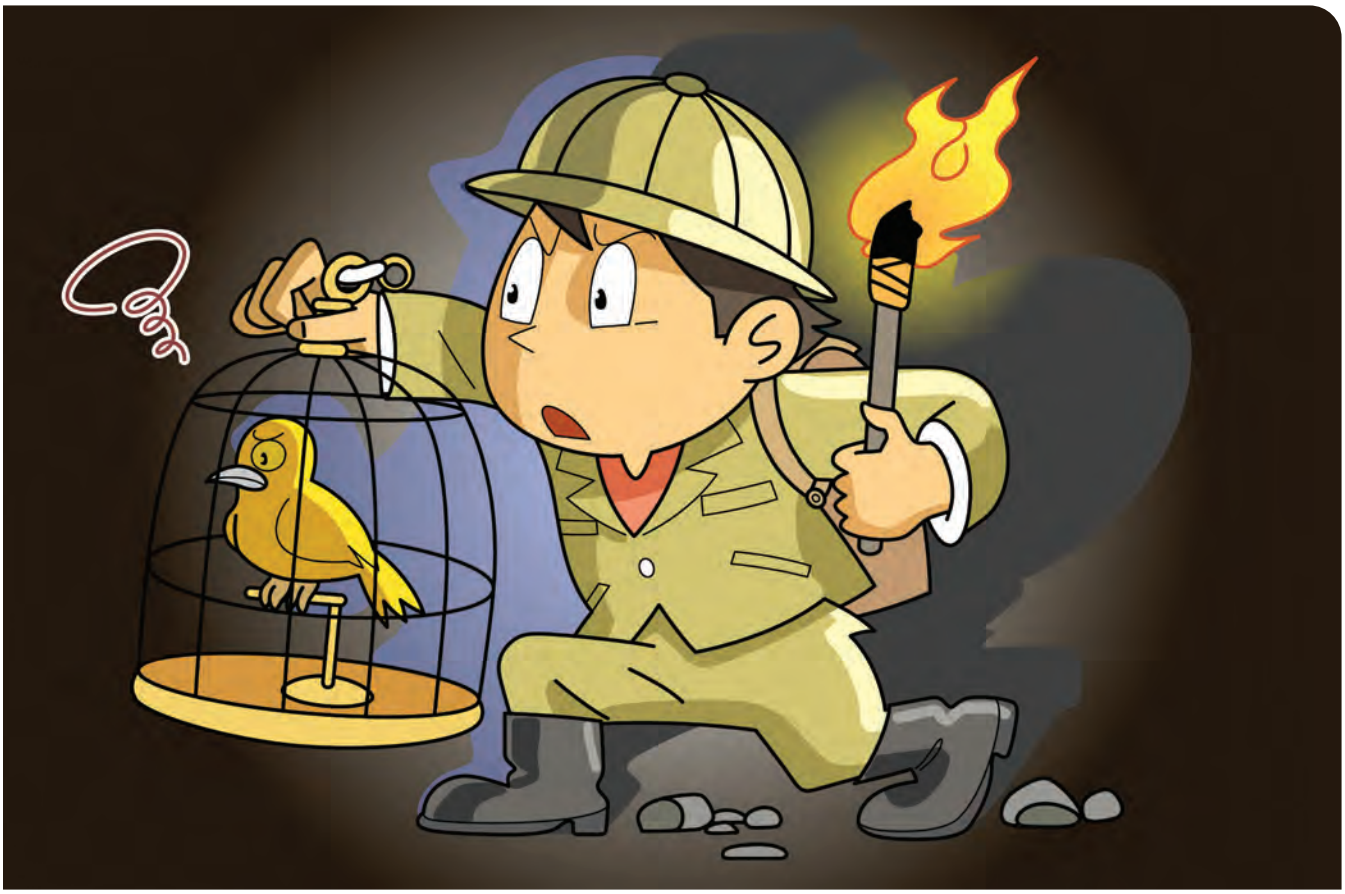
Here's how to go about getting that flexibility and agility embedded as a prelude to raising resilience and operational maturity.

First, technology must incorporate automation to enhance team and process efficiency. Organisations will go through a period of education as they operationalise machine learning and AI models for success.

Secondly, aim for the flexibility to manage changing situations and to scale technology and team processes. Planning this in advance will help guide resource allocation and reassess workloads.

Thirdly, teams should have the tools and training for proactive operations where they can anticipate situational requirements and take steps to remediate those triggers of future disruption.

Putting this all together will lead to resilience through operational maturity. Your teams will not be stuck in break-fix mode. Faults will be minimised in advance, leading to time for innovation and improvement. The result is better business operations in toto. Just what's needed as the economic waters get choppy.



Exploring the IT coal mine? Don't forget your canaries

Throughout these uncertain times, it's easy for organisations to lose their way and become unsure of their priorities.

BY EIMEAR GUNN, UKI DIGITAL WORKPLACE SERVICES PRACTICE LEADER, KYNDRYL

It's a difficult time for businesses. Global economic uncertainty is causing organisations across all industries to cut budgets and tighten their purse strings. Despite being part of one of the strongest sectors (financially) throughout the pandemic, confidence is currently low for tech companies.

Stocks have recently crashed on public markets, and we've also seen mass job cuts globally in the sector. Throughout these uncertain times, it's easy for organisations to lose their way and become unsure of their priorities. However, what they mustn't do is lose sight of what is valuable within the business. Employees are and always will be the lifeblood of a business, their canary in the coal mine. Despite this, they are often overlooked and undervalued as a source of insight into their organisation's IT infrastructure operations.

However rapidly artificial intelligence (AI) and machine learning (LM) are developing, humans will always play an essential part in the roll out and implementation of new technologies. The very nature of tech as an industry relies on the constant regeneration of products and services, with new and innovative developments. For example, the rise of low code/no code platforms and solutions will soon form a large part of software engineers' toolkits.

As a result, there will be fewer jobs for people who formerly coded repetitive and ubiquitous functions. Similarly, as cloud functions continue to grow exponentially in use, managing traditional on-premises data centres may soon become obsolete. As such, IT staff in those roles should begin pivoting to new specialised roles now.

Given that the skillsets of tech professionals are constantly having to be revised, it's easy to see why misconceptions exist around the role of employees in the industry. Despite this, the workforce will always remain an IT organisation's most valuable asset, with employees truly at the front line of operations. When the reality of a business's IT infrastructure is observed and understood from the employee's perspective, processes across the business can be brought in line to support people to deliver every aspect of the organisation's work.

Outdated metrics

For many businesses, their traditional ways of working have been used and relied upon for decades. But in that time, both employees and their organisations have evolved immensely. As such, the workforce depends on change occurring to survive and thrive.

The way in which IT operations are measured and run is a great example of this. For example, traditionally, organisations have used of Service-Level Agreements (SLAs) and Key Performance Indicators (KPIs) to measure progress. An SLA defines the level of service expected by a customer from a supplier, laying out the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-on service levels not be achieved. SLAs often take into account factors such as:

- Performance and accuracy
- Timelines (for example, response time)
- Availability such as uptime and downtime
- Service hours and type of support expected

They ensure both the service provider and user are on the same page and help to:

- Establish clear goals
- Set expectations and baselines
- Keep companies accountable
- Ensure timely support
- Make it easier to measure failure and success

SLAs have long been considered a cornerstone of many businesses, but it's reaching the point where they're an outdated metric. In practice, truly understanding an organisations' IT infrastructure from an employee perspective means recognising the increasing irrelevance of SLAs and KPIs and instead implementing metrics that more closely reflect the realities of an organisation's IT department.

Updating the measurement process

One of the roadblocks here is that SLAs are often deeply ingrained within the fibre of a business. Therefore, replacing the metrics may be difficult to execute. It's as much a mindset issue as it is process-based.

