Storage:
Flexibility is the future

DW talks to Moshe Yanai, Founder of 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

CELEBRATING 11 YEARS OF SUCCESS

Announcing the 11th edition of the premier IT awards: The Storage, Digitalisation + Cloud Awards 2020.

In what has been, and continues to be, extraordinary times for the business world, it seems doubly important to recognise the projects, innovations and individuals which have made such a huge difference during 2020. Almost overnight, employees switched from office working to working from home, and the new, or next, normal, means that, into the future, what might be called a 'hybrid work' model looks set to evolve, with flexible working very much the order of the day. What was already becoming a trend as part of many organisations' digital transformation programmes, has been accelerated.

The SDC Awards 2020 will celebrate the achievements of end users and the IT community as they have innovated like never before to ensure business continuity in these challenging times. This year more than any other, please do make sure that you enter our SDC Awards. There's no limit to the number of entries, all of which are free of charge, and we'll be promoting all the short-listed entries via Digitalisation World's multi-media platform over the coming months, ahead of the awards ceremony. We really do want to celebrate and recognise the many amazing achievements which have come about in response to the coronavirus.

SDC AWARDS 2020

www.sdcawards.com

WHY ENTER?

MAXIMISE VISIBILITY
Free PR opportunities with 5 months of marketing utilising the Digitalisation World portfolio.

POSITIONING
Position your product or service as an innovator in your field.

INCREASED CREDIBILITY
An award win, shortlisting or nomination acts as a 3rd party endorsement.

NETWORKING
Over 300 industry leaders attend the gala awards evening.

COMPETITIVE ADVANTAGE
Gain an advantage on your competitors.

NOMINATION IS FREE OF CHARGE AND VOTING IS DONE BY THE READERSHIP OF THE DIGITALISATION WORLD STABLE OF PUBLICATIONS.

Editor's View

By Phil Alsop

Only connect

PEOPLE, PROCESS, PRODUCT. A simple mantra, but one which is rather too frequently ignored or misunderstood.

The current pandemic has forced individuals and businesses alike to re-evaluate many, if not all, aspects of day to day life. Much has been written about the increase in the pace of digital transformation, and plenty about how we have all (hopefully!) gained a better understanding of the things that really matter to us, as opposed to the nice to haves.

From a business perspective, not only have virtually all companies had to make rapid changes to the way in which they interact with both their employees and their customers, but they've also had to gain a better understanding of the equal importance of what might be called the essential business trinity: people, process, product.

Product is the relatively easy bit. After all, there are technology solutions out there which, in the main, offer far more possibilities than are required right now. So, whether it's introducing AI into your business, or leveraging the same AI as part of a customer facing product or solution, by and large you are spoilt for choice.

The process and the people present far more of a challenge. The processes are critical as the catalyst between people and product – whether for your employees or your customers. The processes govern how you deliver product/technology. Get these wrong, and you'll build up resentment. Get these right, and you'll achieve major buy in.

As for the people, well, if you don't understand how they function – what they want, where, when and how, then you'll be facing a constant battle. Your employees will not work efficiently, let alone with the skills and enthusiasm required to differentiate your organisation from others; and your customers will fail to engage with your brand.

The reality is that, unless you recognise the equal importance of the three 'disciplines', you'll struggle to run a successful business. After all, you might have the greatest technology deployed in your business, but if your employees are not able to understand how it works and/or are afraid for their own jobs, they are unlikely to embrace it. And this will impact on everything else down the line.

Equally, if you have the right people and processes in place, but don't offer your customers the products and services for which they are looking, then you might struggle to make that many sales.

Understanding the anxieties and expectations of your employees and your customers is a good place to start when it comes to ensuring that your business model is going to work well for all of your stakeholders. Once you have a good understanding of these, it should be possible to put the right processes in place, inside and outside of your organisation. And the right combination of properly skilled and enabled employees, and the right processes, should go a long way to ensuring that customer expectations are met, if not exceeded.

Contents

OCTOBER / NOVEMBER 2020

18 COVER STORY

Storage – flexibility is the future

Notwithstanding the challenges of current sales environments, Infinidat's revenues in 2020 are breaking records.

DW talks to Moshe Yanai, Founder of Infinidat

10

21

24

28

42

48

09

Survey assesses pandemic's impact on work, with an eye to the future

SERVICENOW has released The Work Survey, one of the most comprehensive global surveys to date on COVID-19's impact on work and the opportunities ahead for a wave of digital innovation in how people work and businesses operate.

Executives and employees across Europe agree technology enabled them to pivot to new ways working faster than thought possible, and digital transformation will accelerate innovation. "The world's dramatic pivot to working digitally is showing everyone what the future of work looks like," said ServiceNow CEO Bill McDermott.

"Digital workflows are the way business gets done in the 21st century. There's no going back. Digital transformation will accelerate. New ways of working will become the norm. We are on the cusp of an unprecedented wave of workflow and workplace innovation."

Fielded in September by Wakefield Research on behalf of ServiceNow, The Work Survey engaged 9,000 executives and employees across industries including financial services, health care, telecommunications, manufacturing, and the public sector.

Key European findings include:
- 92% of executives (both globally and in Europe) say the pandemic made their company rethink how they work. In Europe, 83% of employees (compared with 87% globally) say their company has created better ways of working since the crisis began.
- 92% of executives and 86% of employees say their company

transitioned to new ways of working faster than they thought possible.
- COVID-19 has reduced operating expenses for 90% of European businesses surveyed (88% globally), creating opportunities for investments in digital transformation, research and development, marketing and growth.

Almost half of executives (47%) and over half of employees (55%) in Europe think transitioning to the new normal will be even more challenging than the initial shock of COVID-19. This challenge is exacerbated because most businesses are at a digital disadvantage, with 94% of European executives admitting they still have offline workflows, including document approvals, security incident reports, and technology support requests. Progress has been made, but months into working from home, 61% of executives and 62% of employees across Europe say their companies still do not have a fully integrated system to manage digital workflows.

New systems that were developed, and put in place on the fly, as a result of COVID-19, were seen to have created new and better ways of working by 83% of employees across Europe. However, such systems are felt to still be vulnerable to the next major disruption, with most executives and employees stating that key business functions (such as Customer Service, HR and Finance) would not be able to adapt within 30 days in the event of another disruption. This showcases the need, and opportunity, for robust digital transformation across the enterprise.

While 100% European executives and employees (94%) overwhelmingly tout the benefits of remote working, the challenges are becoming more apparent. Both executives (93%) and employees (78%) across Europe express real concerns about how remote work will impact the business moving forward. The biggest concerns and benefits with continued remote work depends on where you sit.
- Throughout Europe, executives are

most worried about outputs – delays in product or service delivery (54%), while their employees are most concerned about the inputs – reduced collaboration between business units (47%).
- Employees across Europe say that time saved from not commuting or travelling to a workplace (61%) has benefited them most, while executives believe that better use of technology to improve efficiency (50%) is the greatest benefit to their teams.

Over half of employees (52%) in Europe believe their company will prioritize business continuity over workplace safety. More surprising is the fact that 37% of executives actually believe this as well. Even if a company makes an effort to put safety first, many employees don't think they can pull it off, with 43% of European employees saying they do not believe their company will take the necessary steps to ensure their safety. Surprisingly, executives agree. Nearly a third of European executives (32%) admit they don't think their company will take the appropriate steps for safety.

"COVID-19 caused businesses across Europe to change at a pace, the like of which we have never seen before and, if honest, many didn't think was even possible" says Chris Pope, ServiceNow's VP Innovation.

Commenting on the findings, applied futurist and author, Tom Cheesewright, said: "This research comes at an opportune moment as companies begin the transition from the early chaos of the COVID-19 response to the creation of new sustainable approaches.

Some incredible things were achieved under extreme pressure and core hybrid working technologies have been proven. But much work remains. Layers of culture, process and behaviour need to be designed and overlaid on the technological foundations together with a new social contract agreed between employer and employee that embraces distributed working."

Digital transformation budgets increase
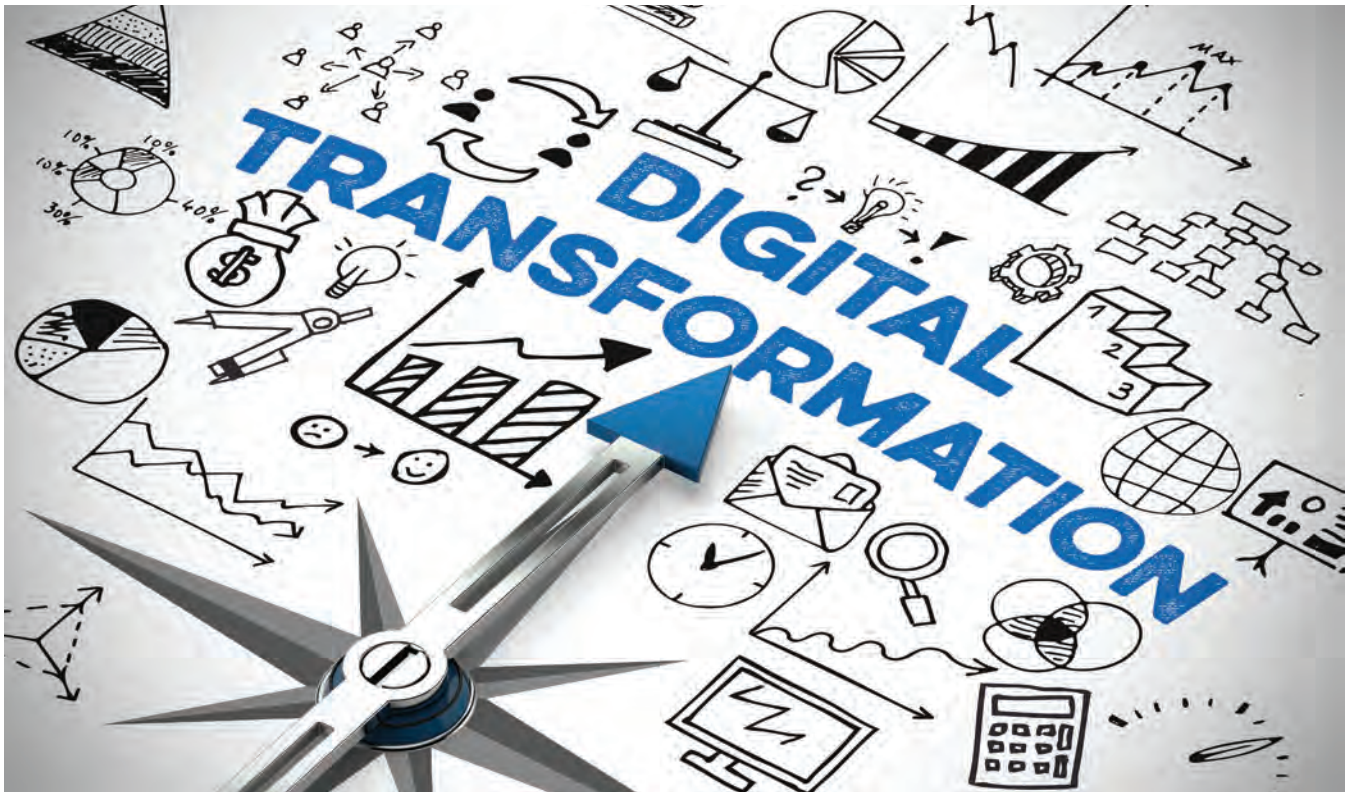
TATA CONSULTANCY SERVICES has published the findings of its global survey titled, "Digital Readiness and COVID-19: Assessing the Impact," revealing that 90% of organizations are maintaining or increasing their digital transformation budgets amid the pandemic.

The global survey engaged almost 300 senior business leaders from large enterprises – 97% with revenue above $1 billion and 44% above $10 billion – spanning 11 industries across North America, Europe and Asia. Six digital capabilities were identified as critical factors in companies withstanding the pandemic:
- End-to-end digital customer experience (CX)
- AI-based analytics to continually improve the CX
- Core enterprise systems in the cloud
- Highly automated core business processes
- Digital sensors tracking products
- Key partnerships in digital ecosystems

The analysis compared organizations that had more advanced digital capabilities in place prior to COVID, referred to as "leaders," with those that had fewer, if any, in place, known as "followers." The study showed that fewer leaders (64%) have seen their revenue decline, compared to followers (73%). Moreover, leaders had better business visibility and a more confident outlook, with 74% of them expecting revenues to bounce back within two years, compared to 54% of followers.

"Before the pandemic, companies' digital capabilities were rapidly becoming central to their success and business transformation initiatives. However, our study revealed how several enterprises were not as far along in developing a digital backbone as they hoped,"said Rajashree R, Chief Marketing Officer, TCS. "Companies that had embraced digital transformation more whole-heartedly performed better during the pandemic and expect a faster rebound, whereas others are now focused on making necessary investments and racing to catch up."

Digital Readiness and COVID-19: Assessing the Impact – Key Findings
·While 68% of companies have seen revenue declines amid COVID-19, 90% of organizations have either maintained or increased their digital transformation budget. ·Among shifts in technology spends due to the pandemic, companies reported maximum increases on: collaborative technologies (65%), cybersecurity (56%), cloud-native technologies (51%) and advanced analytics (39%).

·Prior to the pandemic, the average organization surveyed had only 9% of its workforce working mostly from home. That percentage has increased seven-fold and is expected to remain elevated through 2025, when the average company projects 40% of its employees will work largely from home.

·Business initiatives around an end-to-end CX have seen most traction, already deployed at 25% of companies and under development at 44%. Similarly, the use of analytics and AI to improve CX is deployed at 24% and under development at 39% of companies.

·Higher levels of automation in core business processes is another priority area, already deployed at 23% of companies and under development at 44% of companies.

Europe achieves world enterprise data 'superpower' status

EUROPE is the world's enterprise data superpower according to new research from Digital Realty. Europe is the world's enterprise data superpower, outpacing North America, according to new research released by Digital Realty.

The research comes as the world readies itself for growth brought about by the fourth industrial revolution, or Industry 4.0. According to recent research from McKinsey and the World Economic Forum, Industry 4.0 has the potential to create USD 3.7 trillion in value by 2025.

As digital transformation accelerates, Europe's place as one of the world's primary centres of enterprise data puts it in a strong position to capitalise on this growth.

The Data Gravity Index DGx™ – which measures the creation, aggregation and private exchange of enterprise data across 21 metros – reveals that regions with strong global connectivity and an abundance of data-led industries, such as a thriving technology scene or prominent financial services sector, create so much enterprise data that they produce a 'Data Gravity' effect, exponentially attracting more data to the region.

Europe's pre-eminence in a wide range of knowledge economy industries, such as financial services and complex manufacturing, that create vast amounts of enterprise data, combined with the emergence of data-led industries in Europe, has turned the region into a global 'enterprise data superpower'.

According to the research, the volume of enterprise data being created, aggregated and exchanged among European cities is the largest in the world; even larger than North America. Europe is expected to extend its lead as the world's enterprise data superpower even further in 2024.

London is currently the world's

most powerful centre for enterprise data, with a Data Gravity score of 167.05, outpacing both New York (79.61) and Tokyo (80.32) – largely driven by its prominent and highly connected financial services industry. The average Data Gravity score across all cities is 22.64 and 48.45 across Europe. Four other European cities also currently rank in the top centres of enterprise data: Amsterdam, Dublin, Frankfurt and Paris.

However, it's not only the abundance of enterprise data that's putting European cities in the lead, but the flow of that data between them. According to the Data Gravity Index DGx™, Europe is home to several of the world's most interconnected city pairings, no doubt helped by the regulatory ease of doing business with one another, as well as the cities' thriving financial centres.

These include London and Amsterdam (1st overall), Paris and London (2nd overall), Frankfurt and Paris (5th overall),

London and Frankfurt (6th overall), as well as Dublin and London (10th overall).

Despite the vast benefits of having a thriving data economy with strong, open data exchanges with other cities, being in a city with a strong Data Gravity effect is a mixed blessing for businesses.

Many businesses are accruing increasing amounts of enterprise data in a bid to transform their businesses through digital transformation, but are overwhelmed by volume, weighing down digital transformation efforts in enabling them.

By 2024, as a whole Forbes Global 2000 Enterprises will have accrued enough data to need access to quantum computing to effectively handle it. They will need an additional 8.96 exaFLOPS of compute power and 15,635 exabytes of private data storage annually to effectively manage their enterprise data.

Comparatively, the next quantum computer at Oak Ridge National labs will run at just 1.5 exaFLOPS by 2021.

These unmanageable volumes of enterprise data and the gravity they create are already resulting in issues for businesses beyond IT, including:

- **Limited innovation**
- **Poor customer and employee experiences**
- **Increased costs**
- **Compliance issues**
- **Security**

The Data Gravity megatrend is the summation of several growing forces in businesses, many of which have accelerated in recent months as COVID-19 has driven more business around the world online:

- **Enterprise data stewardship**
- **Mergers and acquisitions**
- **Digital-enabled interactions**
- **Data localisation**
- **Cyber – physical**

Organisations ensure that new accelerated approaches don't run out of steam

CAPGEMINI report finds that some organizations have made significant strides to streamline processes to supercharge scaling innovation efforts by nearly two years, but others still fail to scale.

In a disrupted, fast-changing world, businesses are betting big on innovation and many are locked in a race to harness new technologies. Yet struggling to achieve scale is hampering the ability of organizations to fully leverage the huge potential of emerging technologies and to respond effectively to business disruptions and opportunities. This is according to a new report from the Capgemini Research Institute, "Scaling Innovation – What's the Big Idea?" which explores why most innovations fail to scale.

Almost $300 billion was invested in nearly 32,000 venture capital deals worldwide in 2019.[1] Innovators across the globe filed 3.3 million patent applications in 2018, up 5% from the previous year and a continuation of nine straight years of increases.[2] And within the COVID-19 context, the pandemic has catalyzed the need for innovation and renewal, with 68% of executives saying that they have accelerated existing transformation initiatives.[3] Yet the ability to scale innovation remains in its infancy, with many organizations failing to reap the rewards of big innovation bets.

The impact and value of innovation is only fully realized through scaling and adoption not from ideation or experimentation. Companies that scale and adopt innovation create the desired business impact, achieve accelerated business performance, and gain sustained competitive advantage.
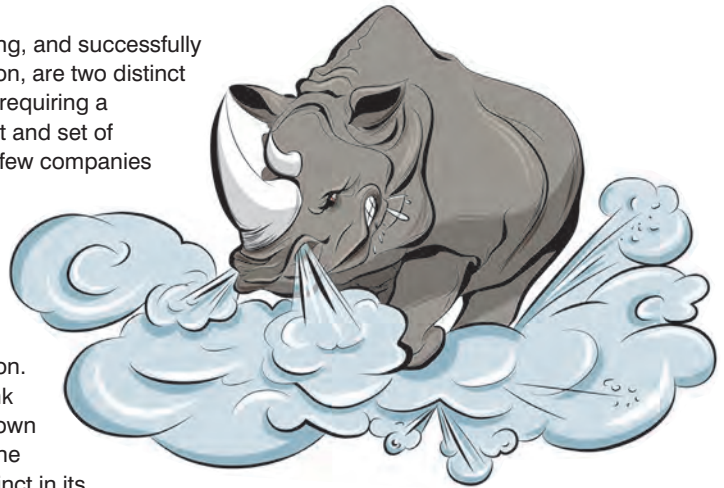
Capgemini's report is developed from the insights of 40 senior executives from global organizations with combined revenues of over $1.7 trillion, as well as academics, and draws on key learnings, best practices, and experiences to deliver actionable recommendations. Large organizations must treat generating and scaling innovation as separate entities Innovating, and successfully scaling innovation, are two distinct functions, often requiring a different mindset and set of skills. However, few companies differentiate between the front-end of generating innovation and the back end of scaling innovation. They do not think of scaling in its own right – a discipline that is quite distinct in its purpose, requirements, and challenges. Although scaling occurs downstream in the innovation journey, it's often a case of too little, too late.

According to the report, often, innovation generation focuses on what is desirable - high-impact, "blue sky" concepts and projects designed to solve an unmet or unstated customer need. It rarely focuses on the two aspects that are more relevant for a large-scale business – viability and feasibility. By treating scaling innovation as a separate discipline, organizations can ensure that they bring in teams or individuals that are more focused on the viability and feasibility of innovation right from the start of the ideation phase. Build momentum exacted by the COVID-19 catalyst.

COVID-19 has expedited innovation across a range of sectors. It has forced companies to take a fresh look at how they approach innovation at scale. Organizations need to ensure that new accelerated approaches don't lose steam.

By continuing to model operations to a sense of urgency, organizations can apply the learnings from the pandemic period for the long term. In these times of crisis, Capgemini has found that organizations have made significant strides to tackle bureaucracy, streamline processes, restructure workforces, and empower front-line leaders. As a result, some companies have been able to supercharge efforts by nearly two years when it comes to scaling innovations.

Companies should now build on this momentum to understand how they can overcome some of the traditional governance challenges that stand in the way of scale, such as bringing your best talent to focus on the issue or overcoming bureaucratic hurdles or organizational silos.

Not every idea can be scaled long-term An innovation culture is important not only for ideating and testing new ideas but also for successfully scaling them within existing or new markets. Capgemini found some of the key components of an innovation culture that supports scale include the promotion of a "learning" culture that accepts failure and the willingness to stop initiatives, even if they initially enjoyed success at scale. Not every idea can be scaled long-term and it's critical that businesses understand when to accept failure at different stages of the innovation journey. Organizational culture is the toughest hurdle to scale innovation; the ability to remove barriers and address problems needs to cascade down from the C-suite across the whole organization.

The report found that, among those organizations who have demonstrated true success with achieving scale, there is a willingness to end the experimentations and innovations that they may love, to make room to scale and try new things.

Worldwide data centre infrastructure spending to grow 6% in 2021

End-user spending on global data center infrastructure is projected to reach $200 billion in 2021, an increase of 6% from 2020, according to the latest forecast from Gartner, Inc. Despite a 10.3% decline in data center spending in 2020 due to restricted cash flow during the pandemic, the data center market is still expected to grow year-over-year through 2024.

"THE PRIORITY for most companies in 2020 is keeping the lights on, so data center growth is generally being pushed back until the market enters the recovery period," said Naveen Mishra, senior research director at Gartner. "Gartner expects larger enterprise data centers sites to hit pause temporarily and then resume expansion plans later this year or early next. However, hyperscalers will continue with their global expansion plans due to continued investments in public cloud."

Lockdowns from COVID-19 will prevent more than 60% of planned new facilities construction in 2020, which is why data center infrastructure revenue will decline 10.3% in 2020 (See Table 1). End-user spending is expected to grow in the single digits starting in 2021.

"Much of the reduced demand in 2020 is expected to return in 2021 when staff can physically be onsite," said Mr. Mishra. "For now, all data center infrastructure segments will be subject to cost containment measures and enterprise buyers are expected to extend life cycles of installed equipment."

Three actions to recover data center infrastructure Opportunities

With slow improvement in economic growth, data center infrastructure general managers should seek to prioritize a select set of existing and new customers. Specifically, Gartner recommends:

1. Training the organization's sales force to engage with the chief financial officer (CFO) and chief procurement officer on a set of cost optimization initiatives such as renegotiating IT contracts, optimizing cloud costs, and consolidating IT.

Worldwide Data Center Infrastructure End-User Spending (Billions of U.S. Dollars)			
	2019	**2020**	**2021**
End-User Spending ($B)	210	188	200
Growth (%)	0.7	-10.3	6.2

Source: Gartner (October 2020)

2. Crafting an industry playbook that helps technology providers understand COVID-19's impact on a range of different industries to then recommend short- to midterm action items for the given providers by each industry.

3. Investing in a new go-to-market model for digital natives to drive innovation. Build momentum around hybrid IT and consumption-based pricing to improve mind share with digital natives.

RPA software revenue to reach nearly $2 billion

Global robotic process automation (RPA) software revenue is projected to reach $1.89 billion in 2021, an increase of 19.5% from 2020, according to the latest forecast from Gartner, Inc. Despite economic pressures caused by the COVID-19 pandemic, the RPA market is still expected to grow at double-digit rates through 2024.

"The key driver for RPA projects is their ability to improve process quality, speed and productivity, each of which is increasingly important as organizations try to meet the demands of cost reduction during COVID-19," said Fabrizio Biscotti, research vice president at Gartner. "Enterprises can quickly make headway on their digital optimization initiatives by investing in RPA software, and the trend isn't going away anytime soon."

Worldwide RPA software revenue is expected to reach $1.58 billion in 2020, an increase of 11.9% from 2019 (see Table 1). Through 2020, average RPA prices are expected to decrease 10% to 15%, with annual 5% to 10% decreases expected in 2021 and 2022, creating strong downward pricing pressure.

COVID-19 increased enterprise interest in RPA

The pandemic and ensuing recession increased interest in RPA for many enterprises. Gartner predicts that 90% of large organizations globally will have adopted RPA in some form by 2022 as they look to digitally empower critical business processes through resilience and scalability, while recalibrating human labor and manual effort.

"Gartner anticipates RPA demand to grow and service providers to more consistently push RPA solutions to their clients because of the impact of COVID-19," said Cathy Tornbohm, distinguished research vice president at Gartner. "The decreased dependency on a human workforce for routine, digital processes will be more attractive to end users not only for cost reduction benefits, but also for insuring their business against future impacts like this pandemic."

Organizations are expected to grow their RPA Capacity

Through 2024, large organizations will triple the capacity of their existing RPA portfolios. The majority of "new" spend will come from large organizations that are purchasing new add-on capacity from their original vendor or partners within the ecosystem. "As organizations grow, they will need to add licenses to run RPA software on additional servers and add additional cores to handle the load," said Mr. Biscotti.

"This trend is a natural reflection of the increasing demands being placed on an organization's 'everywhere' infrastructure."

Future RPA clients will come from non-IT buyers

Adoption of RPA will increase as awareness of RPA grows among business users. In fact, by 2024, Gartner predicts nearly half of all new RPA clients will come from business buyers who are outside the IT organization.

"Leading RPA software vendors have successfully targeted chief financial officers (CFOs) and chief operating officers (COOs), instead of IT alone. They like the quick deployment of low-code/no-code automation. The challenge they have is integrating RPA successfully across heterogeneous, changing environments, which is where IT coordination can make the difference," said Mr. Biscotti.

Worldwide RPA Software Revenue (Millions of U.S. Dollars)			
	2019	**2020**	**2021**
Revenue ($M)	1,411.1	1,579.5	1,888.1
Growth (%)	62.93	11.94	19.53

Source: Gartner (October 2020)

IDC looks to the future

International Data Corporation has announced its IT outlook for 2021 along with top trends and guidance for enterprises as they prepare for The Next Normal.

RECENT IDC data shows that actual market performance has been stronger than suggested by survey and market indicators, especially in the U.S., due largely to cloud and remote work support. Service provider investments to meet demand for cloud and digital services are stable compared to other sectors and remote work/learning has driven stronger PC volume and a greater focus on security for the year. "Overall information and communications technology (ICT) spending is expected to have a 5% compound annual growth rate (CAGR) through 2024.

In terms of total IT spending, we are seeing a more shallow V-shaped drop this year. Total IT spending will drop to about 1% growth this year, but this is far stronger than the 3% decline that was expected earlier in the year," said IDC President Crawford Del Prete.

In a recent IDC survey, 42% of technology decision makers indicated that their organizations plan to invest in technology to close the digital transformation gap. "The pandemic created a business necessity for increasing technology investment and accelerating digital transformation timetables," said Meredith Whalen, Chief Research Officer at IDC. "What we are learning is that many of these initiatives that started as ways to mitigate the economic impact of COVID-19 have become permanent roadmap requirements for Future Enterprise success in the digital economy." IDC's outlook for the Future Enterprise identifies three overarching initiatives that directly link technology investment to digital transformation efforts – creating digital parity across the workforce, designing for new customer demands, and accelerating automation initiatives.

Worldwide Cloud IT Infrastructure Top 5 Vendors, 2019Q2 vs 2020Q2 (shares based on vendor revenue)

Source: IDC 2020
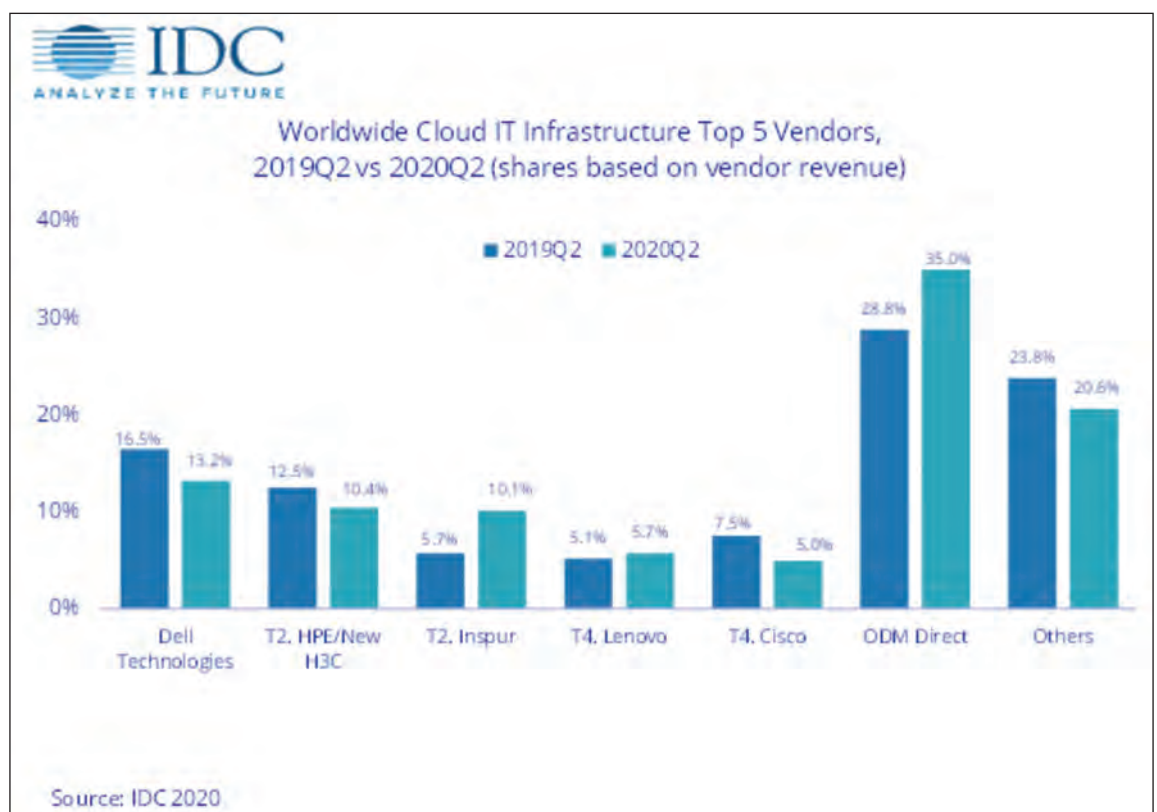
Top 5 EMEA Vendor Revenues ($M)						
Brand	1Q20 Server Revenue	2Q20 Server Revenue	1Q20 Market Share %	2Q20 Market Share %	1Q20/2Q20 Revenue Growth%	1Q20 Server Revenue
HPE	$847.8	$1,024.1	23	26	21	$847.8
Dell EM	$897.8	$777.4	25	20	-13	$897.8
ODM Direct	$544.8	$571.8	15	14	5	$544.8
Lenov	$303.0	$407.4	8	10	34	$303.0
IBM	$216.1	$387.0	6	10	79	$216.1
Others	$828.2	$784.8	23	20	-5	$828.2
Total	$3,637.7	$3,952.5	100	100	9%	$3,637.7

Source: IDC Quarterly Server Tracker, 1Q19

Creating Digital Parity

Before the pandemic, organizations, on average, had only 14% of their employees working from home. That percentage has increased dramatically – to 45% – and many organizations anticipate that work-from-home employees will remain a large proportion of the workforce going forward. Supporting hybrid workforces and ensuring that remote and work-from-home employees have the same sets of connectivity and productivity tools as their in-office counterparts will be essential to long-term success.

* Prediction: By 2023, 75% of the G2000 will commit to providing technical parity to a workforce that is hybrid by design rather than by circumstance, enabling them to work together separately and in real-time.
* Prediction: By 2022, an additional $2 billion will be spent on desktop and workspace as a service by the G2000, as 75% of them incorporate employees' home network/workspace as part of the extended enterprise environment.

Designing for New Customer Demands

Almost half (47.6%) of all U.S. consumers are "very concerned" about their personal health as it relates to the COVID-19 virus, according to IDC's recent U.S. consumer survey. This concern for safety has spurred many businesses to create new contactless consumer experiences, including curbside pickup. Enterprises will also invest in design and user interface requirements for contactless process automation with an emphasis on voice-based experiences and self-service options through mobile apps.
○ **Prediction:** By 2023, 75% of grocery ecommerce orders will be picked up curbside or in store, driving a 35% increase in investment in onsite or nearby micro-fulfillment centers.
○ **Prediction:** In 2021, 40% of development activities will reprioritize design and user interface to support contactless process automation.

Accelerating Automation Initiatives

Enterprises will increasingly adopt automated IT operations practices to support the greater scale required for digitally driven enterprises. Robotic process automation (RPA), robotics, and artificial intelligence (AI) technologies will play a more important role in labor automation while a continued focus on autonomous operations will drive investment in Digital Engineering organizations and digital operations technologies.
○ **Prediction:** By 2022, 45% of repetitive work tasks will be automated and/or augmented by using "digital co-workers," powered by AI, robotics, and RPA.
○ **Prediction:** By 2023, 75% of Global 2000 IT organizations will adopt automated operations practices to transform their IT workforce to support unprecedented scale.

COVID-19's Impact on Industries

The COVID-19 pandemic has created unique situations for specific industries, including healthcare, hospitality, retail, and small and medium businesses (SMBs), requiring them to rethink the way they use technology to engage with customers.
○ **Healthcare:** Telemedicine will be a permanent fixture going forward. With nearly a third of consumers interested in having a telemedicine option post-pandemic, healthcare providers are predicted to increase spending by 70% on connected health technologies by 2023.
○ **Hospitality:** Despite being an industry known for people-based services, 85% of hospitality brands will implement self-service technologies by 2021, changing how they engage with guests.
○ **Restaurants:** Restaurants have taken the economic brunt of the pandemic and many have turned to home delivery out of necessity. Post-pandemic, 30% of restaurants using third party delivery platforms will deploy native delivery options to eliminate third-party fees, increasing profit by 25%.
○ **Retail:** Contactless payments have seen increased adoption during the pandemic and will be viewed as a customer experience imperative going forward, causing 85% of retailers to offer at least two contactless payment options by 2023.

SMBs: At least 30% of SMBs will fail by 2021 leading to a new wave of microbusiness-powered and ecosystem-first disruptors by 2023. These microbusinesses will be single employees that leverage the power of a digital platform to obtain and fulfill work.

Edge Computing spend to reach $250 billion in 2024

The concept of edge computing most often refers to intermediating infrastructure and critical services between core datacenters and intelligent end points. Proliferating enterprise and consumer devices benefit from a digitally transformed technology world through edge capabilities. However edge is defined, the compute, storage, and networking cornerstones gird data creation, analysis, and management outside of the core. A future is unfolding where extraordinary value and opportunity for essential products and services from a myriad of technology ecosystem stakeholders is being created. According to the new Worldwide Edge Spending Guide from International Data Corporation (IDC), the worldwide edge computing market will reach $250.6 billion in 2024 with a compound annual growth rate (CAGR) of 12.5% over the 2019–2024 forecast period.

"Edge products and services are powering the next wave of digital transformation," said Dave McCarthy, research director, Edge Strategies at IDC. "With the ability to place infrastructure and applications close to where data is generated and consumed, organizations of all types are looking to edge technology as a method of improving business agility and creating new customer experiences."

The stable of companies that are present and investing in edge computing continues to grow and increasingly includes a diverse set of competitors. Familiar companies in the hyperscaler space include Amazon Web Services (AWS), Equinix, Google, IBM, Microsoft, Oracle, and Switch among others. Physical infrastructure providers include companies such as AMD, Dell Technologies, Ericsson, HPE, and Intel. Meanwhile, services companies like AT&T, Lumen, and Verizon deliver critical networking capabilities to connect the thousands of planned and deployed edge datacenters.

IDC expects edge expenditures will be concentrated in the U.S. and Western Europe over the next several years. In 2020, the global regional spending shares for the Americas, EMEA, and Asia/Pacific will be 45.0%, 27.9%, and 27.2%, respectively. From an industry perspective, 11 of the 19 standard industry segments will deliver 5% or more of total worldwide spending in 2020. The top two industries for edge spending throughout the forecast are discrete manufacturing and professional services, while retail will overtake process manufacturing to become the third largest industry by the end of the forecast. Professional services will also see the fastest growth in edge spending with a five-year CAGR of 15.4%.