SLAs also have the advantage of being 'native' to the technology at hand; they ensure performance via measurements, like network throughput responsiveness, which are inherently available as a side-effect of operating that technology. As such, organisations may shy away from new measurements as they might appear to be more subjective or qualitative measurements of actual usage experience, which need to be implemented more consciously in addition to the systems themselves.

Implementing experience-level agreements

Implementing a new metric allows organisations to pull meaningful insights out of multiple data sources in a way that empowers businesses to enforce minimum performance levels. Introducing Experience-Level Agreements (XLAs) and Experience Performance Indicators. Though the term has been used and defined in a variety of different ways, essentially, XLAs focus on the measurement of outcomes and the value given by a service, as opposed to having judicial agreements on measures. Unlike SLAs, they combine direct reporting (like the percentage of tickets closed within a given timeframe) and user feedback (such as promoter scores and internal sentiment analysis), resulting in a powerful way of aligning IT strategy with user needs.

User centricity is a major benefit of implementing XLAs. SLAs don't show how IT is performing from the perspective of employees and the business as a whole. That's why it's important to complement them with XLAs and get a better understanding of how employees feel about workplace technology and their organisation's IT support.

An employee's market

In today's labour market, employees are firmly in the driving seat. We've seen The Great Resignation and now 'Quiet Quitting'. Employees know their worth and are taking advantage of the plentiful job vacancies that are currently on offer. As such, there's never been a more important time for organisations to re-evaluate their approach to employee engagement.

We know that technology can have a real impact on employee engagement and loyalty, as well-supported employees are 85% more likely to stay beyond three years. Organisations must ensure that they are considering the employee perspective and needs when it comes to making decisions on their IT infrastructure and departments. This will save significant time and money avoiding an unnecessary recruitment drive, as content employees are more likely to stay put in their organisations. However, the benefits go beyond this as a happy workforce is proven to be more motivated and productive. Regardless of sector, organisations must always consider the needs and priorities of their employees. The importance of maintaining a happy workforce cannot be understated – whatever the outside circumstances. Updating processes and strategies in line with this is key to future-proofing the organisation and ensuring the overall smooth running of the business.

Avoiding shadow IT through no code / low code technologies

Shadow IT is a scenario that makes every IT department uncomfortable: Parallel IT structures can develop in companies over a long period and typically without the knowledge of IT managers.

BY NEIL MURPHY, GLOBAL CHANNEL CHIEF, ABBYY

The use of such solutions, which are not integrated into official structures, represents a major risk to the security of a company. With the advent of so-called no code/low code technologies however, employees without IT expertise now have the right tools at their fingertips to work with artificial intelligence (AI) - and without the need for costly IT implementations or training.

The benefits of such solutions for the workforce are obvious. However, solutions in a modern company should only be implemented with coordination from the IT department and based on internal company guidelines. It's often the role of the CISO (Chief Information Security Officer) to set this policy. Uncontrolled shadow IT must be avoided from the outset and employees must be informed at an early stage about the inherent risks from IT structures that have been changed unintentionally.

Digital natives as drivers of shadow IT

By definition, Shadow IT is the use of any IT system or software that is used without the knowledge of or prior consultation with the company's IT department. This creates structures outside the controlled IT architecture that have security gaps and can therefore provide a perfect attack surface for cybercriminals.

The more unknown applications are used within a company, the higher the risk that outsiders will gain access to the entire corporate network. This is because the IT department cannot protect itself from threats it does not know exist. In addition to the security risk, shadow IT also has other disadvantages. The fact that the acquisition of new software is often only regulated internally within a specific department means that there is no overall uniform overview of which software and licenses are currently in circulation. This can inadvertently lead to duplicate purchases - costs that would be better spent elsewhere.

To effectively combat shadow IT, you must first understand why it occurs. Most employees who use such applications without consulting the IT department don't usually have bad intentions. One relevant trigger for the growth of shadow IT in recent years is the new generation of digital natives, who are increasingly entering the job market and bringing with them a high level of digital affinity. When they encounter digitalisation hurdles, they want to take things into their own hands and create solutions to their problems or independently make their way of working more efficient.

Examples include installing and configuring systems that perform business functions such as automation and data integration, or developing data repositories such as a spreadsheet used to manage customer or product data. In addition, we live in a world that is changing faster than ever. There is no time for long coordination loops with the IT department for new acquisitions, which means that employees are increasingly turning to faster, yet more uncertain, solutions.

No Code/Low Code in action against shadow IT

If one of the main reasons for the growth in shadow IT is employees who are happy to tackle the digitisation of their working methods themselves, then companies should take the next step and provide them with the appropriate tools to enable them to do just that. But this must be done without jeopardising the security of the company.

So-called No Code/Low Code platforms are particularly well suited for this purpose, whereby even non-technical users can easily program and compile applications or small apps using drag & drop. No Code/Low Code platforms can therefore function similarly to the building block principle. We see these types of platforms being well suited for improving the automaton of tedious, time-consuming manual processes such as document processing. Employees are empowered to add AI skills that read and understand documents to increase their productivity. At the same time however, the IT department has a precise overview at all times and can better monitor the constructs and adjust them if necessary. The use of these platforms reduces the need for unauthorised programs and applications - and employees can improve their day-to-day work and be more flexible.

The emergence of shadow IT in companies is often an indication that employees want more digitisation. However, to protect themselves from the dangers and rising costs that come with it, companies should no longer fear the fundamentals of decentralised IT. They should instead provide their employees with the right tools to participate independently in the digitisation of their company

Transparent insight into structures is the key

Before implementing these solutions, IT departments should first gain an overview of the current situation in their organisations. How are they interacting with systems and processes? What applications do employees access outside the established IT structure? What requirements do they fulfil and for which processes do employees need them?

Based on this process and task mining of information, the IT department can then make an informed decision about which functions colleagues need, and which platform is therefore best suited for their company, whether for evaluating work processes or for intelligent document processing. Additionally, the necessary understanding around the dangers of shadow IT and the implications for cybersecurity must be created among all employees.

The emergence of shadow IT in companies is often an indication that employees want more digitisation. However, to protect themselves from the dangers and rising costs that come with it, companies should no longer fear the fundamentals of decentralised IT. They should instead provide their employees with the right tools to participate independently in the digitisation of their company.

RPA is not a silver bullet

Why low-code holds the key to digital transformation success

BY MAT RULE, FOUNDER AND CEO OF TOCA

IF THE UK's businesses didn't need to modernise before the pandemic, they certainly do now. The existential crisis many were plunged into over the past two years has reinforced the resolve of boardrooms everywhere that digital transformation is the future. When deployed effectively, it helps to deliver the agility that every business craves, whilst driving the operational efficiencies and productivity gains essential to survival in a period of high inflation and rising costs.

In this context, robotic process automation (RPA) can be a useful tool. But when deployed the wrong way, or in isolation, it may actually end up worsening legacy dependencies rather than alleviating them. Instead, organisations need to think about the bigger picture – by bringing together apps, automation and extensible integration in a single low-code platform. That's the best way to achieve modernization at a pace that fits the business.

Why we need to modernise

IT modernisation has accelerated significantly during the pandemic, in some industries fast-forwarding businesses by several years. Some experts claim that organisations were pushed over a «technology tipping point» which has transformed them forever. As users rushed online during the crisis, businesses followed suit. Now as COVID recedes, both are staying put in a digital-first world. But this is putting an intense strain on internal corporate IT resources.

Complex user journeys and business processes must be mapped, digitised and, in many cases, automated. Whether it's onboarding a new banking customer or ensuring an NHS cancer patient is referred to the right clinicians, the stakes couldn't be higher. Three-quarters of UK consumers say they're likely to stop buying from a business following one bad customer service experience.