From a technology perspective, services (including professional and provisioned services) will account for

Top Companies, Worldwide Cloud IT Infrastructure Vendor Revenue, Market Share, and Year-Over-Year Growth, Q2 2020 *(Revenues are in Millions)*

	2Q20 Revenue (US$M)	2Q20 Market Share %	2Q19 Revenue (US$M)	2Q19 Market Share %	2Q19/2Q19 Revenue Growth
1. Dell Technologies	$2,506	13.2	$2,330	16.5	7.5
T2. HPE/New H3C Group* **	$1,981	10.4	$1,770	12.5	12.0
T2. Inspur/Inspur Power Systems* **	$1,917	10.1	$812	5.7	136.0
T4. Lenovo*	$1,087	5.7	$728	5.1	49.3
T4. Cisco*	$941	5.0	$1,066	7.5	-11.7
ODM Direct	$6,656	35.0	$4,069	28.8	63.6
Others	$3,925	20.6	$3,371	23.8	16.4
Total	**$19,013**	**100.0**	**$14,147**	**100.0**	**34.4**

IDC's Quarterly Cloud IT Infrastructure Tracker, Q2 2020

Notes:
* IDC declares a statistical tie in the worldwide cloud IT infrastructure market when there is a difference of one percent or less in the vendor revenue shares among two or more vendors.
** Due to the existing joint venture between HPE and the New H3C Group, IDC reports external market share on a global level for HPE as "HPE/New H3C Group" starting from Q2 2016 and going forward.
*** Due to the existing joint venture between IBM and Inspur, IDC reports external market share on a global level for Inspur and Inspur Power Systems as "Inspur/Inspur Power Systems" starting from 3Q 2018.

46.2% of all edge spending in 2024. Hardware follows as the second largest technology category with a 32.2% share of spending, while the remaining 21.6% will go to edge-related software.

"While no technology market has been spared from the economic impact of COVID-19, edge market suppliers are poised to experience sustained growth throughout the forecast from enterprise and service provider investments," said Marcus Torchia, research director with IDC's Customer Insights & Analysis group.

EMEA server spend decreases

International Data Corporation's (IDC) EMEA Server Tracker shows that in 2Q20 the EMEA server market reported a year-on-year (YoY) decrease in vendor revenues of 5.8% to $3.9 billion and a YoY decrease of 6.9% in units shipped to around 470,000. The top 5 vendors in EMEA and their revenues for the quarter are displayed in the table below.

When viewing the EMEA market by product detail, the impact of COVID-19 can clearly be seen, as the SMB market has both seen a slowdown in run rate business and faster adoption of cloud platforms. Tower shipments in 2Q20 decreased 32.5% QoQ, while custom shipments targeted toward cloud platforms grew 8.9% QoQ. Lenovo continued to penetrate the hyperscale market and saw significant growth in 2Q20.

Standard rack-optimized shipments increased 0.8% QoQ in units, though revenues grew 5.1% YoY. "This strong growth in ASPs is a result of both a shift toward higher socket counts and richer configuration component configurations as the market grapples with digital transformation to ensure business continues in these trying times," said Eckhardt Fischer, senior research analyst in the European Infrastructure group.

"ODM shipments are back to pre-COVID levels worldwide and ODM manufacturing facilities are reporting 24 x 7 activity to close the gap in production caused by anti-COVID measures earlier this year and meet COVID-related demand for cloud-deployed digital services," said Kamil Gregor, senior research analyst in the European Infrastructure group. "In the short term, it seems that a 1Q20 drop in consumption has been overcome, but we still need to wait for the longer-term impact of the economic slowdown on infrastructure vendors and buyers and consumers of digital services."

Regional Highlights

Looking at the Western European x86 server market, the U.K. performed well, growing 11.8% YoY in revenue, driven by hyperscale datacenter investments. The same trend was seen in the Netherlands and Ireland in 2Q20. With around $660 million in revenue, Germany maintained its position as the region's largest market.

> While no technology market has been spared from the economic impact of COVID-19, edge market suppliers are poised to experience sustained growth throughout the forecast from enterprise and service provider investments

"Central and Eastern Europe, the Middle East, and Africa [CEMA] server revenue continued its downward trajectory in 2Q20, declining 5.9% year over year to $791.31 million," said Jiri Helebrand, research manager, IDC CEMA. "Reduced business activity due to COVID-19 was the main reason for weak sales, although there are strong differences in performance across the region. The Central and Eastern Europe [CEE] subregion grew 6.9% year over year with revenue of $424.83 million. Ukraine, Czech Republic, and Russia recorded the strongest growth.

Cloud platforms, online services, and strengthening infrastructure to support working from home helped drive sales. The Middle East and Africa [MEA] subregion declined 17.3% year over year to $366.48 million in 2Q as some IT projects were put on hold and nationwide lockdowns and a reduction in cargo flights in some parts of the African region had a negative impact. Israel and Bahrain were the only countries in MEA to record growth."

Public Cloud IT infrastructure spend overtakes traditional IT

According to the International Data Corporation (IDC) Worldwide Quarterly Cloud IT Infrastructure Tracker, vendor revenue from sales of IT infrastructure products (server, enterprise storage, and Ethernet switch) for cloud environments, including public and private cloud, increased 34.4% year over year in the second quarter of 2020 (2Q20). Investments in traditional, non-cloud, IT infrastructure declined 8.7% year over year in 2Q20.

These growth rates show the market response to major adjustments in business, educational, and societal activities caused by the COVID-19 pandemic and the role IT infrastructure plays in these adjustments. Across the world, there were massive shifts to online tools in all aspects of human life, including collaboration, virtual business events, entertainment, shopping, telemedicine, and education. Cloud environments, and particularly public cloud, were a key enabler of this shift. Spending on public

Worldwide Cloud IT Infrastructure Market Forecast by Deployment Type, 2018- 2024 (shares based on Value)

Source: IDC 2020
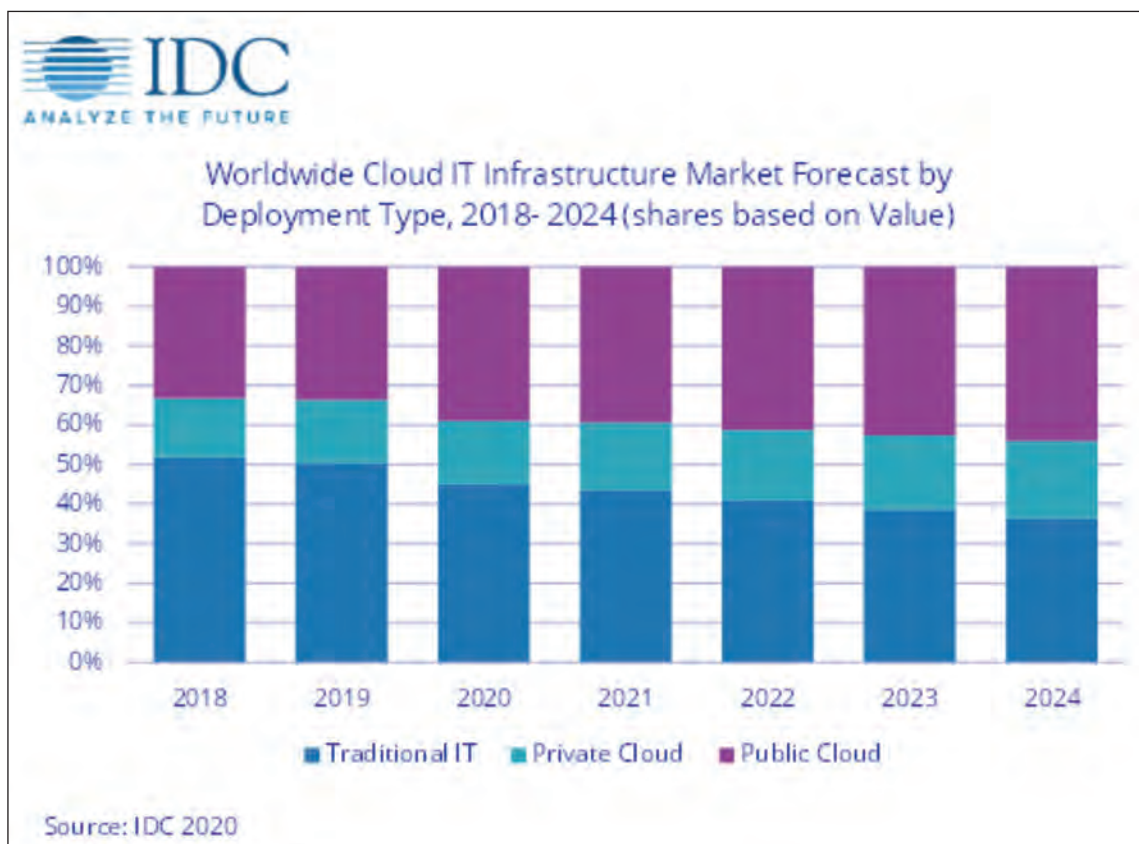
cloud IT infrastructure increased 47.8% year over year in 2Q20, reaching $14.1 billion and exceeding the level of spend on non-cloud IT infrastructure for the first time. Spending on private cloud infrastructure increased 7% year over year in 2Q20 to $5 billion with on-premises private clouds accounting for 64.1% of this amount.

IDC believes the hardware infrastructure market has reached the tipping point and cloud environments will continue to account for an increasingly higher share of overall spending. While IDC increased its forecast for both cloud and non-cloud IT spending for the full year 2020, investments in cloud IT infrastructure are still expected to exceed spending on non-cloud infrastructure, 54.8% to 45.2%. Most of the increase in spending will be driven by public cloud IT infrastructure, which is expected to slow in 2H20 but increase by 16% year over year to $52.4 billion for the full year. Spending on private cloud infrastructure will also experience softness in the second half of the year and will reach $21.5 billion for the full year, an increase of just 0.3% year over year.

As of 2019, the dominance of cloud IT environments over non-cloud already existed for compute platforms and Ethernet switches while the majority of newly shipped storage platforms were still residing in non-cloud environments. Starting in 2020, with increased investments from public cloud providers on storage platforms, this shift will remain persistent across all three technology domains. Within cloud deployment

environments in 2020, compute platforms will remain the largest segment (50.9%) of spending at $37.7 billion while storage platforms will be the fastest growing segment with spending increasing 21.2% to $27.8 billion, and the Ethernet switch segment will grow 3.9% year over year to $8.5 billion.

Spending on cloud IT infrastructure increased across all regions in 2Q20 with the two largest regions, China and the U.S., delivering the highest annual growth rates at 60.5% and 36.9% respectively. In all regions except Central & Eastern Europe and the Middle East & Africa, growth in public cloud infrastructure exceeded growth in private cloud IT. At the vendor level, the results were mixed. Inspur more than doubled its revenue from sales to cloud environments, climbing into a tie* for the second position in the vendor rankings while the group of original design manufacturers (ODM Direct) grew 63.6% year over year. Lenovo's revenue exceeded $1 billion, growing at 49.3% year over year.

Long term, IDC expects spending on cloud IT infrastructure to grow at a five-year compound annual growth rate (CAGR) of 10.4%, reaching $109.3 billion in 2024 and accounting for 63.6% of total IT infrastructure spend. Public cloud datacenters will account for 69.4% of this amount, growing at a 10.9% CAGR. Spending on private cloud infrastructure will grow at a CAGR of 9.3%. Spending on non-cloud IT infrastructure will rebound after 2020 but will continue to decline overall with a CAGR of -1.6%.

Storage:
Flexibility is the future

Notwithstanding the challenges of current sales environments, Infinidat's revenues in 2020 are breaking records. DW talks to Moshe Yanai, Founder of Infinidat.

MOSHE YANAI has been active and successful in the storage industry for over 40 years. In 2011, he founded Infinidat, which currently leads the market for petabyte data storage solutions for enterprise organizations. Recently, and at the age of 70, Yanai announced that after nine years he was moving from the position of CEO to developing the company's new generation solutions of storage. In this interview, Yanai discusses his latest professional choice, the current global data storage market and the impact of the global pandemic.

Yanai says: "Despite the continuing devastation of Covid-19 across the business world – Infinidat's sales in the second quarter of 2020 were the highest since the company's establishment. Our team broke revenue records and even beat the investors' forecasts. Like any company, we had to pivot, make changes and business decisions to adapt to this new situation but it became clear to us that our innovative and disruptive data storage technology is exactly what the market demands, during these challenging times.

"We found that our customers stopped spending and re-examined how they utilised IT budgets and for what. In an age where organisations do not know when and how much the budget will change, they keep as much cash in their pockets as they can. On the other hand, they do not want to lose vital business flexibility that helps them survive this crisis and gain crucial competitive advantage. At Infinidat, we know how to provide these two opposites of business flexibility on the one hand and cost savings on the other, with our unique business model and Elastic Pricing.

"This includes the ability to combine CapEx and OpEx consumption models within a single product, as well as the ability to switch OpEx for a more cost-efficient CapEx model. It enables businesses to postpone expenses while gaining agility, making them optimally positioned to weather the current economic storm."

Future gazing

Yanai continues: "Our customers focus on initiatives that create a competitive advantage and improve operational efficiency. With storage being a critical component of the IT stack, and a top line-item in the IT budget, they look to simplify their storage infrastructures. Through moving to pay-as-you-grow models, businesses can capitalize on our performance and availability while improving their own time to market and optimizing their expenses."

On the future for Infinidat and the wider storage market, Yanai concludes: "Our latest round of investment will be used to further develop next generation data storage technologies, which allows us to deliver high availability storage solutions with world-class customer experience that make our customers' business more flexible, efficient and productive. We are thrilled that the enterprise market expresses confidence in us and appreciates the business values we deliver.

"We have customers who have dozens of InfiniBox solutions that they are happy with! Once they experience the technology, they fall in love with its simplicity and put their trust in us to future proof their IT infrastructure strategy."

Expanded global channel partner ecosystem

Recently, Infinidat announced an increase year on year in the number of strategic global channel partners to nearly 400, in 2020. It has resulted in delivering innovative and apt data storage solutions required by businesses worldwide, during challenging times as well as strengthening Infinidat's sales.

The storage, backup and business continuity solutions developed at Infinidat are designed for enterprise customers that engage with partners who add tangible business value and benefits. Infinidat's considered collaborations with new and existing partners instills

> Our latest round of investment will be used to further develop next generation data storage technologies, which allows us to deliver high availability storage solutions with world-class customer experience that make our customers' business more flexible, efficient and productive. We are thrilled that the enterprise market expresses confidence in us and appreciates the business values we deliver.

trust at every level – offering flexible commercial and consumption models alongside best in class technology to reduce the risk, cost, and complexity of our customers most important asset - their data.

In 2020, the way businesses interact has significantly changed. To ensure the channel partner community is effectively supported during Covid-19, Infinidat held over 60 virtual events during the last six months. Despite the pivot to 100% virtual, the company has maintained a 'business as usual' stance with every channel partner.

Mitch Diodato, Channel Sales Director - North America at Infinidat:"Our North American channel partners are fundamental for delivering strategic growth in our key sectors. In addition, many of our new customers are identified initially through our effective partner collaborations, which amplify optimal routes to market. We continue to focus on investing in our partners, their people and empowering their businesses."

Allen Shahdadi, Vice President of Global Sales at Sycomp: "Infinidat treats its partners like family and an extension of its team – both vendor and channel partners win when there is meaningful trust, incentives, and excellent enterprise solutions. The company has made prudent investments in their new virtual partner portal, which has helped our teams drive innovation and best practices to our customers." Mr. Shinichi Kotani, VP of Sales Division, at Marubeni Information Systems Co. Ltd., Japan: "We were impressed with the value of Infinidat's Partner Program and delighted to see the quick uptake for its solutions within the marketplace, particularly in the finance and automotive sectors. Their online training, supplemented with virtual briefings, bring clarity and focus to our teams and consultants."

Roberto Castelli, General Managerat BCLOUD: "Our customers take full advantage of Infinidat's innovative Partner Programs and virtual briefings, as our teams feel empowered to provide the best recommendations and choices, offering the perfect solutions based on the latest technology and in-depth knowledge available. They make us feel like one of their internal sales teams rather than a systems integrator or VAR. BCLOUD's cooperation with Infinidat allows us to offer cutting-edge solutions for our enterprise customers."

New partner portal launched

Infinidat offers the same training and access to content for its internal teams as for partners, with transparent sharing of intelligence and market-leading solutions. Equipping partners with the data to remain front and centre, across new technology and offerings such as Infinidat's 'elastic pricing models,' have made the channel partner portal more accessible than ever.

Hanan Altif, Channel Partner Director- EMEA and APJ at Infinidat: "We nurture close ties and trust with all our partners across EMEA and APJ. For Infinidat's existing business innovations, such as elastic pricing, where the customer receives the full storage capacity immediately but only pays for the capacity they actually use, we have developed additional channel incentives. This has allowed us to give our family of partners the best tools through which they can offer their customers creative solutions that are financially worthwhile - key to success in our current uncertain economies."

Arrow Electronics and Infinidat add UK to strategic agreement

Global technology provider Arrow Electronics and Infinidat have extended their distribution agreement to cover the UK market, strategically supporting enterprises' revenue growth. Based on the agreement, Infinidat will gain broader access to Arrow`s extensive network of channel contacts in the United Kingdom. The distribution agreement previously covered Germany, Iberia, Italy and the Nordics region. Arrow is Infinidat's sole distributor in the US.

"Managing and forecasting data storage growth is one of the key IT challenges companies need to overcome. We aim to create business value for UK businesses with our software-defined data storage solutions. Arrow is a known and trusted adviser in over 90 countries, distributing data storage systems to large organisations," says Lee Bushnell, channel manager, UK&I at Infinidat. "We look forward to the expanded cooperation, having already successfully completed multiple projects across our key European regions."

Infinidat's enterprise data storage portfolio allows enterprises to consolidate legacy storage into a single InfiniBox system or reduce multiple data protection systems to a single InfiniGuard system, decreasing physical footprint, power requirements and administrative burden. With performance that is faster than AFA systems, Infinidat delivers greater application performance with the highest possible reliability. Critically, Infinidat`s flexible consumption models also support optimal IT spend for business transformation and growth.

Mark McHale, vice president of sales of Arrow`s enterprise computing solutions business for UK and Ireland, added, "Infinidat has put together an innovative set of solutions for data storage, data protection, business continuity and sovereign cloud storage. This delivers high-performance, an Always-On methodology and agile data storage solutions to our channel clients and their end customers.

Infinidat`s solutions target the full data lifecycle and open up new opportunities for end users to manage and analyse data. We are looking forward to expanding our offering with their team."

Jumpstarting the hyperautomation journey with intelligent automation

Gartner calls 'hyperautomation' the most important of the top 10 strategic technology trends for 2020. Is it worth the hype? The short answer is, "Yes."

BY TYLER SUSS, PRODUCT MARKETING DIRECTOR AT KOFAX

AS 2020 has unfolded, digital disruption has had many organisations feeling the pressure to innovate to streamline internal operations and customer-facing experiences more quickly. However, as organisations look to drive innovation by transforming business processes, they often run into roadblocks or are uncertain of where to begin.

Hyperautomation may be the solution. Hyperautomation deals with the application of advanced technologies, including artificial intelligence (AI) and machine learning (ML), to increase the scope of automated processes and augment the efforts of the human workforce.

Fast tracking hyperautomation

Hyperautomation requires implementing the right combination of the right technologies, in the right order, at the right time. By adopting an intelligent automation platform, organisations gain the tools they need to jumpstart digital transformation and follow a methodology that catapults them into a state of hyperautomation:

Process discovery: Organisations can use IA to easily analyse patterns and tasks, then quickly identify automation opportunities. Businesses can also discover potential challenges with compliance or regulatory issues and remediate them swiftly.

Digital workflow orchestration: They can centrally build and run automated digital workflows in collaboration with existing applications and human workers. Orchestrating multiple people, actions, software robots, policies and systems enables organisations to analyse, measure and optimise business activities.

Robotic Process Automation (RPA): Businesses can reliably and efficiently automate repetitive, manual tasks across the enterprise, even through web interfaces and business apps.

AI and machine learning: Advanced automation technologies can be leveraged to understand, classify, and extract data including voice, text, chat, and images. AI allows organisations to automatically recognise people and documents, understand the content and context of communications, and make more insightful business decisions. Machine learning improves the accuracy of document identification, classification and separation conducted as part of cognitive capture and RPA.

Digital workforce management: An Intelligent Automation platform provides the capability to govern a growing digital workforce, including software robots that improve security, compliance, scalability, and auditability. Organisations can increase work capacity without adding headcount.

Analytics: Businesses can measure the impact of intelligent automation across the enterprise and calculate ROI. Improved visibility, process intelligence and insight into customers, employees and business partners give executives the tools and information needed to adapt to changing market conditions and customer expectations.

Benefits of hyperautomation

The benefits of hyperautomation are measurable:

Reduced costs: Intelligent automation of business processes and workflows reduces the time and resources needed to complete manual tasks and cuts down on the number of errors.

Scalability: Hyperautomation transforms a manual or complex task into a reliable and repeatable process. A collaborative ecosystem of complementary technologies and humans working together generates exponentially better outcomes across the business.

Personalised customer experience: Hyperautomation enables organisations to deliver a more personalised customer experience, resulting in improved satisfaction, loyalty, and revenue.

Operational excellence: An efficient workforce comprised of the right blend of human and digital workers creates a flexible and agile organisation that can swiftly respond to changing market conditions.

Employee work satisfaction: Human workers enjoy the more thought-provoking and strategic work automation allows them. Workers get more satisfaction out of their jobs when they can see the added value they bring.

Executives who want to drive innovation and transform business processes will do well to consider hyperautomation.

> Businesses can measure the impact of intelligent automation across the enterprise and calculate ROI. Improved visibility, process intelligence and insight into customers, employees and business partners give executives the tools and information needed to adapt to changing market conditions and customer expectations

DW

DIGITAL CHANGE
MANAGEMENT
SUMMIT

**25.11
2020**

www.dcmsummit.com

**How Managed Service Providers and Cloud Service
Providers can help SMEs on the road to digital transformation**
A unique online event to connect MSPs, VARs and System
Integrators with their target market

Weathering the storm

The key barriers to an effective data and analytics strategy.

BY JAMES DON-CAROLIS, MANAGING DIRECTOR, TRUECUE

WHILE MANY INDUSTRIES are focusing on re-opening plans at this critical time of recovery, the past four months are still having a detrimental effect on almost every sector, impacting organisations of all sizes. That being said, ironically, the disruption we have all experienced has also become a defining catalyst for positive change.

In response to evoAlving government legislation and lockdown rules, businesses and public bodies have had to quickly adapt and re-evaluate their standard operational strategies as a priority. According to recent research from Forrester, prior to COVID-19, less than a third of IT processes had been digitised. In a bid to survive the disruption, business leaders are now supercharging their digital transformation strategies, hoping for a return to 'business as usual' as soon as possible.

Although the unprecedented period of uncertainty has made it problematic for businesses to plan ahead, those making insight-driven decisions are far more likely to survive than those making gut-driven decisions. Having a true understanding of business data is essential for any business leader to make accurate forecasts and prepare effectively for an uncertain future. Subsequently, a data-driven approach to business has been brought to the fore. As stated in Gartner's Build a Data-Driven Enterprise, by 2023, data literacy will become an explicit and

necessary driver of business value, supported by its inclusion in over 80% of data and analytics strategies and change management programs.

We recently conducted a survey of 100 data and IT professionals which revealed more than a quarter (27%) of organisations are still reliant on ad-hoc analytics, with over a fifth (21%) reliant on their internal IT teams to drive forward their data and analytics strategy. As only 13% reported having a centralised analytics team in place, it is evident that a large number of organisations did not have a dedicated data and analytics strategy in place prior to COVID-19.

There are a number of fundamental challenges businesses must address if they are to become more data driven. From having the right technologies in place and cultivating a culture of data and analytics that is central to the business strategy, to adopting a business-led approach rather than IT-led approach.

The data function must be business-led, but it is often IT-led

Although the IT department may have an understanding of what makes a strong data strategy, it may not necessarily be aware of what the business needs to be able to understand from analysing its data. In a recent survey from PWC, it reveals that highly data-driven organisations are three times more likely to report improvements in decision making. Therefore, adopting the data function as a business-led approach will ensure organisations have access to more reliable and valuable information which can be used to support a successful digital transformation.

Accessing data from disparate sources instantly

Due to recent uncertainty, daily or even hourly reports and insights are more readily required by business leaders if they are to keep on top of ongoing disruption and make critical business decisions accordingly. Relying on Excel spreadsheets and not having a dedicated data warehouse or a trained analytics team in place can make it very difficult to easily consolidate, validate and structure disparate data sources for analytics consumption so that critical business decisions can be made quickly. This challenge is highlighted more so by key-employee dependencies and a lack of backup capability should certain individuals not be available to perform these critical tasks.

The last few months have demonstrated that analytics maturity can be vital to gaining easy access to critical datasets, while removing any staff dependencies that can be exacerbated with existing remote working practices. Having a clear data strategy in place can help businesses overcome new challenges, especially those related to COVID-19.

According to a recent survey of 300 analytics

professionals, nearly half of the respondents stated that analytics is 'front and centre' in helping inform them on major decisions in response to this critical period of recovery.

Creating and implementing a data strategy that includes designing and building agile, affordable, non-technical data management and business intelligence infrastructure is now easier to achieve. SaaS offerings that bring simplicity to cloud data warehousing provide businesses with instant access to the analytics they need to understand their business and make strategic decisions quickly.

A data and analytics strategy without a data-driven culture

In some cases, businesses have data and analytics strategies in place, but a data and analytics culture is not central to the business strategy. As a result, not all employees have a full understanding of the data technologies and analytics capabilities across the business. In fact, a recent report by Deloitte revealed that the minority (37%) of organisations who had embedded a strong data driven culture were actually twice as likely to exceed their business goals than the majority (63%) who did not have such a strong analytics culture.

Although the main analytics function and strategy should always be the responsibility of qualified professionals, each member of staff should be upskilled, so they have an awareness of the existing data technologies and analytics capabilities across the business. By doing so business leaders can ensure data and analytics isn't simply a by-product of individual Charlotteprocesses, but an essential component, not only for their role but the how it benefits the entire organisation.

Weathering the storm and being prepared for this critical period of recovery

To survive and thrive in the current climate, business leaders must have instant access to all data on historic performance so they are able to consider an array of possibilities and better predict the position they will be in, in months to come. This should in turn also speed up the process of returning to 'business as usual' as quickly as possible.

A data-driven culture and a data and analytics function run by the business is important, but the fundamental element businesses must look to address – particularly with employees working remotely – is having suitable infrastructure in place.

It is important for business leaders to note that a good solution is more than just technology, it is about having access to genuine insight that will allow focus on making the best decisions based on trusted data.
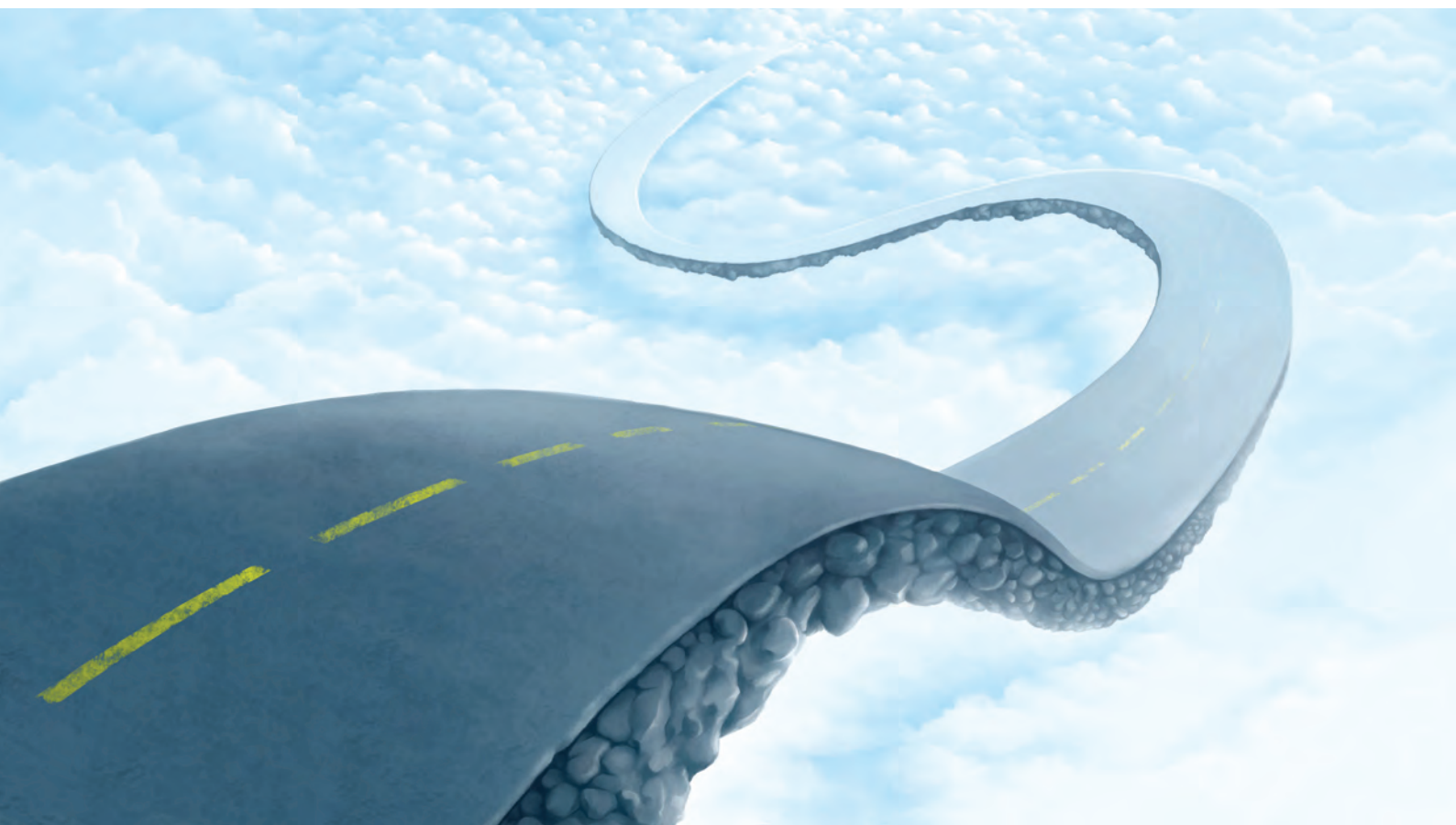
Are we there yet?

The long, hot road trip to the Cloud

BY SCOTT LEATHERMAN, CMO, VIRTANA

"IF I HAVE to pull this car over, there will be trouble!" Does this evoke childhood memories of summer adventures in the family car? It's the same sort of dread we get when the IT budget holder turns around and threatens to pull over on our journey to the cloud, or hybrid cloud. The family summer road trip may be filled with great expectations, but the last thing we want is an unforeseen disruption along the way. And migration to the cloud is no different. To continue this analogy, the bumps on the road to avoid are the ones around cost, performance, and risk. So, here are some thoughts on how to identify the challenges and navigate to your destination smoothly:

The Line of Business needs to pee (they think)

Planning business needs is always a challenge – especially at the speed of change in today's disruptive markets. The unforeseen impact of the COVID-19 pandemic is one example. We hear it a lot in our industry: "We don't know which applications are using the most bandwidth and how much they are costing us." And with 59% of infrastructure managers citing infrastructure cost overruns as their biggest concern, there's definitely room for immediate improvement. Having clarity into your application topology with a clear map to performance is mission-critical for a successful hybrid cloud journey.

Because this is such a dynamic process, it needs to be mapped and measured daily, in real time. But simply automating VMs to workload balance does not give you the clarity needed to understand what and when to move in your hybrid journey. You need the ability to understand why and when things changed so you can effectively plan or resolve the issues.

According to Gartner Research, on average, AWS deployments are 40% over-provisioned to meet unexpected capacity and performance issues – which defeats the purpose of moving to the public cloud. "Know before you go" should be a mantra for every

hybrid journey manager – and parent managing backseat bladder needs.

IT just hit a major pothole and now has a flat tire.

A flat tire only ruins a trip if you don't have a spare, the tools, and the knowledge required to fix it. For most, the actual solution is to call AAA or in this case, get a third-party systems integrator (SI). Calling an SI to help solve an unforeseen problem is not a bad idea, but it does come with a hefty price tag and a level of dependency that doesn't mirror the model of moving to a public cloud. With the right solutions in place, even a pandemic like COVID-19 should not disrupt your business.

That said, it takes time and effort to get there, and no journey worth taking is easy. Having integrated solutions and partners are critical to the hybrid cloud journey. And so is knowing when to fix it yourself and when to call in support to save you millions.

Too much luggage from the DBAs.

Packing the back of the family Ford "Wagon Queen Family Truckster" is a special skill set. It's like playing Tetris with your family's luggage. Right-sizing infrastructure capacity while supporting applications is like making sure all the luggage fits in the car, and that you still have room to move your feet. Sure, you could buy a bigger car to manage the payload, but the expense doesn't justify the performance. You need the clarity to act across your private and public cloud infrastructure in a single solution without disruption is required. That level of optimization is a constant to remaining competitive, enabling you to transform your infrastructure from being seen as a cost of business to being recognized as a revenue generator.

Compliance just gave you a speeding ticket

No matter how well-intentioned and on the right side of the law your compliance team is, it can feel like you are in a police chase. And while you don't mean any harm – the law is the law. In the rush to the cloud, you're not often asked how you will manage the migration, you're simply asked how fast you can move – reminiscent of another epic journey: "We've got a long way to go and a short time to get there."

Regardless of whether you identify with Smokey or the Bandit, you cannot deny that Sheriff Buford T. Justice (AKA Compliance/Security Officer) will slow you down. So, work early and often with your compliance team to ensure that where you store your data, and who has access to your data always remains in compliance.

Leadership just ran out of gas on the migration budget...

… and now they want to know when the cost of running applications is best on-premises vs. across the public clouds?

Cost is all about transparency to the needs of the application infrastructure. Too many enterprises are finding that the rush to the cloud was expensive and not well planned, and are shifting critical apps back to the private infrastructure. But you need to go beyond just resourcing noisy neighbors with VM automation. A long-term solution is to optimize the application performance with an integrated APM and infrastructure solution.

A more immediate and tactical solution is to leverage a hybrid infrastructure platform that works across multiple on-premises vendors, and public cloud vendors to give you the cost analysis you need. PayPal is a good example. The team leveraged an on-premises solution for more than nine years during hyper-growth. While they continually optimized their on-premises infrastructure to expand 300%, the total number of employees managing the infrastructure remained flat. Talk about doing more with less.

Application managers are fighting over the music

On-premises vs. public cloud, VMs vs. containers, AWS vs. Google vs. Azure. Where should those applications be running, and how can they migrate them? These may seem like the most trivial of issues to be concerned about, but devops, architects, and managers have deep loyalties way beyond rational factors like cost, performance, and control.

Having the ability to manage and plan cost across a multi-vendor hybrid infrastructure to maintain your performance SLAs is critical. Don't let blind loyalty or the loudest voice control your path. Your hybrid optimization platform should afford you real-time planning and cloud brokerage to ensure you are optimized for cost and performance.

Your early talent team has been doing the same TikTok dance in the backseat for the past eight hours.

Hearing the same story about why the journey is behind schedule, or the same ask for more budget to meet performance SLAs, or even a repeated request to deviate from the existing roadmap, can wear you down or dilute your focus. It's important to have a multi-department/cross-functional plan and mapped roles, and to measure performance. Keep the entire team (multiple owners of the "cloud" in a large enterprise) engaged and on the same plan to avoid going into a loop of burned resources and nerves.

Are we there yet?

As with most family trips to magical destinations, the road to a successful cloud migration is fraught with unexpected disruptions – but a good plan can avoid most common challenges. So, no matter what stage you might be at in your hybrid cloud journey, we hope you will reach out to us before you feel the need to pull over when the going gets tough.

Look up: Cloud skills are on the rise

In a matter of months, COVID-19 has completely upended decades of tradition and social dynamics of the modern office. As our daily lives turn almost completely to digital interactions digital skills, long growing in importance, are now centre stage as critical to success in the current work environment.

BY NICK TURNER, VP EMEA DRUVA

THOSE THAT CAN competitively leverage emergent digital platforms like the cloud have a more substantial skills advantage than ever before. According to the EU Skills Agenda, "The COVID-19 pandemic has clearly shown that digital skills are not just an asset for career progress. They are essential to work…"

While these trends have long been clear, this generation-defining event presents an unmistakable inflection point that is not lost on employees. Recent research from techUK found that 60 percent of online adults in the UK have since shown interest in developing their digital skills over the next year. Yet many of those who seek upskilling the most face the greatest challenges, with younger workers significantly affected by unemployment and the impact of COVID-19 on our education system.