Adding to these pressures are the macroeconomic challenges of the post-COVID era, characterized by soaring energy prices, high wage demands and a scarcity of raw materials. A recent British Chambers of Commerce study found that 62 percent of businesses reported energy prices were forcing them to increase costs.

A slow death

Against this backdrop, increasing automation makes

a lot of sense. It can drive operational efficiencies, enhance employee and customer experiences, and help to keep a lid on rising business costs. Even before the current crisis, RPA was seen as something of a silver bullet to fast-tracking the kind of digital improvements businesses craved. By early 2020, nearly two-thirds (62 percent) of firms had either deployed the technology or were intending to start within the year. It was adopted with gusto for good reason, offering businesses the ability to scale their operations, free up staff to work on higher-value projects, reduce human error and deliver improved customer experiences.

However, many RPA projects have since been dying a slow death. Why? Because they were misconceived. IT and business leaders reasoned that ripping out all of their legacy systems and starting from scratch would result in too much cost and untenable project delays. So they sought to paper over the cracks by connecting RPA to legacy systems. But in many cases that has entrenched these same organisations even further into their legacy environments, creating webs of interdependencies that are hard to unravel and modernise.

By creating complex workarounds to bridge new solutions with old systems using RPA, they have painted themselves into a corner. Phil Fersht at analyst firm HfS summed it up back in 2019: “RPA hasn’t inspired enterprises to rewire their business processes – it’s really just helped them move data around the company faster and require less manual intervention.» And herein lies the problem.

A stepping stone to the cloud

Organisations need to find a way to modernize their hybrid legacy/cloud environments – in an incremental manner that can still deliver high-impact results in just a matter of weeks. This “art of the possible” approach is about leveraging existing processes and legacy systems, without getting locked into backwards-looking dependencies.

Where RPA helped businesses to continue what they were doing, combining automation with a low-code app development platform, businesses can start to re-engineer their applications. In this way, businesses can circumvent digital transformation roadblocks and empower business technologists to innovate, whilst freeing up developers to focus on mission-critical work.

However, even here there are challenges. Many no-code/low-code tools don’t support legacy solutions across different departments, systems and customer/user journeys, they can also exacerbate data silos.

That’s why organisations must look to consolidate on a single low-code platform that can support application development, automation and integration demands to drive faster, lower-cost digital transformation with no technical debt. In this way, they will be able to go beyond automating broken processes via siloed RPA deployments. Instead, businesses can deliver complete solutions that sit across disparate systems, and combine multiple technologies to create seamless digital experiences.

The right platform will be able to pull data from anywhere in the organisation to create applications that automate manual tasks, streamline inefficient processes and accelerate transformational change. Legacy isn’t going away any time soon. But with a hybrid approach like this that works, organizations have a stepping stone to a new cloud-centric future.

The API timebomb

The rise of the public API (Application Programming Interface) has been meteoric and it's rapidly taking over from the web app as the preferred mechanism for computer-to-computer communications.

BY ANDY MILLS, VP EMEA, CEQUENCE SECURITY

APIs ENABLE businesses to rapidly rollout real-time services by reducing the amount of code that developers need to write from scratch. They're so versatile that services can easily be swapped in and out without changes having to be made to the end application.

APIs have delivered velocity and competitive advantage to companies of all sizes with IDC research calculating that 10-50% of enterprise revenue is derived from APIs, making them the interface of choice for data interchange between applications.

But this versatility is not without its price. APIs are equally attractive to attackers because they provide ready access to the backend systems holding sensitive data. As adoption grows, so too does the API attack surface, potentially creating a ticking timebomb because of the poor security afforded to these middlemen.

According to the Enterprise Strategy Group (ESG), application environments will see a significant step change in the next two years. While 35% of organisations currently run their apps over public cloud i.e. IAAS, this will almost double to 67%, and while 39% run these apps over microservices today, this will rise to 71%. It's a similar story with API adoption. Today, 28% of web apps and websites use APIs but that will rise to 57%. But security isn't keeping pace.

Why protecting APIs is a struggle

APIs are stateless in nature and include the command, payload, and content, making them challenging to secure. Typically developed iteratively, they evolve over time, and this can see their footprint fluctuate or previous iterations continue to persist. Updates tend to be performed weekly or even daily, resulting in multiple earlier versions and if these aren't taken down or kept track of via an automated inventory they then can become shadow or zombie APIs and possible targets for attack.

Protecting APIs is no easy feat, which is why many security teams have adapted existing solutions such as Intrusion Prevention Systems (IPS), next gen firewalls, or app security tools such as a Web Application Firewall (WAF). However, these tools are unlikely to spot and flag malicious activity because while some may contain insecure code the vast majority won't but can still be taken over. Commonly referred to as 'Living off the Land' (LotL) attacks, this sees the API's own functionality used against it.

As a LotL attack doesn't involve the use of signatures or break any rules, such activity is unlikely to be detected. If we look at the top attack method according to the OWASP Top 10 – Broken Object Level Authorisation (BOLA formerly IDOR) – the attacker simply must understand the business logic of the API to gain legitimate access to data. This means that reverse-engineering an API can provide the insight needed; there's no need to exploit a vulnerability, so it could be argued it's not an attack in the traditional sense.

Trust in tools misplaced

What's concerning is that many aren't even aware that these tools are performing badly. The same ESG survey found that 46 percent use multiple tools because they think this increases the protection offered and 38 percent chose to add in yet more tools if these weren't performing as expected, adding to the technology stack and the headache of monitoring, and maintaining this. More than a third thought their solutions offered complete protection even though they weren't designed to provide API security.

	DISCOVERY Identify all public facing APIs	INVENTORY Track all identified APIs	COMPLIANCE Governance & best practices	DETECTION Detect attacks in action	PREVENTION Block attacks in real time	TESTING Secure APIs before go-live
API Gateways	○	◑	◑	○	○	○
API Security Tools	◔	◑	◑	◑	○	◑
CI/CD Tools	○	◕	◔	○	○	◑
Network Security Tools	○	○	○	◑	◑	○
App Security Tools (WAFs)	○	○	○	◑	◑	○
Bot Mitigation	○	○	○	◑	◑	○
API Specification Conformance Tools	○	○	◕	○	○	◕
Runtime Risk Assessment Tools	○	○	◕	○	○	◕
Testing (IAST, DAST, SAST, RASP)	○	○	●	○	○	●

➤ Tool Comparison: The patchwork protection offered by API security tools today

At this point it's also worth mentioning that there's a lot of confusion in the marketplace. An API gateway, for instance, should not be considered an API security tool. It enables the business to discover and track its APIs but does not discover or remediate coding errors nor does it stop or block API attacks. Indeed, an API gateway can exacerbate the problem by acting as a single point of failure that, if compromised, then provides access to all the APIs it routes.

There are numerous examples of companies falling foul of API attacks such as Account Takeover (ATO), for example, and as APIs become more entrenched in supply chains, so the problem grows. The attack against MailChimp earlier this year should serve as a warning of how far a well-orchestrated attack can reach. It saw the compromise of API keys used to provide account access and the attackers then actively sought out finance and crypto clients. One of these was Trezor, a maker of cryptowallets. A phishing email was then sent out to Trezor customers who were urged to reset their accounts using a cloned Trezor application.

Adopting a unified approach to API protection

Such attacks indicate that modern services built on API infrastructure are not adequately protected. It is only a matter of time before we begin to see API abuse ramp-up, which is why Gartner has already warned that APIs are set to become the most frequent attack vector. To counter this, we need to rethink our approach to API protection before it is too late.

To begin with, it's necessary to discover and create an accurate runtime inventory of APIs that documents when these are spun up, updated, or retired. This not only provides visibility but also the means to track APIs to ensure they comply with best practice. Armed with an inventory you can begin to focus on detection and looking for tell-tale signs of an attack or Indicators of Compromise (IoCs). Those tools we mentioned above can help here if the attack is based on known threats or involves a brute force attack, but the chances are it will be more subtle in approach, requiring behavioural analysis. Comparing log-in success and failure rates to accounts, for example, and benchmarking these within your industry, can help determine ATO attacks. Or perhaps a single username is being used but is originating from multiple IP addresses, again an IoC.