As employees actively seek to improve their digital competences, and the next generation enters the workforce, how can businesses help guide the development of digital skills for the future? The answer starts with one fundamental truth: post-COVID more than ever, the future is in the cloud.

Skills for the cloud era

Cloud is the industry-defining shift of our generation. It offers frictionless rollout of innovation, democratises cutting-edge technology, and allows for scale unimaginable not long ago. These factors fundamentally change the model of how we consume technology. A model based on demand, where companies can pay for what they need, when they need it and developers can get virtually anything on demand - compute, storage, databases and more.

Yet implementing the cloud is not automatic or something that can simple be accomplished with the flick of a switch. IT requires significant skills in areas like backup, data protection and data management, security provisioning, and more. As businesses pursue

advancement in the cloud, a potential lack of talent presents very real threats to success, and in turn the larger economy. According to the EU Skills Agenda, even the pre-COVID demand for digital experts could not be met. In cyber security alone, there's a skills gap in excess of a quarter of a million workers.

Furthermore, while layoffs stemming from the current pandemic meaning more mobility in the talent pools, those with the most critical skills are the least likely to have been affected – meaning digital talent shortages prior to the pandemic will only be exacerbated as companies compete for an edge in the next normal.

Cultivating skills internally

For companies to have the talent critical to digital success, they must actively cultivate skills internally. The good news is, there has never been a better time to reskill existing workers and upskill young workers. By leveraging the significant variation in existing workload (i.e., employees with less immediate work to do) companies can take advantage of downtime to cultivate talent. According to a recent Gartner study, 79 percent of HR leaders are currently, or are considering, leveraging the fluctuating workloads during the pandemic as an opportunity to upskill employees. As HR leaders look towards these future skills, they are actively navigating a changing

landscape – determining competencies that will be required in order to support a more remote economy reliant on cloud technology. Working with the cloud doesn't just require skills in cloud migration, but in customer service, cybersecurity and DevOps.

With modern SaaS services, many of those skills can now be learned on the job. Employees no longer require in-depth competencies like sophisticated coding. Instead, new talent can lean on higher-level knowledge of aspects central to cloud computing to make them effective at engaging with SaaS providers, shaping and implementing the most relevant solutions in a timely and cost-effective fashion.

As Gartner emphasises, such training must be directly tied to day-to-day work realities: built in as readily-consumed, bite-sized increments. Upskilling must also be tied to coaching and on-the-job experience, the latter of which can account for as much as 70 percent of learning.

By honing talent development to the areas of greatest need and making upskilling tools accessible to those with capacity to learn – companies stand to emerge from the pandemic better prepared to tackle the competitive demands of the cloud era, with a more diverse and capable workforce than ever before.

Enabling digital learning with network visibility

The need to connect remotely has hugely affected all students this year, altering their university experience.

BY ADRIAN ROWLEY, SENIOR DIRECTOR SALES ENGINEERING EMEA AT GIGAMON

THE PANDEMIC'S IMPACT on higher education institutions, and its workforce however, has been equally significant, as they have had to immediately pivot to distance teaching to maintain operations and minimise disruption. A recent study from Universities UK shows most universities are planning to hold in-person classes this autumn, but with the situation continuously changing depending on infection rates, the reality is that institutions will continue to shut their doors unpredictably and face-to-face lessons are set to be regularly interrupted.

While this shifting landscape will present many challenges, it will give some universities the opportunity to reimagine the learning model and embrace innovative new ways to teach. Sure, it's time for higher education institutions to future-proof their networks to remain relevant in the era of digital learning. But holding classes remotely requires resilient and seamless networks, functioning with modern systems and overseen by efficient operations. How can universities successfully enable this shift – particularly with IT budgets shrinking due to student cancellations and drops in enrolments?

A continuing effort

Even before the pandemic, some institutions were already questioning the existing teaching model – the traditional classroom-based learning environment – and considering the modernisation of their practices and minimisation of their dependence on legacy IT systems. As technologic innovation transforms other sectors, universities have been looking to enhance the learning experience to improve cost efficiency, attract digital-natives and stand out from other institutions to encourage high-paying international applicants. At the core of such new developments is, without a doubt, technology. Medical students are able to study the human body through hologram-like projections, computing pupils are benefitting from AI-powered teaching assistants, and language students learning foreign tongues in record times thanks to virtual reality labs in which they converse with AI avatars.

But, it's not all about futuristic technology powering new learning techniques. The focus is also on replacing administrative tools – many of them legacy, on-premise systems – with more effective solutions. While this was a pressing need before COVID-19, the advent of remote learning has made this an absolute priority: universities need IT systems that can support remote access for workers logging in from home or elsewhere, enable digital learning tools for students, and power new business models (such as subscription-based classes) designed with flexibility in mind. These initiatives are critical to maintaining university rankings, student population and revenue, as well as justifying tuition fees in what has inevitably become a very different, virtual educational environment. Needless to say, that using

> Now more than ever, InfoSec teams must ensure constant, unclouded visibility into all network traffic to spot any anomalies before they become a significant problem, prevent blind spots and mitigate risks, thereby helping prevent breaches

more and new technology for distance learning and teaching creates new challenges for a university's infrastructure.

Future-proofing university networks

Regardless of previous innovation projects in higher education, digital learning is now a fundamental service for universities if they want to remain operational and competitive in the current climate. But, what does this mean for university NetOps teams? University networks were already among the most heavily trafficked. Now, with distance learning, these networks will be stretched even further and will have even greater performance and bandwidth requirements. Meanwhile, budget cuts are affecting IT capabilities and impacting future investments. These challenges culminate in less than ideal circumstances in which to accelerate new digital initiatives, such as technology-powered learning. Doing more with less and making the most of existing technology investments is crucial.

The only way to achieve this is through real-time, accurate visibility across the institution's network, which allows teams to understand and optimise performance of existing technologies and applications. Supporting remote access for students and employees requires network resilience. So, NetOps teams must leverage visibility to monitor increasingly complex networks, and spot and eliminate potential bottlenecks that could impact performance, thereby accommodating the exponential growth in traffic volumes.

The security element

Among other challenges, the adoption of distance learning has caused a significant rise in cyberattacks on universities. These incidents must be prevented not only because they may compromise sensitive data relating to students, teachers and other employees', but also because they can disrupt classes. The networks of higher education organisations are traditionally a hacker's heaven, with huge numbers of devices (organisational and user-owned), and complex networks used for studying, working, and researching, as well as personal activities. In fact, only last year there were over 800 breaches flagged in the education sector, double the number of security incidents that took place in 2018. Then, earlier this year, the switch to remote access caused networks to turn inside-out, further expanding attack surfaces, diminishing defences and increasing risks. Both

universities and colleges have endured hackers interrupting remote classes with unwelcome activities. There have also been a number of financially-motivated attacks with hackers targeting educational institutions with ransomware.

In addition, research universities have been victims of state-sponsored attacks, aimed at stealing intellectual property and hindering research. Improving cyber threat detection and response in universities is paramount. Now more than ever, InfoSec teams must ensure constant, unclouded visibility into all network traffic to spot any anomalies before they become a significant problem, prevent blind spots and mitigate risks, thereby helping prevent breaches. In the era of digital learning, this won't be easy as threats could originate from a myriad of devices and locations – that's why visibility must pervade the entire network. Threat detection has to be aided with technology, not just to improve accuracy, but to support overstretched IT teams operating with limited resources.

As the global crisis moves through unpredictable phases, it's likely that higher education teaching will continue to change. While we're unsure what the learning experience will look like in a few months – let alone a year – we know it will never be the same.

This, however, can be a positive for both students and universities themselves. Disruption of normal events can be a catalyst for innovation and can encourage creative thinking and funding aimed at doing things better and, in this case, make education more valuable to more people. Distance learning may just be the beginning of the new tomorrow for education.

Looking to automation to maximise the potential of IoT

Gartner predicted in 2017 that there will be 20 billion connected things online by 2020. Since that prediction, we've seen the adoption of IoT technology meet and surpass the predictor's expectations. The number of companies that will invest in IoT will continue to expand rapidly due to technological advancements producing sensors that are smaller, cheaper and more effective.

BY SIMON SPRING, ACCOUNT DIRECTOR EMEA, AT WHERESCAPE

THE CHALLENGE is no longer in the technology, but in the value organisations can extract from the data they collect. IT teams that are deploying new IoT solutions and need to deliver the value the companies desire from their investment, are struggling with several roadblocks in fulfilling this task.

Extracting value by making insights quickly and easily accessible to the business from data has always been difficult, often like finding a needle in a haystack. Adding more data, data sources, data types and streaming data to the mix can make it close to impossible to get the desired value with existing methods of data processing, storage and analytics. To make the most out of their investment in IoT, organisations need to get several important things aligned within their strategy.

Looking to Automation

Due to the sheer volume of connected devices and the amounts of data they produce, the only realistic solution to cope with the massive amounts of IoT data is automation. Automation helps organisations to ingest, transform and deliver data and insights from it in real-time. It can ensure that IT teams can absorb the astronomical volume of data and be in a position to deliver insights in a way that the businesses can use and extract value from it.

Automation eliminates the burden of hand-coding the repetitive and time-intensive aspects of data infrastructure projects for data warehousing teams which, in turn, delivers several critical advantages. Insights from the data can be delivered in a much shorter time frame at a lower cost with drastically improved quality and reliability of the results. It additionally frees up data warehousing teams to concentrate on the more strategic work of analysis and data output. However, it is not enough to just automate the processing of data. The only way to realistically process data is on a streaming basis from devices out in the field as soon as it is created, not at a point in time in the future.

Automation plays a critical role in the processing of data. In the case of processing data from devices in the field, streaming data automation allows data warehousing teams to process data as it is created in the field, closing the gap from data to insights.

For example, a bus company that has hundreds of buses on the road every day wants to understand, as close to real time as possible, how its fleet of buses is performing so that it can maximise the efficiency of its service. With IoT-data captured from on board sensors, the bus company can analyse that data in real-time in the field, allowing it to diagnose and detect problems immediately.

Historically, data was downloaded from sensors at the end of the day, which proved problematic, because the bus could have already broken down or could have been behind schedule all day. There would be no way to get ahead of the problem. However, with streaming data automation, if a bus was in danger of breaking down, the problem could be picked up by sensor units in real-time and then steps could be taken to prevent it. By processing data in real-time, the bus company could identify immediately if the brake pads were wearing thin and could then notify a mechanic to replace them, before the bus could break down.

Understanding IoT Data Sources

There are many different types of data sources and formats created and leveraged by IoT devices - sensors in buses' breaks, thousands of sensors in a modern airplane, video surveillance cameras, machines in a factory. Some of it is traditional, structured data but there's an increasing amount of semi-structured and unstructured information produced that also needs to be processed in near real-time. Before this data can be transformed into insights, it needs to be collated and processed into a more manageable form. Attempting to do this complex task manually is not an option given data volume and complexity. Automation is the only way to do this efficiently.

In certain cases, value can be gained by consuming entire streams of data. Those data sets can be saved in their entirety to be analysed at a later point in time to identify trends. But, generally, it is more beneficial to filter all data during ingestion. To understand exactly what to do with different IoT data streams, organisations need to build an information flow that creates a big picture view of the critical, time sensitive information most valuable to their organisation.

At the same time, organisations need to identify the historical information they should store that will be useful to reveal trends over time. Something like a data lake architecture can be useful as a repository to store the full mass of structured, semi-structured and unstructured data in its native format. However, automation tools will then be needed to transform the data from an indistinct heap of ones and zeros into valuable insights.

IoT's Impact on Storage

When it comes to infrastructure to support IoT environments, the knee-jerk reaction to the huge increase in data from IoT devices is to buy a lot more storage. However, with this growth being exponential, this is a costly and short-term strategy. Instead, businesses need to consider how to transform the data in the process of being stored – and, by doing that, decrease it in the process. Data analysed in real time means that organisations can save down data summaries rather than large transactional tables for future analysis.

Not only does this save on storage costs, but it also speeds up future reporting processes, and improves the quality and reliability of insights. It's a question of sifting out what is valuable and what is not. That said, there is often value in storing the raw data for a period of time to test exploratory workloads. For this, cloud storage can be a cost-effective short term option as part of a data lake infrastructure. However, it will also be critical to deploy automation tools to organise this information, manage the schemas, and allow the data to be analysed, queried and searched in the most effective format.

The IoT Market is Growing

Sensors for every thinkable purpose have become very affordable and IoT is quickly becoming mainstream. The market's economic value is expected to reach $11.1 trillion by 2025. It is no longer limited to big enterprises with large budgets as many smaller companies are looking for ways to improve their business based on the information IoT-applications can provide.

Additionally, for sensors and other IoT applications, mature automation tools are also available to accelerate the time to value and create an immediate impact. The next step for many companies to manage and drive value from their data will be the implementation of artificial intelligence, deep learning and machine learning. We will then see that the limit of what companies do with their data will no longer come from their ability to afford the technology, but instead from their creative application of the insights that they are able to create.

The new enterprise data dilemma

Data analytics and ML in a multi-cloud enterprise.

BY VINAY WAGH, DIRECTOR OF PRODUCT AT DATABRICKS

OVER THE PAST DECADE we have seen the evolution of how enterprises manage their data from being on-premises to a gradual shift towards cloud, and it is raising some familiar concerns. These are things like security, governance, vendor lock-in, or missing out on best-of-breed solutions, to name a few.

Today, most organizations are not standardizing on a single cloud. They select the best platform for each workload to optimize their business outcomes. As a result, we are now on the precipice of the next evolution, multi-cloud, and there are two types of enterprises emerging: those that are already multi-cloud and those that will be.

It's important to note that multi-cloud is not about abstracting cloud providers so users can seamlessly run the same workload anywhere. Instead, multi-cloud is about making a choice between cloud providers based on the use case and making the migration of workloads from one cloud to another feasible. Enterprises are already faced with the growing proliferation of different departments on different clouds optimizing for best-of-breed services from cloud providers, and then there is an entirely different beast of integrating cloud strategies from mergers and acquisitions. Though one might

immediately think this is a management nightmare in the making, which it can be if not done right, there are benefits as well. Specifically, benefits that increase the opportunity for business agility, flexibility, and scalability, while avoiding the dreaded vendor lock-in.

In such a complex multi-cloud landscape, having a long term data strategy that allows businesses to securely use quality data across multiple clouds without having to worry about data migration is a requirement. What's equally important is providing a consistent and collaborative open unified data analytics platform that extends across clouds for data teams to use the data and generate business value.

The role of open source technology

Utilizing open source as a part of the data quality and integrity strategy that extends multiple clouds is important for enterprises to consider. An open source storage layer ensures the consistent treatment and experience for data while further enabling a working multi-cloud strategy. It is a critical part of maintaining quality and integrity and having that layer in open source enables portability.

Why is it critical? Because only open-source technologies and data formats can truly enable the benefits of multi-cloud.

The ability to automate configurations, enforce security and governance policies, and replicate data in open formats across clouds give you a true choice between cloud providers.

The data quality challenge

Today, investing in machine learning (ML) is one of the most important data priorities for cloud-powered organizations. However, ML models are only as good as the data they learn from. Therefore, maintaining a high standard of data quality and integrity in a multi-cloud environment is extremely important.

The solution to maintaining data quality starts with having the right data governance policies in place, so you can manage who is responsible for ensuring the quality of a specified dataset, which groups/teams are allowed to access it, and what applications are using the dataset to make which business decisions. This allows you to measure quality issues and build accountability into the process.

not try to abstract core security functions to be cloud-agnostic. Instead, it will embrace the cloud-native constructs and advantages of each provider that are built for their respective cloud. The key to success around multi-cloud data security and governance is figuring out how to build a consistent framework on top of the cloud provider's constructs that easily defines policies and implements them across a wide range of users working on data analytics and ML. This framework can also abstract out the cloud-specific implementation so that developers and data scientists don't need to write cloud-specific code.

For example, in the case of data analytics and ML, having a unified platform could provide a policy framework that allows your admin to specify which users have access to PII data, create clusters to process data, share notebooks or run ETL jobs, or have restricted access to production workspaces. The multi-cloud powered business is here to stay Businesses realize the importance of data and are

> The solution to maintaining data quality starts with having the right data governance policies in place, so you can manage who is responsible for ensuring the quality of a specified dataset, which groups/teams are allowed to access it, and what applications are using the dataset to make which business decisions

Technology plays a critical role here. With the increasing quantity of data produced each day, the manner in which you store your data sets the stage in what you'll be able to do with it later. Every organization has a mixed approach across data lakes and data warehouses that is best for their use cases. These of course come with benefits and challenges across data management, flexibility, and usability. When we specifically focus on data lakes, having a storage layer on top of the data lake that provides transactional guarantees and schema enforcement that it in turn ensures high integrity and quality of data.

What about security?

Often, organisations need to use some of their most proprietary and important data to build ML-powered applications. Therefore, security is extremely important. Correctly implementing and maintaining security policies on one cloud is hard enough, now applying that on two or more can significantly compound the difficulty.

However, ensuring data security in a multi-cloud infrastructure isn't a fairy tale that requires some magical amulet to unite all security policies together. Technically speaking, a good multi-cloud strategy will

using it to make informed decisions via analytics and using machine learning to solve challenges, create new data products and revenue streams, improve operational efficiencies, and more. In many cases, thriving organizations are treating data as one of their most valuable assets. The organizations that are redefining their space are the ones that are implementing data strategies that enable them to use their data at scale, which mandates high data quality standards with the right security policies. As we move towards an increasingly larger multi-cloud landscape, businesses need to quickly ensure that data quality is maintained across clouds with strong data governance and security. Without these, organizations are not able to use their data assets to their fullest potential. Private digital workspaces for accessing data are going to be the future where the compliance and governance teams will function best when tied together to the cloud provider and the enterprise network.

Ultimately, a unified data analytics platform addresses these challenges by helping organisations bring all their users and data together in an open, simple, scalable and secure service that extends the entire data lifecycle and can leverage the native capabilities of multiple clouds.

Avoid the double whammy of high costs and ineffective implementation in ITSM

IT efficiency remains a major objective for enterprises in every sector, all too-frequently undermined by costly or ineffectual implementation of ITSM solutions. Yet ITSM is critical to the future.

BY MARK TWOMEY, CEO, XCESSION

DESPITE THE PANDEMIC, research and advisory company Technavio says growth in the IT service management software (ITSM) market will be nearly eight per cent this year (2020), climbing to nine per cent overall up to 2024.