Of course, some APIs will contain insecure code which is why much of the emphasis to date has been on 'shift left' and the need to introduce security at the development stage. It's this focus that most API security tools take but in doing so they fail to allow for the fact that perfectly coded APIs can still be susceptible to attack. Yes, APIs should be tested and secured before go-live, but coding errors or misconfiguration can happen after go-live too. In fact, the Cloud Security Alliance has just moved API misconfiguration from seventh to third place in its list of 'Top Threats to Cloud Computing', suggesting current approaches are not working.

The missing part of the puzzle which the security sector has until recently baulked at is prevention. Utilising machine learning, however, it becomes possible to spot a malicious attack masquerading as legitimate behaviour and to block attacks in real-time. Various techniques can then be used to create subterfuge, obfuscate potential targets, and deflect attacks. Taken together, all six elements – discovery, inventory, compliance, detection, prevention, and testing – then create a security approach that covers the entire API lifecycle offering unified API protection and our best hope when it comes to defusing the API attack surface.

Where are the tech-led solutions to the IT industry's own skills gap?

Like many industries, the technology sector is facing a significant and prolonged skills shortage. With a dearth of qualified candidates, training new hires to reduce the talent gap is costing business leaders not only money, but also their time as programs are being developed to address these growing concerns.

BY EMMANUEL MÉTHIVIER, BUSINESS PROGRAM DIRECTOR, AXWAY

ONE OF THE MAJOR influencing factors on the employment landscape in recent years has been the impact of 'The Great Resignation'. This term referred initially to major career changes that people made for a variety of reasons—to pursue a new vocation, start a new business, take early retirement, seek more purpose-fulfilling work, or to simply reduce overwork and stress.

But more recently, this situation has evolved into a different scenario, and today, organisations must also not only cope with the talent shortage caused by lack of candidate choice, but also the huge problems created when legacy staff move on. These people often embody company knowledge, experience, and cultural values that are extremely difficult to replace, particularly in the short term. Alongside the growing skills shortage came a push from business leaders to undergo digital transformation strategies. For instance, companies have been investing heavily to bring on new and powerful software and hardware like the cloud, IoT devices, and a variety of APIs to help them introduce or scale-up automation to address this skills gap challenge.

Embracing new opportunities – Applying APIs

It goes without saying that effective recruitment hinges on finding the right personnel at the moment

when they are needed. All this takes time, effort and quite often, significant financial outlay. But what if there were other options? Can businesses come up with fresh tech-led strategies to combat the talent exodus?

The current labour scarcity gives a chance for innovative thinking within businesses. This is crucial at a time when despite obvious economic challenges, UK unemployment has fallen to its lowest level since 1974. Looking at APIs specifically, these are pieces of software that provide developers with a set of functions and procedures whereby one application is able access the data and features of other applications, services or operating systems.

In practical terms, the role of APIs is as a go-between for different software platforms, allowing two unrelated applications to interconnect, share data and functionality. As such, APIs represent one key area of technology innovation that is able to help reduce the skills gap, not least because of their third-party capabilities, but also their ability to be used by non-technical employees across teams, companies, partners and clients. This gives businesses a great chance to overcome the "great resignation" dilemma and simultaneously address today's and tomorrow's market demands.
In practical terms, this means transitioning to the digital era and utilising a combination of cloud, SaaS, and API-enabled EDI and B2B integration solutions. According to a recent McKinsey & Co. study, there is a "$1 trillion opportunity" at stake, as more organisations implement cutting-edge technologies like augmented reality, blockchain, machine learning and artificial intelligence.

As a result, businesses are accelerating their plans to move operations to the cloud in order to save costs, modernise their B2B ecosystems, make data available to suppliers, boost productivity and expand their reach. Collectively, these technologies are helping organisations to directly address their current skills shortages or help retain top talent with more powerful and effective technologies. Yet all of this can take some time. The challenge is to work with specialists to support current key operations in an efficient manner.

B2B integration

As suppliers and partners move to the cloud, B2B integration – connecting an enterprise to all its customers, suppliers, financial institutions and regulatory bodies to quickly communicate with them – is becoming more complex. At the same time, IT leaders are being inundated with a wide variety of options, platforms and services to help them digitally transform their processes.

To inform decision-making and ensure organisations choose the right platform for their needs, there are some key questions to consider:

- Does current B2B integration support traditional EDI flows while also satisfying customers' API-driven demands in today's digital economy?
- Do existing systems work in tandem with the shift to the "Integration as a service" model?
- Does cloud-based B2B integration have the potential to reduce costs by 20, 30 or even 40%?

To address these challenges, enterprises are increasingly outsourcing their B2B integration services to vendors that can help provide end-to-end integration services, along with the knowledge and skills needed to do this effectively.

More enterprises today rely on a balanced mix of API and EDI integrations to support and enhance their data flow. EDI and API managed cloud processes create more business agility, while cloud adoption can help reduce EDI risks and quickly scale up key parts of the business. Whilst the long-term implications of the IT skills gap still remain to be seen, companies need to be utilising technology to help meet their needs across increasingly competitive markets.

Finding the right fit

How to select monitoring solutions for your hybrid or cloud-based applications and infrastructure

BY MARTIN HODGSON, REGIONAL MANAGER, NORTHERN EUROPE, AT PAESSLER AG

AS COMPANIES rush to the cloud, it's crucial that IT teams have what they need to keep their applications and infrastructures up and running.

Our research found that one of the biggest frustrations for IT teams at work is when systems are flagged as having problems when none exist. A third of the respondents (34%) say false positives are their biggest bug bear.

Frustrations like these can lead to a drop in productivity and can be a huge distraction for teams, wasting their time trying to solve problems that don't actually exist, and preventing them from addressing actual business critical issues.

For organisations taking a cloud-first approach, there's even more to consider when searching for the best monitoring solution including cloud service costs or operating at a global scale.

So, what are the key areas to consider when looking at how you monitor your technology applications and infrastructure?

#1 Keep an eye on cloud service costs
If you follow the cloud-first approach, you will inevitably have virtual devices in use that reside on the Internet. Most likely, your provider is either Amazon Web Services (AWS), Google Cloud Platform (GCP) or Microsoft Azure.

All these services are charged for, and you are usually billed according to actual usage. The more computing resources and storage space you need, the higher the costs. So, the first important point is to keep track of these costs in as much detail as possible - and to be automatically notified as soon as costs threaten to get out of hand.

#2 Think global
If you're the IT administrator at a global company, for example a company with pure online sales for the distribution of its products with customers and partners located all over the world, thinking on a global scale, and having an accessible online store is essential.

The same applies to employees, who need fast access to the necessary cloud resources at all times, whether from Europe or from Asia. The future monitoring solution must be able to regularly check and permanently monitor worldwide accessibility.

#3 Combine IT and OT
One of the best ways to minimise blind spots in your infrastructure is to consolidate all your monitoring data in one tool. For monitoring the industrial Ethernet, you can use the same principles as traditional IT, for example: SNMP, bandwidth monitoring with flow protocols, and so on.

Industrial gateways can be monitored using OPC UA and other protocols. If your devices support Modbus, a common OT protocol, you can also hand it over to the care of tools such as PRTG.

#4 Don't forget your local resources
In addition to all the cloud services and the production floor, many companies also still have local components that they also want to monitor. This is where monitoring tools can make full use of a unified monitoring approach - even if the actual monitoring solution resides completely in the cloud.

If you're the IT administrator at a global company, for example a company with pure online sales for the distribution of its products with customers and partners located all over the world, thinking on a global scale, and having an accessible online store is essential

#5 Discover peace of mind
An all-in-one monitoring solution that keeps an eye on your entire business infrastructure and alerts you before problems occur nothing less should be the goal of every admin.

You should also make sure that you have individually configurable dashboard functions available. This way you can create overviews and always have an insight into your critical infrastructure components.

If a component in your network is faulty, a properly configured notification management system helps you to ensure that the responsible colleagues are informed immediately.

Monitoring solutions of this nature not only benefit the infrastructure at hand but allow for your company's team to sleep tight at night. Nothing is better than knowing you have an IT/OT infrastructure guardian protecting your systems 24x7, 365x12.

Legacy systems: What's needed for successful application modernisation?

The main goal of legacy application modernisation is that the business and IT both have a better understanding of the data landscape across the enterprise while also ensuring business resilience.

BY DANNY SANDWELL, DATA STRATEGIST AT QUEST.

ONE OF THE BIGGEST HURDLES to application modernisation is the fear of change. Too many organisations are adhering to the saying "if it isn't broke, don't fix it," and are simply unwilling to risk disrupting something that still works and is critical for the business functions.

As a result, many organisations are still operating with outdated and potentially vulnerable legacy systems. The challenge is that legacy systems are still widespread and used across many industries such as government, banking, manufacturing and healthcare and they weren't built to manage the use cases of today's digital business.

The reality is that legacy systems are becoming a growing challenge, with many issues arising when it comes to integrating them to the new IT infrastructure. Most of the time, legacy systems are seen as holding back growth, consuming a disproportionate share of IT budgets and exposing the enterprise to cyberattacks.

At the same time, new data privacy regulations like GDPR, CCPA and HIPAA are hard to be integrated within old legacy systems, leaving businesses exposed to financial and reputational risks from non-compliance. But it's getting to the point where older technologies are holding back businesses in the face of the growing competition, who are more agile and don't necessarily require the resources to support those technologies.

Therefore, the potential risks of relying on outdated technologies to perform critical tasks should not be overlooked. A successful modernisation strategy should always take into consideration the priorities and risks associated with it, to ultimately allow the organisation to understand how to mitigate them and what will put them in a much better place.

There are too many opportunities for businesses to mine their data for insights, reduce costs and reap competitive advantage, but organisations must move beyond their legacy applications first by keeping in mind the next six steps for a successful enablement.

Model process flows and data structures

Modernising a legacy application is like creating one from scratch in that it must be conceptualised and modelled first. A legacy application already has process flows, data structures and interdependencies that need to be untangled and understood so they can be redesigned in the new architecture. As a solution, process modelling tools can help by visualising workflows and connect data inputs/outputs so they can be understood by business and technical users alike.

In addition, data modelling tools dive deeper into the data to help organisations define and categorise their data and establish standards and rules so it can be consumed and used by information systems. Together, these modelling activities provide a

complete picture of the modernised application and its future structure.

Unlock and migrate data

The data stored by legacy applications can be difficult to liberate from those systems. It may be in an inconsistent format with similar data from other systems, or it may be locked into a database version that was not kept updated. When planning an application modernisation initiative, it is important to think about how to migrate the data from the old structure to the new one.

As a result, deploying data replication tools is useful to transform the data during the migration process and keep sources and targets synchronised to prevent business disruptions.

Manage infrastructure and application operations
Once an application is freed from its legacy limitations, it can benefit from agile methodologies such as BizDevOps and DataOps and the continuous integration/continuous development (CI/CD) tools that can accelerate the delivery of business value. Many organisations have already adopted aspects of agile and DevOps for their modern applications but may not be taking full advantage of tools that automate processes around builds, testing and deployment or ensuring that what is delivered meets the needs of the business.

Monitor application and database performance
The drive to modernise legacy applications is often due to the cost of maintaining older hardware, operating systems or programming languages, but it can also be because the application is performing poorly and frustrating users with slow processing and wait times. An important goal of the modernisation is likely to dramatically improve application performance, speed and efficiency. Keeping that application performing optimally can be accomplished through application and database performance monitoring to proactively identify potential issues and assist with their resolution. This can also detect poor query performance and automatically tune queries for optimal execution that will help optimise database workloads and keep unplanned cloud costs down.

Make data governance a modernisation priority
Data governance refers to how data is used in the organisation, by whom and the rules and policies that control access. It allows businesses to assess what is the data that is at risk and what is the nature of that data. While data governance structures are essential for any regulated entity, they are also indispensable for any organisation concerned with data privacy and security.

Data governance frameworks can be difficult to operationalise since they require cultural changes around how data is treated and accessed. However, with the help of automation you can perform data cataloguing, data lineage and data mapping - making it possible to harvest, activate and govern enterprise data.

As a result, deploying data replication tools is useful to transform the data during the migration process and keep sources and targets synchronised to prevent business disruptions

Protect sensitive data

Legacy applications contain a range of sensitive data – not just personally identifiable information, but financial data and other types of data that could damage the business if exposed. During the application modernisation process, it is important to identify that sensitive data and take steps to protect it throughout development, test and production. Organisations can protect sensitive data using techniques like masking, redaction or encryption – no matter where that data resides.

The main goal of legacy application modernisation is that the business and IT both have a better understanding of the data landscape across the enterprise while also ensuring business resilience. It is key for business leaders to set expectations up front in terms of what they are looking to achieve and have a clear strategy and budget aligned for the reality of what it is that they are undertaking. In the end, everybody will be in a much better position to understand what is really going to happen with the other side of that coin and ultimately ensure legacy application modernisation gets the business and IT in agreement, balancing the needs of the business against the ability of IT to deliver on those needs.

TD SYNNEX streamlines backup and disaster recovery

A leading technology distributor and IT solution aggregator, TD SYNNEX has an in-house team of system administrators that understands the critical importance of backup and disaster recovery (DR). To provide data protection and ensure high availability for large company databases, the team implemented Quantum DXi® series backup appliances. Quantum deduplication, replication, and encryption capabilities have helped TD SYNNEX achieve consistent backup performance, cost-effective scalability, and enhanced security for business-critical data.

The system administration team at TD SYNNEX manages the large internal databases that contain vital product information, price lists, inventories, and sales records for the company. To keep the business running smoothly, this team must ensure that this business-critical data is well protected and that databases are continuously available.

The team has developed multi-layered plan for data protection and database availability. Administrators back up databases locally to appliances and then replicate that data to geographically dispersed data centers. If there is a problem with a database, users can rapidly retrieve data from a backup or access replicated data from a different data center. The backup and DR strategy works well. But it requires robust, reliable backup appliances that can ingest and transfer large, growing volumes of data.

Facing performance challenges from backup appliances

For several years, TD SYNNEX relied on Quantum products for backing up databases. As a Quantum distributor, the company had a strong relationship with Quantum and was very familiar with Quantum solutions. “We started using Quantum DXi-series backup appliances more than 12 years ago, and we were very happy with the features and performance,” says Jason Shen, senior director of system administration at TD SYNNEX. “But when it was time to retire those appliances, we made a change to a product from a different vendor.” At first, the new product delivered comparable performance to the Quantum systems. But Shen’s team found that performance degraded as the company backed up more files. “Processing more files required more and more CPU power – which meant that we needed

to add nodes," says Shen. "We wanted the ability to scale without having to purchase more servers." Shen's team decided to conduct an in-depth proof of concept, comparing the Quantum DXi6700, DXi6900, and DXi9100 appliances with the existing systems from the other vendor. The results were clear. "Our proof of concept showed that Quantum DXi appliances were more stable than our other systems," says Shen. "We could continue to write more data into the DXi appliances and still experience consistent performance."