The deployment of ITSM should turbo-charge IT efficiency, reducing the hours spent on routine processes, eliminating a layer of costs and providing a faster, more resilient, productive network. Unfortunately, many enterprises find themselves being hit from two sides once they have selected their software and signed off the business case. On the one

hand they pay for unnecessary licences and on the other they have to foot the bill for unnecessarily costly implementation services which fail to deliver the gains promised.

The drawbacks of vendor-specific implementers

The reasons for this frequently lie in the choice of implementer, which in many cases will either be the software vendor itself, or far more likely, one of its implementation partners. This is a market that tends to undermine the interests of the customer. Pressures on margin from the vendor mean the partner sells licences that are not needed or prolongs implementation in order to maximise fees.

This is not to underplay the importance of expertise in a vendor's products. Expertise is always worth paying for and organisations with specialist skills should be remunerated accordingly. Being a Gold or Platinum partner of a vendor, however, is more often than not a badge of sales-excellence rather than product or industry expertise.

Let's not forget that ITSM software, though highly beneficial, is potentially very costly, with long commitments of at least four or five years and implementation periods of 12 months in some cases. For sales people the rewards can be substantial, with licences based on users, servers, or the number of automations. Getting the balance right between the various types of licence can have a major impact on cost. It is not unknown for "true-ups" to reveal an organisation has been using far more licences than originally scoped, a situation to the financial benefit of the implementer.

Engage an independent implementer focused on outcomes, not licence sales

Any organisation facing this set of challenges needs to work out how it can get the value out of its ITSM investment faster. It needs a partner that is customer-focused rather than vendor-focused, and preferably not trying to sell licences.

Independence in ITSM implementation has long been underestimated. Having access to truly objective but expert recommendations provides a far better outcome, drawing on the best solutions for each task, irrespective of vendor or number of licences sold.

For many complex enterprises, multi-vendor ITSM solutions are frequently required, as part of a best-of-breed approach. Multiple orchestration or automation tools may be required, plugging into supplier systems. In any case, many existing infrastructures already have multiple management systems, with the main ITSM software from one vendor, but the most suitable reporting or analysis tool from another.

Achieving the best outcome when multiple solutions are required is difficult when implementation is undertaken by a partner tied to a specific vendor. Vendors or implementers are ready with answers that tick boxes in RFQs but which are not necessarily the right solution. When value-realisation begins, the process proves to be far more difficult than customers ever imagined.

Indeed there is often friction between the vendor and their implementation partner, who may even have scoped out a project that is very different. There is often no roadmap detailing how to extract best value from the new software over time. As organisations' needs change, software and its licences should be tailored to what they require, rather than continuing as before to optimise partners' fees.

> Enterprises can avoid most of these ITSM pitfalls if they are prepared to opt for an independent implementation partner

Independent implementers, by contrast, will understand an enterprise's existing or newly-acquired software tools and be ready to use them in a more integrated manner, delivering the outcome required without having to spend money on more licences.

And as they go about their work, a form of knowledge-transfer takes place. Customers understand more about what they need and have greater insight into what the market offers, ensuring they have not just the best solution for their needs, but also the most suitable version.

Breadth of solution knowledge is a great advantage

Enterprises can avoid most of these ITSM pitfalls if they are prepared to opt for an independent implementation partner. A partner that is not tied to any vendor but has the necessary breadth of software knowledge and implementation experience to focus on the customer's own requirements and business aims. An independent implementation partner that is not selling licences to claw back lost margin.

Breadth of software knowledge and genuine agnosticism bring real benefits for enterprises in ITSM implementation. If they want to avoid being hit by a double or triple-whammy of high implementation costs, unnecessary licences and misconceived or poorly-functioning ITSM solutions, they should think hard before opting for a vendor-partner. Opting instead for independence is the most reliable way to ensure they benefit from objective expertise that focuses on their needs and provides them with the optimum set of solutions.

How to break down siloes and unleash the power of AI

The biggest thing holding back AI, is people.

BY JED MOLE, CMO OF ACXIOM

WE'RE NOT TALKING about AI replacing jobs here, it's more about people's tendency to create siloes. We need to make sure we've got a patch of turf that we're responsible for. One we can protect and ultimately, be seen as key to the delivery of good performance.

Data-driven insight is only as good as the meaning attached to it, and when customer data is sitting within different departments, no one has a true 360 view of the customer, and no one can address or anticipate their needs accurately.

A report by Deloitte at the end of last year argued that to become a truly AI-fuelled organisation, a company will need to fundamentally rethink the way humans and machines interact within working environments. But where to start?

Where is the customer data?

We're at a tipping point in the conversation around data. Businesses have gathered more than ever before but have yet to realise the true value it can bring to customers and business alike. This lack of clear value from data has led to a lack of true understanding when it comes to data and a dip in the trust of some customers and regulators. Looking forward, the challenge for brands is mastering the complexity that data brings to realise customer value.

Success will be achieved by those who are able to break down siloes and barriers by bringing marketing, data and tech together. This is easier said than done of course, our habit of creating siloes is hard to kick. It is easy to create data sets, databases, dart marts and more, it all sounds pretty innocuous, but if you cannot

connect the data when you need to then you have a disconnected and incomplete view of your number one priority, your customer.

Connecting data may be necessary in a 'slow data' sense, for example for longer-range analytics or it may be necessary in a 'fast data' sense, real time connections of actions and insights to deliver relevance in the moment.

Of course, this is just the data view, as we added telemarketing tech to direct mail tech, then overlaid an email platform, followed by a social media platform, DMP, CDP and so on, we solved one problem (the absence of a channel) by adding often disconnected siloes. It's a challenge to avoid the temptation to silo.

When AI comes to town

Artificial intelligence is a wonderful technology that promises a lot for the future of customer interactions. It can analyse and predict what we want or need at rates that simply aren't possible for human-led analytics. Whether it's research, manufacturing or on a broader scale just helping at home via our smart devices, the potential and power of AI is massive.

To move from potential to reality, paradoxically means adding humanity. What I mean by that is we need to shape its remit, give it a chance to get it right and, central to that, is giving AI the data necessary to give

the customer an interaction they'd really value. In having a complete picture of the customer, the first person to benefit is the customer themselves.

We see time and time again that customers are willing to share their data so long as they know it'll be protected, and used to offer them convenience, a relevant recommendation or a tangible offer, such as money off.

Achieving that customer satisfaction is gold dust, and it means the whole cycle keeps turning. The customer is more likely to engage with the brand, then that data can be used again to make their experience better again.

Change for the better

A huge change for the better, that most organisations would benefit from, is eradicating or at least reducing silos. AI is the shiny new thing that promises so much, but like previous holders of that title, connected customer data, that is as complete and accurate as possible, is the number one factor for success and the number one priority.

The building blocks for that success include: 1. having a proper data strategy (that includes data privacy), 2. an identity management solution and 3. a unified data layer, physical or virtual, that enables data potential to become value for all.

Gaining transparent and actionable insights through intelligent data fabrics

Aging data lakes, while popular in previous years through their promise of being able to provide an overview of useful business data, haven't lived up to the expectations they were due to deliver. Instead they have struggled to provide the true visibility for transparent business decision making.

BY JOE LICHTENBERG, PRODUCT AND INDUSTRY MARKETING, INTERSYSTEMS

NOW, as technology continues to advance and the need for real-time access to data becomes increasingly important, particularly in light of ongoing macro-economic trends, new data management solutions are required to utilise existing architectures in place and to clear the murky data created in these lakes. Alongside other advantages, utilisation of intelligent data fabrics are now allowing businesses to retrieve key information from their data to provide actionable insights. By having this ability to access data in real-time, businesses can move forward confidently during a crisis.

Bringing together real-time and historical data
It has become increasingly difficult to integrate, transform, normalise, and harmonise the many different data points in data lakes so that organisations can gain a consistent and comprehensive overview and are able to use them effectively. Further complexity has been added due to the growing availability of real-time data and the subsequent requirement to harmonise this alongside batch data.

Additional complications arise when businesses need to use real-time and historical data to make decisions in the moment. Ultimately, data lakes have shown themselves to be incompatible with these requirements, and many organisations are now looking for a way to combine both real-time data and batch data in a way that allows them to gain actionable insights.
Intelligent data fabrics provide the opportunity for businesses to complement their current technology with new innovations, and enables them to continue to extract value from their existing data architecture

and investments without having to rip and replace old systems. In many businesses that are operating in a highly siloed, distributed environment with many legacy applications and data stores, this need is coupled with the requirement for technology that can create interfaces to their existing infrastructure. They also need to be able to aggregate, integrate, transform, and normalise the data on demand. With data lakes proving themselves to in effect be just another silo, a new approach is needed for businesses to get the most out of the data at their disposal. This is where intelligent data fabrics can provide a steppingstone to the next generation of data architecture.

Why intelligent data fabrics are different
In their ability to transform and harmonise the data so that it is actionable, intelligent data fabrics possess a key differentiator. They are able to incorporate a wide range of analytics capabilities, from analytic SQL to machine learning, to support the needs of the business. By allowing existing applications and data to remain in place, intelligent data fabrics enable organisations to get the most from previous investments, while helping them gain business value from the data stored in lakes quickly and flexibly to help meet the needs of a variety of business initiatives. This includes everything from scenario planning and risk modelling, to running simulations for wealth management to identify new sources of alpha.

Using traditional technologies with data lakes can create challenges in trying to gain these capabilities. Via traditional means, multiple architectural layers would be needed, including scalable data stores, an

integration layer, transformation, normalisation, and harmonisation capabilities, a metadata layer, as well as a real-time, distributed caching layer. Then, there is also a need for an intelligence layer, with application logic and analytics capabilities, and a real-time layer. Building such an architecture traditionally required a wide range of products as well as integrations and maintenance of the products, making it extremely complex and costly to build and maintain.

New advances in technology can assist the stack in terms of implementation, maintenance, and an application development standpoint, making it more streamlined and simplified. There is no longer a need for different development paradigms to manage the various application layers. It is also higher performance as latency is reduced due to the removal of interfaces to connect the different layers of the architecture, allowing organisations to incorporate transaction and event data into analyses and processes in near-real-time.

The role of data fabrics in digital transformation strategies

Crucially, increases in data volumes and workloads can be accommodated through the scalability of modern intelligent data fabrics. For example, in the finance sector this is particularly critical where markets and volatility levels have spiked during the COVID-19 pandemic. Furthermore, it can assist a business' long-term goal for digital transformation as it breaks down data siloes, helping to remove operational inefficiencies and streamline processes which are the central aims of all digital transformation strategies. Once siloes have been broken down, organisations gain an overarching view of the enterprise data from internal and external sources, and with that comes the synergy to be able to use that data for a wider range of purposes.

Along with the benefit of information being accessed from all corners of the organisation, alongside the all-

important metadata, it also enables data provenance and lineage. This is critical for businesses to be able to understand the source of the data and what actions have been applied to it so that they can validate and trust the data which is being used to make significant business decisions.

Real-time insights from the cockpit perspective Incorporating an intelligent data fabric can provide a comprehensive, real-time operational "cockpit" to the business. To see the value of this in practice, look at flying a plane - a scenario in which pilots need to synthesise a variety of data to do so safely.

Thanks to advances in technology, pilots now have all the signals they need being combined and analysed in real-time and presented in a display and with alerts that can predict the risk of incidents and suggest corrective actions in real-time, without requiring the pilot to manually interpret different signals from the various parts of the plane. In times of crisis, such as an imminent stall, these capabilities become critically important. Similarly, businesses today want this same capability to filter out the data that isn't important and to bring the information that is to the surface. These capabilities can steer the business in normal times and become critically important in times of crisis as we're seeing now.

Transparency is key for future architectures

With external crises impacting on organisations' decision making, businesses are looking for transparency and insights in data to help devise better strategies now and for the future. Whether batch or real-time data, intelligent data fabrics allow businesses to deliver value back to their customers and gain increased efficiency. Through use of these techniques, data transparency can be achieved without businesses having to upgrade their technology infrastructure, helping to save on costs and ultimately reduce risk moving forward.

Shoring up business continuity with citizen developers

The last six months have brought about some of the greatest shifts in the business world to date – and as a result, organisations have been under mounting pressure to turn up the heat on digital-led initiatives. This is all while employee numbers have decreased, where staff have been furloughed and other cost-cutting measures have been implemented, as remote working has steeply increased.

BY YAD JAURA, PRODUCT MARKETING MANAGER AT NETCALL

IN ADDITION to keeping the lights on and revenue coming in, businesses are under pressure to innovate – which is no mean feat in the current business climate. One area in particular that could cause headaches is the level of technical skill needed to drive this higher level of transformation. However, bringing in highly-skilled developers to drive new initiatives is not necessarily the answer – or even an option, given the costs involved.

The challenges surrounding digital-first

Over the years, the demand for software developers has grown exponentially as businesses strive towards a digital-first future. Analysis from IT trade association

CompTIA revealed more than 165,000 IT job openings were advertised in Q3 of 2019, representing a 19% increase quarter-on-quarter. Out of these openings, the software developer role was among the most sought-after, with more than 59,000 postings in the quarter alone – despite there simply not being enough developers to go around.

However, with the average salary for DevOps engineering jobs in the UK currently estimated at £72,500, the cost of employing such skills will prove problematic for businesses that are carefully balancing innovation with budgetary constraints. According to predictions from Forrester, companies in 2020 will cut tech budgets 6% to 10% from 2019 levels and by 10% to 14% from 2020 plans[1]. As a result, and with prolonged economic uncertainty ahead, investing in new tech talent has had to take a back seat for a number of businesses. Alongside ever-increasing demands from the business for innovation through new apps, this has led to a considerable IT backlog, where projects have been put on hold, and time to market has been significantly delayed due to the right skills not being available. As revealed in a recent IDC Survey Spotlight, one of the biggest issues caused by the lack of IT skills among European organisations are delays in developing new products and services, delays in deployment of new hardware or software, and difficulties in meeting objectives.

The traditional software development model has only perpetuated this need for expensive developers. At last, this is changing. New app development alternatives are available that address the requirement to simplify software development and, for the first time, usher in the possibility for citizen developers to effect meaningful digital change. This from the people already inside the business with a ready-made understanding of the problems that need solving. Now there is an alternative that allows businesses to overcome the barriers to delivering the innovation that may have been holding them back.

Innovating from within

Instead of spending significant time and investment searching and recruiting for external skills, innovating from within, and enabling existing employees to become citizen developers, is a time and cost-effective solution. Citizen developers can add value to businesses and drive developments from the very core of the organisation – whilst their in-depth understanding of specific process challenges help ensure that new systems and applications suit the needs of both the company and internal staff.

The opportunity for citizen developers within a business is endless – and this is where low-code technology plays a crucial role, as it allows employees with varying levels of technical skill to design and build powerful applications. These tools have advanced to the point where the creation of enterprise-grade apps is now possible, opening up enormous possibilities for organisations looking to increase their pace of innovation. In this way, the tools have democratised the software development process – and are now enabling a larger proportion of employees, who have a range of expertise from across the business, to drive innovation. It's giving citizen developers the power and ability to take organisations to the next level as businesses continue along their recovery journey.

Overcoming the process disconnect

Whilst the technical skills from a qualified software developer are extremely valuable, often these developers do not possess the day-to-day experience of the processes they have been hired to optimise. This leads to a 'process disconnect', where improvements made by the developer do not necessarily fit with the desired outcome from the employees who will be using them. Existing employees, on the other hand, who operate at the frontline, can utilise this knowledge to enhance processes and drive greater efficiencies. Due to their working knowledge of these systems, these employees will have their own ideas on where efficiencies can be made, based on any challenges they have previously faced and process optimisations they would personally like to see.

By embracing low-code technology, which can be used by anyone, no matter their level of technical ability, existing employees can make these changes first-hand. And by enabling people to quickly prototype new processes and workflows without any need for specialised technical skills, businesses can innovate and implement significant changes without having to rely on highly-trained developers.

Opening up the scope for complex applications Whilst some initially (and incorrectly) may assume that low-code is simplistic and only suitable for basic applications, this technology in fact opens up the scope for a range of complex platforms that can bring significant value to a business – as well as its customers. One project that is effectively utilising process application technology including low-code is the Lloyds Market Association's (LMA) 'Gemini' claims expert management solution. Following the development of a digital claims expert catalogue, using modern Platform-as-a-Service (PaaS) technologies, the team are now using this to better understand their true spend on claims experts whilst monitoring and optimising performance. During a time where technology budgets are tight and access to digital skills is challenging, placing the power back into the hands of employees will be crucial to not only providing business continuity, but propelling businesses forward into the 'next normal'.

Further reading
1] Forrester Research Inc. - WEBINAR – Where and How to Adjust Tech Budgets In The Pandemic Recession

Strengthening borderless networks

Five ways cloud-managed DDI can help.

BY MALCOLM MURPHY, TECHNICAL DIRECTOR, EMEA AT INFOBLOX

AS THE TRADITIONAL NOTION of enterprise borders continues to disappear, it is critical organisations have easy and secure access to the global systems and data they need for day-to-day operations. But today, keeping the lights on isn't enough, and forward-looking organisations are moving to the cloud and investing in technologies such as SD-WAN, SaaS, IPv6 and IoT to improve processes and optimise performance.

The rise in demand for direct-to-cloud access at the edge has created the need for a more de-centralised networking model, one that protects both the hub and spoke environments. For example, not only does a retail chain need to keep its HQ (the hub) online, but every single store (the spokes) need to be connected to HQ, and each other, in order to process transactions and manage real-time inventory, amongst many other things.

The need to extend IT infrastructure across multi and hybrid cloud environments, and all the bells and whistles that come with it, brings a multitude of challenges that will drain a lot of time and resources from the average IT team. What organisations now need is a more simplistic and reliable way to manage their network, devices, apps and services across all environments and in any location. That begs the question, how can organisations solve networking challenges at the edge, whilst resources are stretched thin, without compromising on the end result?

Cloud-managed DDI (DNS, DHCP and IPAM [IP Address Management]) allows organisations to build a unified solution to facilitate all communications via an IP-based network. By shifting the management of DDI to the cloud, organisations can manage their borderless enterprise centrally in one location, making it far more secure and reliable than traditional on-premise DDI solutions. By optimising network access and performance across all locations, cloud-managed DDI if fast becoming the backbone of digital transformation.

So, how do you convince stakeholders that cloud-managed DDI is worth the investment?

Here are five ways that cloud managed DDI can address a number of key challenges for borderless networks:

1. Cost efficiencies through flexibility

Not all branches or remote-sites in an organisation will need enterprise-grade DDI services. Some may already use a DNS that ticks all the boxes in each location, but is instead looking for DHCP or IP address management services for some of its smaller offices. In the same vein, some may want to grow DDI capabilities

in some locations and not others. Flexibility is key here. Organisations currently going through digital transformation, being able to roll out DDI slowly will enable them to upgrade DHCP whilst keeping current IP address management solutions with very little disruptions. Cloud-managed DDI prevents organisations from overinvesting where there is no need, for example in offices or branches where the technology may go unused, as it offers the flexibility to implement the best fit DDI for each location.

2. Removing latency

Many businesses depend on important real-time information, whether it be from manufacturing facilities, supply chain networks or remote offices. In addition, when we think about how much of the world's businesses depend on IoT technology, it's easy to imagine the negative impacts that latency can have. Yet, this is what can happen when organisations backhaul DNS and DHCP through an HQ's data centre.

Beyond latency, if a data centre goes down for any reason, the link to the HQ is cut and no information from the edge will reach the central unit for DNS and DHSCP resolution, causing them to go offline. This is why local DDI maintenance is critical to ensuring always-on networking across all environments.

3. Reliable application access

With businesses increasingly prioritising the expansion of their global footprints and the number of remote-workers skyrocketing in the past few months, being able to reliably access critical applications from the network edge has never been more important. To do so, organisations need to shift away from MPLS architectures to avoid backhauling traffic through the data centre and compromising on speed for end-users on the network edge.
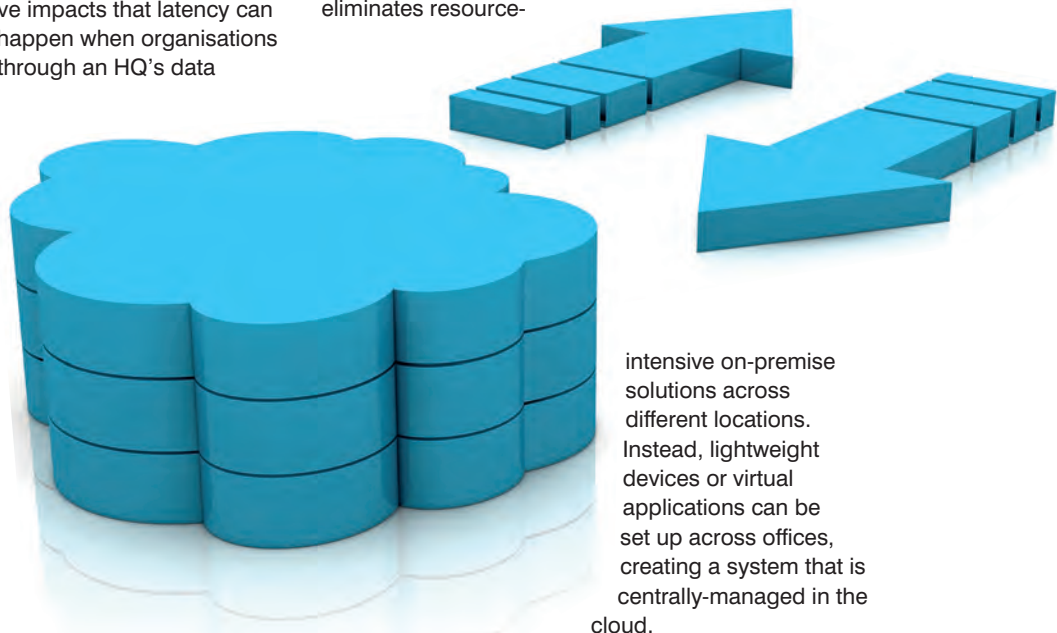
When it comes to moving towards cloud applications like Microsoft Office 365, a new kind of infrastructure is needed to ensure DDI services can be delivered centrally via the cloud and that remote location traffic can connect with closest local PoPs in the cloud, minimising backlog.

4. Scaling on the edge

Cloud-native organisations do exist. They were born in the cloud and don't have to deal with the idea of a centralised data centre because their applications and services are managed and delivered 100% in the cloud. But whilst they themselves are cloud-native, it can be hard to find a cloud solution for managing remote offices and locations.

To this day, DDI services like DHCP are often managed on-site through hardware routers, and a large organisation could have thousands set up globally. Commonly, on-premise solutions are hard to scale, take up a lot of resources and provide no easy way to manage and monitor the various locations.

For cloud-native organisations, cloud-managed DDI eliminates resource-intensive on-premise solutions across different locations. Instead, lightweight devices or virtual applications can be set up across offices, creating a system that is centrally-managed in the cloud.

5. A central control system

Cloud-managed DDI brings together an organisations core network services - DNS and IPAM, on one platform in the cloud. Swapping out on-premise DNS and DHCP controllers, which are siloed in each location, with cloud-native technology allows organisations to accelerate their digital transformation. This means better performance across remote locations with higher reliability and faster access when it comes to cloud-based apps.

With an explosion of workflows on the edge, traditional networking won't cut it. Growing organisations require flexible solutions that speed up workflows to meet the increased immediacy demanded by a globalised economy.

> Cloud-managed DDI brings together an organisations core network services - DNS and IPAM, on one platform in the cloud

Data Gathering

a legitimate means of getting ahead

The importance of data is undeniable. Its uses are woven into every sector and function of the global economy. In fact, the cold, hard reality is that without having access to valuable data, you will struggle to get ahead.

BY JULIUS CERNIAUSKAS, CEO, OXYLABS

SIMPLY, the organisations that leverage their data to make decisions when it comes to strategizing are less likely to make mistakes and are better prepared to compete with competitors and cater to their customers.

Historically, accessing insightful data was a challenging process, complicated by laborious (and often tedious) collection methods. However, advancements in technology, like Artificial Intelligence and Machine Learning have rapidly shifted the needle and have now made the data gathering process far more efficient and accessible.

The amount of publicly available data is vast and being able to leverage it can often represent

the difference between success and failure. Data gathering solutions are now recognised as a legitimate means of capturing information, in an ethical way, to aid decision making. Therefore, it is no surprise that the data industry is expected to grow by almost $100bn within the next five years.

Proven data gathering methods require a good quality proxy to help ensure the user is anonymous and allows them to enter a website without having their IP address blocked, providing a secure and reliable way of gathering data.

Even though many people are aware of web data gathering (or web scraping as it is more commonly known), most of don't understand the true value it can deliver for a business. Let's explore it:

Business intelligence

Gathering internal data is an essential consideration for any business, as it can help identify how well campaigns are performing and provides business leaders with the necessary information to make well-informed decisions.

However, if a business is looking to go further, it will also need to gather external data to stay ahead of the competition. Data gathering technology helps significantly, as it will enable a company to gather information on the closest of rivals from tracking changes in pricing, auditing the product line, observing presence online to reviewing public engagement and even monitoring generic promotional activity. With access to this variety of insights, an organisation is able to understand its

competitor's movements, regardless of where they are in the world and use that knowledge to stay ahead.

Stock market research

As discussed, business intelligence is key to helping a business get ahead. One of the biggest environments it can do this in is the stock market. For years, manually performing stock market research was almost impossible for most businesses as it would prove to be costly and inefficient. Luckily, using data gathering services can automatically keep track of current stocks in the market and access incredibly valuable financial data quickly and easily.

As far as data gathering uses go, being able to capture stock market research is hugely beneficial. The right data gathering tool can analyse and refine data by removing all the redundancies, which will leave only the usable data. This reliable data can then be analysed with specific software to give a precise result that can be used to make an informed decision on investments. The offset of this is huge savings in time, money and resources, which can then be passed on to the business.

Dynamic pricing

Since most businesses set their prices based on the laws of supply and demand, flexibility over pricing is crucial. That way, it's easier to remain competitive in the market while bringing in as much revenue as possible. If a business fails to price its products appropriately, it is likely to miss out on potential revenue to its savvier competitors.

Luckily, it doesn't have to be this way, as data gathering services can be used to set an effective dynamic pricing strategy, meaning it automatically gathers the latest pricing information as opposed to having to acquire it manually. Once this data is attained a business can then set the price for its product or service appropriately, depending on the conditions of the market.

Enhanced lead generation

Lead generation is by far the most important part of the sales process for most organisations. Based on Ringlead statistics, 85% of B2B marketers say that lead generation is their most important content marketing goal. However, attaining the required information through publicly available sources and social people data can be incredibly time consuming.

Data gathering services can be incredibly useful in terms of lead generation, as they can provide organisations with access to a considerable amount of valuable information. Once it has been structured into an understandable format, there will be a massive database of potential clients on hand. Therefore, enabling marketers to develop tailored campaigns, designed to reach more relevant customers and hopefully in turn result in converted leads.

> The last few years have seen organisations increasingly leverage publicly available data, with many now relying on data more than ever to get a better understanding of their competitors and customers. Web scraping has played a fundamental role in achieving this. But it's important to develop new, innovative methods of web scraping to stay one step ahead of the market

Looking ahead

The last few years have seen organisations increasingly leverage publicly available data, with many now relying on data more than ever to get a better understanding of their competitors and customers. Web scraping has played a fundamental role in achieving this. But it's important to develop new, innovative methods of web scraping to stay one step ahead of the market.

As an example, the role of AI and Machine Learning is already beginning to play a significant contribution. At Oxylabs, we've recently released a Next-Gen Residential Proxies platform, enabling users to collect publicly available data, without the threat of detection by anti-bot solutions. The platform is the first of its kind to integrate AI and Machine Learning and provides the highest success rate for web data collection. Again, this will support organisations looking to enhance their business intelligence and lead generation capabilities.

Additionally, in order to expand Oxylabs influence in the data industry, we have also created an AI & ML advisory board, comprising of prominent professionals from the world of machine learning, AI, and data science, many of whom have experience working in highly reputable companies and universities like NASA and Massachusetts Institute of Technology (MIT).

This is only the tip of the iceberg – as organisations dig deeper into the data available to them, they will need the right tools and platforms in place to support their data collection efforts. Data gathering solutions are a legitimate means of capturing information in an ethical way, but it is crucial that proxy service providers ensure ethics and innovation are at the heart of their offering.

Outside the four walls of the data centre

Almost four in 10 people in the EU began working remotely in the first few months of 2020, according to a study carried out by Eurofund. This is a seismic shift considering that the amount of people who regularly worked remotely before the pandemic took hold ranged from as low as 6% to as high as 23%, depending on country.

BY MICHAEL CADE, SENIOR GLOBAL TECHNOLOGIST, VEEAM

NOW THAT ORGANISATIONS and employees have seen some of the benefits of remote working, many companies are likely to build more flexible and agile working arrangements into their long-term strategies. For IT departments, the impact of this is huge.
The digital fortress

Formerly, a company's IT infrastructure was contained within its own four walls. Employees used hardware such as PCs, printers and phones which remained securely in the office, while software programmes and data were stored in on-premises data centres. IT had full control over the performance, maintenance and security of the organisation's technology stack.

Early remote working initiatives were tightly controlled with users connecting to Virtual Private Networks (VPN), so that the only thing that left the data centre was the employee and the limited hardware. Over the VPN, the IT department could maintain visibility of security protocols and maintain administrators' rights to ensure employees were not installing unapproved, potentially high-risk software.

Along came the cloud, which allowed organisations to scale-up their data storage capacity as well as their ability to back up files to remote locations. However, with the cloud came greater agility and choice for employees. Shadow IT, the phenomenon of employees using applications of their own choosing to store and access company data outside the data centre's four walls – on personal devices and online accounts – became a challenge to IT departments.

Fast-forward to 2020, when at some stages nearly half of Europe has been working remotely, and the four walls of the data centre have fallen as far as many businesses are concerned. Some organisations found themselves supporting remote workers for the first time – many with employees who would not be working from company-issued laptops and smartphones. A report from OneLogin, which surveyed 5,000 global workers from the UK, the US, Germany, France and Ireland, found that only 33% of employers in the UK enforce multi-factor authentication for employees who are working remotely.

From a cyber-security perspective, this is a critical risk. Previously, the data centre was analogous to a fortress. Everything that went in or out was strictly monitored and the threat from external sources was low. This is why one of the most well-known forms of cyber-attack is a Trojan virus – one that tricks the victim into thinking they are receiving or opening a legitimate file, document or link – effectively inviting in the attacker. Now, not only have the gates of the digital fortress been flung wide open, the people who used to be inside are now distributed. And, every single one represents a possible entry point for a malicious threat. The attack vector hasn't just increased, it's exploded.

Increased threat vector

IT departments often have little to zero visibility of whether or not employees are connecting to the VPN, particularly when employees are using personal devices. Furthermore, personal devices aren't just being used outside the data centre's four walls, but in family home environments and shared households. Not only do IT teams have far less control over the apps, websites and content their employees are engaging with, there is no guarantee they are the only person using that device. While the organisation might not have visibility of data now being stored and used outside the four walls, it is still ultimately responsible for it.

Given this vastly increased threat vector and risk to data systems, organisations must ensure they have a robust Cloud Data Management strategy in place to ensure data is backed up, protected and recoverable across all devices and applications. Employee best practices and training are vital to this – helping IT teams ensure that users are connected via the VPN and are storing company data in secure cloud environments, rather than on personal accounts or their own desktops. If data cannot be backed up it is not protected, and in the event of unplanned downtime or a cyber breach that data will be unrecoverable. Moreover, organisations are adopting Software as a Service (SaaS) solutions in their droves.

For example, Microsoft Teams grew from 32 million to 72 million users between March 2019 and April 2020. For businesses using SaaS solutions such as Microsoft Teams and Microsoft Office 365, backups of data need to be conducted on a continuous basis – either on premises or in cloud object storage. This will protect the business against a single point of failure that is outside their control.

As a combination of working from home and from offices becomes increasingly commonplace – even for organisations who previously had little-to-no track record of supporting remote working – the cyber-attack vector will remain high. It is therefore critical that businesses have a clear strategy for managing data across their cloud and data provisioning. This includes ensuring that data is backed up at all times, recoverable in the event of a disaster, outage or cyber-attack, and is as protected from external malicious threats as possible.

Before adopting Artificial Intelligence, CISOs must answer the following questions

The use of artificial intelligence (AI) is hugely prevalent in almost all aspects of our day-to-day lives including security. Looking at the security landscape, supervised machine learning (ML) is well established in threat detection but unsupervised ML and deep learning are increasingly popular tools for post breach anomaly detection.

BY JEREMY D'HOINNE, RESEARCH VICE PRESIDENT, GARTNER

HOWEVER, as AI use in security technology becomes even more commonplace, CISOs need to only study its benefits but also the risks of using AI long-term. By 2022, the replacement of conventional security approaches through ML technologies will make organisations less secure by a third.

Take a step back

There are many myths and misconceptions when it comes to AI and failing to understand this at the heart of a security team could do untold damage.

Where can AI be useful to a CISO's strategy? Most advanced AI algorithms can immediately reveal key information about vulnerabilities, attacks, threats, incidents and responses.

Engaging this function in the first instance can result in a noticeable strengthening of a security team's capabilities. Other tools such as probabilistic reasoning (often generalised as ML) and computational logic (commonly referred to as rule-based systems) can also bring huge benefits.

So what can the risks be? Because many large algorithms consume large amounts of data, CISOs must understand the implications of using an AI product when it comes to data security and privacy. Many mature organisations have jumped on the AI bandwagon without evaluating the tools they already have in use that may be doing a more effective job of security and risk management than a new tool could achieve.

ML is not immune to attacks and AI should not be treated as a silver bullet for protection. There is no assurance that AI is better than all alternate techniques and it can be fallible, offering incorrect and incomplete conclusions.

CISOs ought to focus on the end-desired outcome when it comes to their security strategy and ask themselves the following questions:
- Do my team and I have a strong understanding of different AI implementations?
- Do we need AI for the problem we are trying to solve?
- Are these AI tools designed to address our specific needs?
- How can we measure that it is worth the investment?
- What will be the impact of using AI for this?

Beyond the hype

When AI first entered the technology landscape, we saw exaggerated expectations on what it might be able to do coupled with fears on job security. The idea that AI was going to replace human jobs became rampant. In 2020, this should no longer be a concern – through this year, AI will be a positive job motivator, creating 2.3 million jobs whilst only eliminating 1.8 million.

AI has the potential to improve the effectiveness of a security team, however the idea that it can give organisations the ability to predict future attacks is nothing more than a smokescreen.
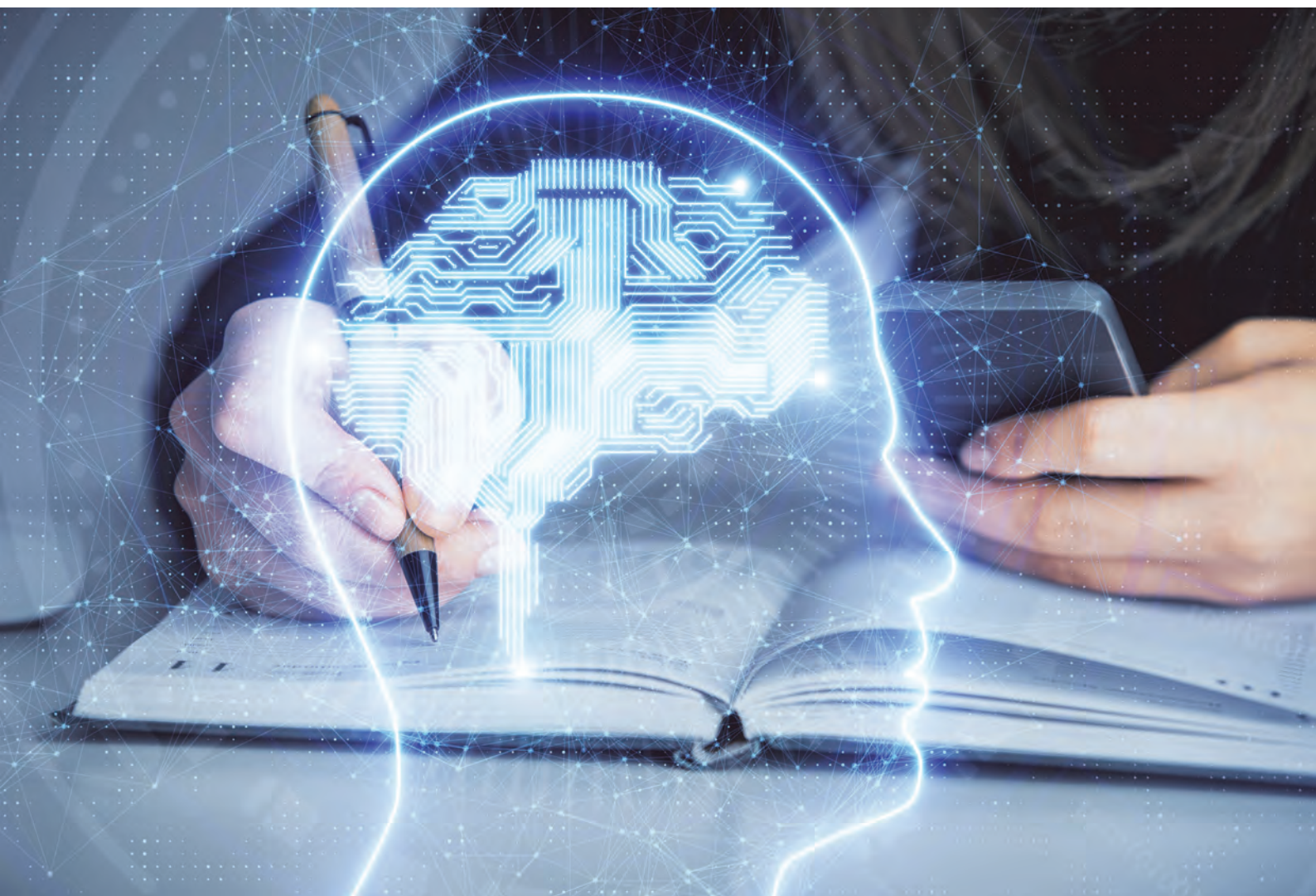
Organisations should find AI at its most effective when humans work with the technology rather than relying on it to replace human input entirely. We should not be aiming for sole AI automation, instead CISOs should be striving for 'smart automation' when it comes to their technology strategy.