Returning to Quantum DXi for Backup and DR
The TD SYNNEX team began replacing the other systems with new Quantum DXi9100 backup appliances. Each system can support from 204 TB to 2 PB of capacity and deliver up to 63 TB/hour of performance. The company now uses multiple DXi9100 appliances to back up data locally and then replicate that data across data centers in California, South Carolina, and Ontario. With the Quantum remote replication capabilities, replication is completely automatic. "The Quantum replication capability was a key reason why we selected the DXi-series appliances," says Shen.

Maintaining strong data protection with full daily backups and replication

The Quantum variable-length deduplication algorithm used by DXi appliances enables TD SYNNEX to back up less data and transfer less data across the network than with other appliances. As a result, the company can complete full backups and replication frequently – and that means better data protection.

"We need to back up approximately 8 TB of data," says Shen. "Quantum deduplication allows us to back up all of that data and transfer it offsite daily. Without Quantum deduplication, there's no way we could transfer that much data every day."

Simplifying Backup Processes with Quantum
By switching back to Quantum DXiseries appliances for backup, the TD SYNNEX team can use simpler processes. "With the systems we're replacing, we had to change our backup process to write to four distinct nodes," says Shen. "The Quantum platform

enables us to use just one IP address. We can back up data without complex networking."

Safeguarding data with built-in encryption

Backing up and replicating data are critical for avoiding data loss and ensuring business continuity. But TD SYNNEX takes additional steps to safeguard data from security threats. With Quantum DXi appliances, Shen's team can take advantage of self-encrypting drives (SEDs), which provide hardware-based data-at-rest encryption for all data. Even if a drive is physically removed from a DXi appliance, data cannot be read using another device or system.

Gaining cost-effective scalability

Replacing the existing systems with Quantum appliances enabled TD SYNNEX to avoid the costs of purchasing more servers. "When we compared Quantum DXi systems with the other systems, Quantum definitely had a lower cost per TB," says Shen. Looking ahead, Shen and his team know they can continue to protect databases and ensure business continuity even as those databases grow. "We no longer have to consider costly upgrades to maintain our existing backup schedules," says Shen. "With Quantum, we can scale our databases – and our business – while staying as efficient as possible."

The Quantum variable-length deduplication algorithm used by DXi appliances enables TD SYNNEX to back up less data and transfer less data across the network than with other appliances. As a result, the company can complete full backups and replication frequently – and that means better data protection

Should the power we seek come from within?

Onsite Power Generation, is it the end of the road for diesel generators -and if so what should be your plan (B) Be?

BY JASON KOFFLER, FOUNDER & MANAGING DIRECTOR, CRITICAL POWER SUPPLIES

DIESEL GENERATORS have played a key role in data centres up to now but is their cost now prohibitive not only in terms of fuel but also emissions? Can the power from within show the way forward?Certainly, peak demand can be offset by the new types of energy solutions coming on line.

When we start to think about powering from within, we have several choices, whether it's peak shaving with onsite energy storage, combined energy storage or energy optimisation.

Our new energy solutions should be thought of as before the meter solutions and after the meter solutions. in terms of everyday data centres we are really looking at solutions behind the meter. Applications could be focused on peak Shaving and Self-consumption optimisation. The questions we need to be looking at, are we looking for minor changes to our power use or step changes in how we use power on site? Therefore, how we integrate power creation and storage into our onsite applications.
If we were to start to factor in the government's EPC ratings for 2027 and 2030 and then look at how fines may be charged for sites, energy storage is a great answer for making our building more energy efficient and improving existing EPC RATINGS.

From 1 April 2027, the minimum required rating would rise to 'C', so landlords must have improved the building by then or have registered a valid exemption. If the building possessed a 'C' rating as of April 2025, the landlord would be compliant with the regulations.

In the second compliance window, from 2028 to 2030, a landlord would have to present a valid EPC by 1 April 2028 and from 1 April 2030, the minimum rating would rise to 'B'. If the building possessed a 'B' rating as of April 2028, the landlord would comply.

It's worthwhile considering that

Peak shaving:
Charge your batteries whenever electricity rates are low or with renewable energy and discharge to avoid paying peak prices during the most expensive times of the day.

Bristol airport is currently investigating how they can provide Electric car owners with free airport parking in return for the right to charge and discharge their car during its stay in the airport car park.

Self-consumption:
Reduce your energy bill through self-consumption. Combined with renewable energy sources this also significantly reduces your carbon footprint.

Concluding points
How to release the power instead of consuming it.

- Power monitoring and measurement.
- Identifying underutilised or idle servers.
- Deploy environmental sensors to your racks.
- Implement remote power control.
- Optimise airflow management in server cabinets.
- Remote working and the shift to the cloud.
- Release the power on-site with onsite energy creation and storage.

So, whether its Peak Shaving or Self Consumption you have the power.
www.criticalpowersupplies.co.uk

Battery technology: The backbone of modern data centres

Data is central to our modern lives, whether that is in business or personally. As a result, the reliance we put on the data centres that contain this data is increasing rapidly.

BY THOMAS VERGHESE, TECHNICAL MANAGER AT ENERSYS

AS WE BECOME more concerned about energy usage, it is important to note that data centres use around 1-1.5% of global energy[1] – and this figure will inevitably rise even though efficiency improvements mean that energy consumption is rising at a slower rate than data generation. However, managing electricity consumption is a key issue for data centre operators, to meet international guidelines and comply with their social responsibility.

Changes in Data Centres

In the face of this growth, it comes as no surprise that the structure of data centres is changing, and this is equally applicable to the Uninterruptible Power Supplies (UPS) that they rely on to address power outages. Until recently, UPS batteries were sized to give typically 10 to 15 minutes of autonomy thereby allowing enough time for generators to be brought online, or an orderly shut-down performed. However, as modern generators can be remotely or automatically operated this time has reduced to less than 5 minutes in many cases, therefore requiring less battery capacity.

Another trend that seeks to reduce energy consumption is running data centres at elevated ambient temperatures, which reduces the need for air conditioning. To achieve this, all equipment (including the servers and UPS batteries) must be capable of being reliable in these conditions.

Battery Technology

Battery technology has progressed significantly in recent years, although lead-acid remains a popular technology in data centre UPS systems. In the early days, traditional flooded lead-acid batteries were used. While effective, their operation meant over time maintenance with the topping up with water was required and due to the rate of gas emissions, high ventilation requirements were needed.

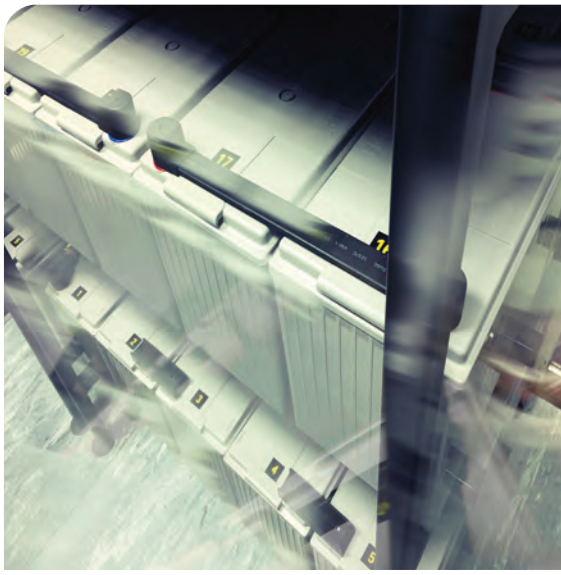
The next generation was valve-regulated lead-acid (VRLA) that immobilized the electrolyte in a gel or absorbent glass mat (AGM). This approach significantly reduced the water loss resulting in no topping up being required and a significant reduction in the ventilation requirements, thereby improving operating costs. In fact, AGM-based VRLA batteries have become very common in data centres in recent years.

AGM VRLA technology has further advanced with the advent of Thin Plate Pure Lead (TPPL) technology, which adds several significant benefits. Here, thinner grids of very high purity are utilized to form the plates, resulting in a greater contact area between the plate and the active material/electrolyte.

Benefits of TPPL Technology

As the plates in TPPL batteries are thinner, more can be stacked in the same volume. This not only boosts power density; it also ensures that TPPL batteries are faster to charge and can deal with larger current peaks.

The higher density reduces the space occupied by batteries by around 20%,



freeing up additional space for servers, thereby increasing revenue for the data centre operators.

Batteries are a significant part of data centre expenditure and all batteries have a finite life expectancy.

TPPL-based batteries have been demonstrated to have a lifespan of 8-10 years which represents a 25% increase over VRLA-type batteries. Furthermore, TPPL batteries are suited to the higher temperatures found in data centres that have reduced their air conditioning capacity to reduce energy usage. However, there is some degradation of service life due to the elevated temperatures so data centre operators should consider the best trade-off between reduced energy costs and more frequent battery replacement.

Another feature of TPPL technology is its low self-discharge characteristics that mean they can be stored for longer than traditional lead acid battery types.

Typically, a TPPL battery can be stored at 20?C for up to 2 years without needing a refresh charge.

As they exhibit high charge acceptance when compared to other lead-acid technologies (AGM, VRLA or flooded), TPPL batteries can be recharged quickly, and they are ready to respond again within a very short period. This means they can deal with situations where multiple outages could occur.

Summary

The pace of change in data centres continues to increase, fuelled by the increasing amounts of data our society is generating as well as the thirst for ever more frequent access to this data. The recent pandemic will have exacerbated this situation due to increased remote working.

Coupling this with greater instability in mains power, due to a variety of factors including increased demand and it is more important than ever before that data centre operators have access to reliable, high-performance battery technologies to support their UPS. TPPL batteries represent the latest generation of lead-acid batteries that have been used in backup applications for decades and this exciting new technology delivers many benefits that help data centre operators meet their demanding challenges.

For more information about data centre UPS batteries, please visit enersys.com

[1] Digitalization and Energy Report, International Energy Agency, November 2018.

Hillstone and the DCA

With a long history of load bank Design, Rental and UK Manufacture, Hillstone have been uniquely placed within the data centre testing industry for the past 14 years.

BY PAUL SMETHURST, MD HILLSTONE LOADBANKS

OUR ORIGINS go back over 30 years with load banks for testing batteries in the North Sea oil & gas and UK power station battery systems. These founding engineering principals have led the evolution of our data centre commissioning across the world.

From the initial rack load bank designs for BT and original heatload IST testing for Telecity in London and the BBC at Media City in Manchester, our product development and investment helped pioneered data centre commissioning, testing and UTI certifications.

Having been a member of The DCA - Data Centre Alliance since 2015, the opportunity to be part of the special interest group for a best practice guide on data centre commissioning, was a natural fit from our load bank perspective.

The responsibility of the contributors representing this Trade Association, are focused to ensure the audience benefits from the best practice guide of how to utilise design and build data points that can become part of and enhance existing metrics used in the running data centre operations. (The IEEE reference 10 relative metrics just on energy).

This has formulated the guide to consider the wider perspective from the 'design and build' process and the journey across to the operational requirements on the client side.

A key area of the guide is to include and explain the benefits of utilising 'ongoing calibration check points' for the benefit of tracking the day-to-day requirements of auditing, compliance reporting and environmental demands on today's data centres.

From the initial stage of design and build the guides focus is commissioning and is explained from the commonly used and adopted principals of 'The 5 stages of data centre commissioning from ASHRAE'. These are broken down under the sections of:

1 – Factory Acceptance Testing
2 - Component Verification
3 - Component Installation,
4 – Site Acceptance Testing
5 - Integrated System Testing

Within each of these sections the guide highlights the benefits of robust commissioning and how to utilise the obtained data from vendors and where the commissioning process needs to be benchmarked for value of datum points that will be used with ongoing calibration during the operation of the data centre.

The Data centre Alliance Special Interest Group Best Practice Guide on data centre commissioning will benefit all stakeholders when making decisions relating to operating a variable IT digital load.

https://www.hillstone.co.uk

Talent won't just come knocking – Launch of the rising star programme

When it comes to the talent shortage, the data centre industry needs to transition from talking to acting. However, there is something preventing the industry from doing so and I can't seem to put my finger on it.

BY ADELLE DESOUZA – DCA ADVISORY BOARD AND FOUNDER HIREHIGHER

We like being a well-kept secret?
I QUESTION whether we actually like being a 'well-kept secret' at an exclusive 'invite only' party or is it the fact that the 'old boys network' helps to keep our jobs safe? The cost of living is real, and we must help those who seek to get on the ladder.

I've read that in mature data centre markets, such as North America and Western Europe, much of the existing workforce is aging and many professionals expect to retire around the same time, leaving data centres with a shortfall on both headcount and experience. Our small pool of talent keeps salaries high for those of us who made the right choice all those years ago.

Maybe it's the role of the HR teams?
Does it just come down to the people and talent team – is it their remit? What will happen when you need to recruit in your own team? Many employers are simply not drafting a job description with realistic expectations, whether it's multiple years of experience required for entry-level roles, or at times arbitrary inclusions i.e., 'Degree preferred'.

We must amend our expectations when it comes to recruitment. A recent Uptime Institute report on the global data centre market, stated: 'The most successful employers in the sector take multiple steps to attract and retain top talent, including revisiting advertised job requirements, implementing training and mentoring programmes and ensuring adequate diversity efforts. I am not saying that these two suggestions are the reasons why we have failed to make progress in this space, I am merely highlighting what it could be.

Final thoughts – maybe it's just very difficult to know what to do when the problem is so widespread and multi-layered. Much like disillusioned voters wondering what difference their vote will make, it is easy to see how industry players could feel the same. Having one scheme in one company doesn't address our issue and while plausible for some to have schemes with teams and coordinators, this is not the case for all. With these issues in mind, I'd like to introduce you all to **The Rising Star Programme (RSP),** created by HireHigher and supported by The DCA. This initiative is dedicated to addressing the skills problems faced by the industry - attraction, acquisition and retention of talent. The programmes initiatives acknowledge the feedback from not only data centre professionals, but millennials and Gen-Z both from within and outside of the industry.

The Rising Star Programme recognises that change is on the horizon. The responsibility for attracting skills does not lie with one organisation, the programme requires pledged support from organisations across the industry who want to drive change and who accept action must be taken.

Find out more about **The Rising Star Programme here**

The design & build process of data centres

Currently, achieving a buildable Stage 5 design for a data centre is a convoluted process .

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

THIS IS DICTATED more by a demand to shift perceived contractual Risk than it is to conduct the most efficient and cost-effective development of the initial client brief. Consequently, the benefits of true collaboration utilising BIM modelling are compromised or even removed all together. The client appoints a team of consultants, engineer and architects to produce a Stage 2 then Stage 3 design. But they want to retain that team to oversee the later design development by the contracting team.

So, they then either send the Stage 3 design out to the marketplace to obtain bids from contractors or they proceed to pay their design team to develop the project to Stage 4 and then go out to the marketplace. The bidding and bid-review process will involve the raising

and resolution of various Queries and RFIs that are often relevant to the overall tender costs.

Once awarded, with either a greater or lesser quantity of outstanding queries to be resolved, the Contractor then appoints his design team who have to re-validate and repeat a fair amount of what the client's designers have already done, to satisfy their own corporate QA procedures and their Insurers in producing their own Stage 4 then Stage 5 designs. That takes time and incurs additional design fees solely to allow the contractor's designers to own the design liability.

Because the design process involves the selection of a number of criteria that have a range of acceptable values, the comparison of original design loads and duties with those resulting from the contractor's design validation is often difficult. Workshops are often required to compare base design criteria to understand the root cause of any differences.

There is still, even at this advanced stage, the risk that some fundamental question or an accumulation of lesser issues will delay the completion of the contractor's design and require resolution by referral to the original client design team. As such, both programme and costs are still not fully confirmed.

Another issue created by this protracted process is that the client's designers, wanting to incorporate a measure of flexibility for the client's requirements and because they are not expert in the detailed installation techniques, are not able to hone certain aspects of the design to minimise costs such as pipe and duct sizing.

Likewise, the design progresses to a fairly advanced stage using major equipment whose actual cost has not been benchmarked in the current market.

There seems to be a general opinion that the process described above is the best way of retaining access to a competitive contractor marketplace and thereby keeping costs down... However, in reality, this creates several significant risks.

Commercial:

- Additional design fees are incurred.
- The base client design is optimised for early-stage flexibility, not lowest build cost.
- Suppliers and manufacturers are not confirmed until the contractor's design is substantially complete.
- In the fast-changing market of current times, PQS consultants budget and costplan advice is often out of date by the time the Stage 4 design is sufficiently advanced to allow the procurement of major equipment and therefore both the contractor and client are at risk of having inadequate allowances.

Timeline:

- Additional time is required to address the contractor design team queries and to allow the contractor's designers to repeat certain elements of the design process.
- Completion of the contractor's design will affect procurement and manufacturing of equipment.
- Later completion of the contractor's design means a later date for the full confirmation of builders work openings, fire-stopping requirements, support steelwork, leave-down walls, craneage etc.

Technical:

- Late proposals by the contractor to utilise alternative manufacturers or to 'streamline' distribution systems, even if done to identify Value Engineering at the client's request, risks introducing errors in performance and material compliance.
- Acoustic modelling and CFD modelling have to be validated on the contractor's design and are therefore available later, when the resolution of any issues identified has the least amount of time available.
- The very fact that the client's design team's output is primarily to allow contractor pricing and not intended to be used to build to, introduces the risk that a level of detailed design is not undertaken until the contractor's design is underway.

In the current market, engaging contractors at the earliest opportunity significantly reduces most of the above risks and if anything, also secures firmer and more favourable pricing at a much earlier date.
https://www.michaellonsdale.com/

The NDCA project

We have some really serious challenges in the Data Centre sector, on one hand we have the growth of digital services, everything is going online, and not to forget that only half the world has access to the internet, and on the other energy security problems, and the net zero goals.

BY JOHN BOOTH, MD, NDCA

WE HAVE AN AGING WORKFORCE and as we do not have a recognised career path within the sector, in fact almost every event I've been to about this topic, has resulted in a simple fact, that most of the people "fell into" the industry. Most of them came from other sectors be they IT, HVAC or ex-military personnel.

Luckily, the UTI has recently published a career map and our goal now is to attract graduates to start in the industry, but there is still quite a major problem.

Other sectors have formal training facilities, which provide theoretical and PRACTICAL training, and all people working in that industry have to be formally accredited, think electrician, plumbers, gas fitters etc, they have to be "card carrying" to do their job, in our sector we do not do that, and we should.

The NDCA's (National Data Centre Academy's) sole role is to create a world-class purpose-built data centre training facility which will offer space where traditional classroom training can be delivered as well as providing practical DC space where that theory can really be put to the test. The facility can be utilised by not only existing training companies but also DC providers and suppliers.

The potential for this practical training facility is endless, for example it will also be used as a semi-permanent exhibition space or showroom, enabling vendors to showcase their own equipment, as an innovation, research incubator hub

or as an internal staff training resource to gain practical hands-on or VR experience without the fear of causing any damage.

With the stakes so high, most businesses simply can't afford to let staff on to the shop floor without both adequate training and practical hands-on experience, so it's no surprise that interest in this facility is so high. Let's face it you would not trust your life to a pilot who had only read an instruction manual to fly a 747 without practical experience; the NDCA offers the data centre sector with the equivalent flight simulator which airlines and the Air Traffic Control Authority trust to make sure their own staff are fit for purpose. As a visitors' centre, school pupils have the opportunity to experience what a data centre is all about and discover the mission critical role it plays in their increasingly digital world. What better way to capture the imagination of the next generation of data centre experts than to give them a peek inside what could very likely be their future career.

There is no limit to what can be achieved and by working together as we have all the tools at our fingertips to shape the data centre workforce of the future. The NDCA has recently submitted a funding request (Nov 22) to the West Midlands Combined Authority – Innovation Accelerator with its partners, DCA, Digital Birmingham, Birmingham City University and Connectium Ltd and if successful we will be opening in Q2/3 2023.

Please visit the linked in page, NDCA website or contact info@nationaldatacentre.academy for more information.

Managing energy market volatility

Highly volatile energy markets justifiably dominate the headlines and should be an area of great concern and focus for data centres.

BY BOBBY COLLINSON,MD, NOVEUS ENERGY

WHILE THE UK government's business energy support will shield some against volatile prices there is still much uncertainty beyond April 2023 when the scheme ends.

In response, Noveus Energy's Managing Director, Bobby Collinson, will be discussing how to manage market volatility utilising a dynamic approach at The DCA's latest 10x10 event in London. While here you can get a quick overview of what Bobby means by taking a dynamic approach – one that brings together risk management and energy purchasing, and proactively incorporates renewables into your strategy.

Dynamic risk management and purchasing

In my experience, data centres are looking for a clearly defined strategy and approach that delivers a competitive price and cost certainty that meets their tenants' requirements. This can be achieved with a dynamic risk management and energy purchasing strategy, which data centres are well placed to implement, and in my opinion, should be adopted as best practice.

With the current energy market fluctuations, at Noveus Energy we monitor markets daily, advising our customers when to buy and sell, including how to deal with all too often price spikes and when to switch buying tactics to take advantage of market volatility.

Described above is what we call a dynamic approach – one that delivers a lower commodity cost by maximising the benefit of market volatility and limiting the risk of buying on the wrong day when prices are artificially high.

It requires an in-depth understanding of the market, daily analysis, and ongoing adjustments to deliver a lower price than the average market, with decisions constantly reviewed.

In normal market conditions and with a dynamic approach, you can save up to 10% on energy procurement. However, you could achieve considerably more savings in the current highly volatile environment, but you must be fleet of foot – daily, weekly – as the market is changing rapidly all the time.

Renewables integral to your strategy

Across the energy market I witness many consultants adopting a static approach for their clients, where the risk and purchasing strategy is set at the beginning of a contract and is rarely – if ever – reviewed or adjusted throughout. With this approach, renewables are often viewed as a separate issue and unaligned to the energy risk management strategy. However, it is my view that renewables should be an integral part of the risk management strategy and power purchasing agreements (PPAs) and onsite renewables must be considered as a mechanism to hedge market risks and create a more balanced energy strategy for your business.

There are many PPA options available to you, including virtual, hybrid, corporate/sleeved, time-of-use and private wire arrangements, as well as the option to have renewable energy sources directly onsite – and with current market prices these offer good value at the present time.

Now is also a time when data centre tenants will be insisting on renewable power, and when reducing emissions and achieving net-zero targets are central challenges. But be aware that the renewables market is extremely fast moving, and both the cost and availability will come under pressure in the next 12-24 months.

If you would like to informally discuss any of the above, please get in touch with Bobby Collinson at Noveus Energy.

MANAGED SERVICES SUMMIT EUROPE

managedservicessummit.com/europe

13 JUNE 2023

MANAGED SERVICES SUMMIT LONDON

managedservicessummit.com

13 SEPTEMBER 2023

MANAGED SERVICES SUMMIT NORTH

managedservicessummit.com/north

NOVEMBER 2023

CREATING VALUE with MANAGED SERVICES

managedservicessummit.com

@MSSEvent