Although AI may feel like an established technology, is in fact still an emerging technology. In theory, it is not a CISO's role to determine whether an emerging tool is to benefit their organisation - the technology should prove that itself over time. Switching to this mind-set will ensure that security and risk management leaders do not fall foul of the wrong AI strategy.

Today, AI does not exist in its full capacity. CISOs need to balance both their resistance to change and their fear of missing out biases to achieve a balanced AI strategy.

When AI first entered the technology landscape, we saw exaggerated expectations on what it might be able to do coupled with fears on job security. The idea that AI was going to replace human jobs became rampant. In 2020, this should no longer be a concern – through this year, AI will be a positive job motivator, creating 2.3 million jobs whilst only eliminating 1.8 million

Cybersecurity: How the physical layer impacts the overall strategy

By Jon Barker, Technical Manager, Chatsworth Products Europe

IN A REALITY where data has become the world's most valued asset, privacy and ethical management of data are not only considered priorities but also law. Cybersecurity has taken on a new meaning within every IT budget, as it is the responsibility of the enterprise organisation to ensure their data will be kept safe and uncompromised. Within the many layers of cybersecurity, the first line of defense being physical security is generally well understood in ICT. However, there are differing opinions when it comes to executing a simple and effective strategy, and how it should be deployed.

How often do enterprise organisations assess the required level of physical security for protecting data? Are they compliant with regulations that address data security? Most importantly, how is their IT team applying physical security and complying with privacy laws within a hybrid data centre architecture, where the data centre, colocation, cloud and edge sites coexist?

Regulatory Compliance

All data privacy standards and regulations require physical access control measures for data processing and storage equipment, but with most regulations, it is up to organisations to decide which specific method or technology to use.

In general, compliance to regulations requires a method to:
- Physically secure data processing and storage equipment
- Identify and manage authorised accessors
- Manage access to the physically secure space
- Keep records of access to the physically secure space

In 2018, the urgency for data centre owners to protect data became even more apparent with the introduction of the General Data Protection Regulation (GDPR), applicable to businesses operating within the European Union (EU). GDPR is a strict set of regulations that gives data protection and security policies a new level of priority. Although GDPR is an EU regulation, any organisation collecting or processing data for individuals within the EU should also have a compliance strategy.

Data Centres will need to be able to demonstrate examples of preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

Considerations When Building an Access Control System

Majority breaches occur in the network, therefore little attention is paid to physical security. It is important to acknowledge that the intent of data privacy and security regulations is to prevent a data breach. Therefore, preventing a data breach should drive the decisions around physical security.

For an enterprise-owned, single tenant site, for example, room-level security could be perceived as sufficient. But particularly in multitenant data centres (MTDCs) and remote sites, physical access control at the cabinet level simplifies management and prevents unauthorised users to access the servers and switches in which data is stored.

Any enterprises would probably argue that they already comply with privacy regulations. Most data centre cabinets have locked keys. But how can organisations ensure cabinet doors are secure? How do they document access to cabinets? How do they recover keys from users? What is the official response when a key is lost or stolen?

Electronic lock and access control systems automate monitoring, documenting and control of access and allow fast reprogramming if access rights change or if a credential is lost or stolen. These types of control systems support three types of keys:

Something a person has – Access card
- Assign and change credentials quickly without the need for changing the locks, but an access card can still be lost or stolen

Something a person knows – Keypad passwords
- A password is more difficult to steal, but it can be guessed or reprogrammed

Something a person is – Biometrics
- Biometric authentication is uniquely associated with an individual digital print and is only allowed for rare instances of fraud

A comprehensive electronic access control solution can play a vital role in a data centres user access management plan. It is important to consider the levels of security for each type of access: single-factor or multi-factor authentication. Dual and multi-factor systems may require an upgrade at the electronic lock to include an additional reader.

Essential Considerations for Rack-Level Electronic Lock Solution

When selecting a rack-level electronic lock solution, there are essential capabilities to consider:
⊙ Electronic Locks

Electronic locks secure the doors on cabinets, sense access attempts and indicate door latch (lock) opened or closed condition. These are typically swing handle with an integrated solenoid that operates the latch to opened or closed condition, a proximity sensor that indicates condition of the latch opened or closed, and an access card reader that senses and reads values from presented keys. The lock also carries a mechanical key override to handle door openings during a power outage.

Access card readers are required to be compatible with the card types provided to individuals within an organisation. Types of access cards can vary from 125 kHz proximity cards to simple 13.5 MHz smart cards, to next-generation smart cards with one-time passwords.

With access card technologies changing very rapidly, the ideal scenario would be for the swing handle and the reader to be separate integrated modules. Some

models may also include an integrated keypad or biometric reader.

Single-Factor or Multi-Factor Authentication

Multiple levels of authentication may be preferred, depending on the level of security required. Some electronic locks may include an additional keypad for a unique PIN entry.

More advanced solutions may include a biometric reader. Biometric authentication methods require consideration for privacy laws. It is recommended that it should be used alongside an RFID card, the biometric imprint is stored on an individual's badge rather than a centralised database.

Door Sensors

As well as collecting input and monitoring the cabinet lock status, an electronic locking solution for needs to monitor the status of the multiple cabinet doors themselves. In the event a door is opened, a warning notification should be triggered immediately, followed by additional warnings if the door is left open for an extended period.

Wiring and Network Connections

There are three types of network connections: The first is through rack intelligent power distribution units (PDUs). The second via a separate networked controller module. The third in which the locks are connected to a building's security access panel. In the first two scenarios the locks are managed by IT through a data centre infrastructure management (DCIM) software solution. The latter is managed through the building security system, which is also used to manage access within the entire building.

Networking Through PDUs

Advanced rack PDUs can now integrate with environmental monitoring sensors and access control. This mends the need for power management, environmental monitoring and access control, as all three can be handled at once. This is done via a straightforward, easy-to-use web interface, all networked under one IP address.

With an integrated PDU system, there is no need for a dedicated controller for the electronic locks. The locks also get

powered up through auxiliary ports on the PDU. Operators can monitor, manage and authorise each cabinet access attempt wherever the cabinet is situated through remote management to the PDU, which is already part of the data centre cabinet ecosystem. This significantly reduces the initial cost of deployment of cabinet-level locks as well as ongoing operating costs. Using this integrated, intuitive interface, data centre operators are easily able to provide log reports for critical audit trails for regulatory compliance. It also reduces the need therefore cost for wiring the electronic access systems to security panels.

Card IDs can be stored within the PDU web interface. The PDU firmware should support either a standalone list of authorised users or integrate with third-party databases that control user access and rights management. For centralised authentication, either enterprise authentication services (i.e. those supporting networking protocols RADIUS, LDAP, Active Directory) or a DCIM solution can be used.

Networking Through a Separate Controller Module

Electronic locks can also be managed through a dedicated controller module located in every cabinet. While this does increase the initial hardware cost, ongoing operational costs can still be significantly reduced by networking several locks through advanced IP consolidation technology. The PDUs that support IP consolidation allow multiple PDUs to connect through a single physical network connection, IP address and interface, thereby reducing network overhead to monitor at the rack level. For example, some IP consolidation solutions allow up to 32 controllers to be networked under only one IP address with an alternate second connection for failover capability. This means MTDCs and colocation providers do not have to pass on unnecessary networking costs to their tenants.

Like PDU-integrated system, authentication and management could be provided through interfaces that IT organisations already use. For the widest range of compatibility and security for the network, ensure that the PDU or the dedicated controller supports the IPv4 and IPv6 protocols for TCP/IP addressing with static or dynamic address assignments. Simple network management protocol (SNMP) v1, v2c and v3 protocols should be used for third-party DCIM software integration.

The web interface should support HTTP or HTTPS sessions with definable ports. Network connections should support encryption and certificates. The email server connection should be outbound only with transport layer security (TLS) and definable ports. For ease of maintenance, the controller module should support bulk configuration and firmware upgrades. The firmware should log every system change.

Networking Through Security Access Panels

With this approach, cabinet-level electronic locks are connected to a Wiegand technology-based security access panel that in turn communicates with a building access control solution. The security panels provide power to the locks.

The advantage of this approach is that it leverages the same access control system that is used for campus security. Given the high number of cabinets on a data centre floor, this solution requires installation of additional access control panels for connecting the handles on the cabinets. It is powered and controlled from that system and that system's software.

Conclusion

As greater amounts of confidential data get stored in the cloud, physical access control at the cabinet level needs to become a norm rather than an exception.

A myriad of solutions that vary based on the level of security, management modes and budgets are available for organisations to consider.

Technology media company International Data Group (IDG) predicts 50 ZB of data will be created world-wide this year. It is safe to say that enterprise businesses that inspire trust and know how to ethically address risk, security, and compliance will excel in a big way.

Physical security – A need mixed with paranoia?

Ian Bitterlin, Consulting Engineer & formerly Visiting Professor, University of Leeds

DATA CENTRE LOCATIONS vary widely, from those that hunker down inside razor wire fences to those embedded in city centre multi-tenant buildings, but they all share a demand for some degree of physical security. Some of that demand is created by the 'business' of the facility (governmental, military, security services, finance and banking, all of which have regulations in form or another that they must meet) but much of it is the result of 'salesman's puff' or paranoia by users or potential colocation clients.

There are standards that lay down principles, such as in EN 50600 (Part 2-5: Security systems) based on layers of access (the onion-ring principle) but it lacks the full exploration of 'hold-up time' – the delay introduced by each layer that could enable a sufficiently timely response and intervention by security staff. For example it does not proscribe the layers in sufficient detail, only in principle, such that the last layer (closest to the hardware) can be provided by a lock on the IT cabinet without regard to the fragility of such locks – one swift jemmy-bar and hey presto!

My preference is for a detail design of detection, alarm, hold-up time in layers and timely intervention – all based upon the clients' needs, budget and the given site constraints. I do not know if they are still in use but there was a UK government 'standard' based on Intrusion Levels, e.g. IL1-5 (or was it 1-7?) where the upper end described a forced entry based on a 'man with an aggressive machine'. I am sure it meant a hydraulic excavator, but you can substitute a firearm or suicide-belt if required. That brings up the point that the only way to really protect against a terrorist is with a 24/7 armed response force on site – something that is only reserved in the UK for government security facilities,

such as MI5 or GCHQ, but is common in countries with relaxed firearm regulations. For examples of paranoia look at vehicle traps intended to prevent a ram-raid. Has there even been a ram-raid attack on a data centre? But, although it looks good and isn't hugely expensive, a cheaper solution is to make the site entrance a 90° turn so that no vehicle, no matter how large or fast, can gather enough momentum.

So, the first step is a risk analysis to identify possible threats. Is it from people wanting to physically access the hardware? To steal it or the information contained on it? There was the theft of servers from a London facility where the perps broke in via the roof – making an opening, not using one. The press story was that sensitive credit card information was stored but when the high-end microprocessors turned up on eBay a

few days later it put 'private enterprise' into focus.

So high security could be achieved by including CCTV on the local routes to site and the approach road, a separate entrance for delivery trucks and no car parking inside the perimeter fence. The fence should be 2.5-3m high, topped with razor wire, and buried 1m, with a back-up of vertical steel columns set in concrete, to act as a 'tank-trap' etc. Vibration monitors on the fence and in the perimeter ground to detect digging or tunnelling. For a few metres, a dense planting of African thorn bushes to slow down intruders. Then CCTV, motion activated, infra-red and conventional flood lighting with both dummy and real cameras and photocell or proximity sensors around the external wall of the facility complete the open area between the permitter fence and the structure.

Personnel entry is gained through a non-tailgating turnstile that is controlled from the security office (which should not be shared with the ingress room) and the route from the gate to the front door contained so that visitors or staff cannot enter the site without going through the ingress point. The loading dock is usually a weak point.

An operational policy (not always adhered to) is that no visitors without 24h notice, photo ID and a security check. No tailgating and an access control system that gives almost nobody 'access all areas' permission completes the internal security. Corridor lighting should be motion controlled but also with a security override (for complete darkness to cause confusion) with infra-red CCTV etc. I have seen consideration of corridors with an override on the fire-suppression system to slow down intruders.

Then the perimeter of the structure should be secure and strong enough to meet the design risk. No glass or fenestration, highly secure emergency exits, interwoven CCTV systems (one visible, one concealed), no M&E plant visible from any point on the perimeter that has free public access. For example, an outside wall facing a public highway might need to incorporate a blast wall to resist a car-bomb or rocket-grenade, or simply a welded steel-mesh inner layer to increase the hold-up time of a machine. The steel-mesh (or rebar) can also double up as a Faraday Cage if fine enough and properly earthed, or the inner wall lining of the most sensitive rooms can be lined in copper sheet – both a common solution if the client is concerned about truck-mounted mobile EMP weapons. The 'possible' list goes on, and on, but the client must pay for it and that very often moderates the 'needs'.

Last, but not least, there is a new threat being considered by many operators – the disablement from outside the fence. No theft, ICT intervention or physical breach but just remove a key component of data centre functionality to attack the users' business. The first is to disable the fibre connection, without which the data centre cannot communicate. Satellite back-up does not have the bandwidth required and the fibre-pits are outside the facility, neatly identified in the cast iron lids. Lift the lid(s) and even the simplest fire device destroys the link for many days. The second newer threat is from drones – a £1,000 drone can fly 3km with a camera for guidance and carrying a 1kg payload. Make that payload a glass jar of acid and fly it into the rooftop heat rejection coils (most European facilities have dry coolers) and the aluminium coils are destroyed with a cooling 'stop'.

Did I mention paranoia?

Elevating data centre security with rack-level electronic access control

From data centres housing information for a single organization to co-location data centres where multiple companies are hosting their data in one location, managing physical access at the rack level is becoming a significant challenge for facility managers.

BY MIKE FAHY, COMMERCIAL PRODUCT MANAGER, ELECTRONIC ACCESS SOLUTIONS, SOUTHCO, INC.

THE ENDLESSLY growing mountains of personal, private data collected as part of routine transactions in our digital world continue to be a target for cyber criminals, who are moving beyond digital theft to the real world by targeting the servers that contain this data.

In 2017, the global average total cost of a data breach was $3.86 million – up 6.4% from the previous year. As the total cost of data breaches rise, the probability of an organization undergoing a data breach increases to a staggering 27.9%, with cybercrime ranking among the top three risks in the world by the World

Economic Forum. These numbers are staggering and grow costlier every day, with data security breaches impacting governments, financial corporations, credit card companies, telecoms and healthcare organizations.

While firewalls, data encryption and antivirus/anti-malware tools handle the logical side of data protection and security, the physical heart of our digital world – also known as the data centre – demands an exceptional level of protection, which can be achieved through a multi-layered approach to access control.

The Risks Keep Growing

As more personal information is pushed into the digital world, the risks and costs of data breaches continue to climb. According to the Breach Level Index, there were 1,765 publicly disclosed data breaches in 2017, leading to the successful theft or loss of 2.6 billion data records. To net it out, that equals approximately 4,949 records stolen every minute, or 82 records every second. Organizations found in violation of data regulations face costly consequences. This situation dramatically elevates the importance of physical protection and security for data centre managers. As

more businesses, governments and organizations move toward cloud-based data storage, regulatory bodies are placing a stronger emphasis on data protection, making it more important than ever for data centre managers to ensure that their security administration meets industry standards.

The Payment Card Industry Data Security Standard (PCI DSS) for instance, is regarded as one the most significant data protection standards in the IT industry today. PCI DSS is designed to protect the personal data of consumers and sets access control requirements for the entities that secure their information. The regulation calls for monitoring and tracking personnel who might have physical access to data or systems that house cardholder data. This access should be appropriately controlled and restricted. Personnel covered under PCI DSS include full- and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. The regulation also covers visitors, such as vendors and guests, who enter the facility for a short duration – usually up to one day.

But aren't most data breaches completed by outside hackers breaking in through firewalls and not by people within an organization? The data says otherwise. In many cases, according to research conducted by IBM, the next attack could be from within an organization. In 2015, 60 percent of all attacks were carried out by insiders—either those with malicious intent or those who served as inadvertent actors – by configuring a server incorrectly or leaving a port open on accident.

For the data centre manager, the benefits of compliance are two-fold. Compliance not only protects the confidential nature of the data stored within the data centre, it also protects the data centre from regulatory penalties and the added cost of lost productivity that may occur as a result of a data breach.

Securing Assets with EAS

Managing access to the data centre is becoming more complicated as data housing facilities continue to expand their hosting capabilities. From data centres housing information for a single organization to co-location data centres

where multiple companies are hosting their data in one location, traditional key management is becoming a significant challenge for facility managers. Personnel from one or several organizations may access the data centre at any given time, making key management increasingly difficult to track. Data centres typically have multiple layers of security and access control: at the front door of the building, then a man trap to get past the lobby, then access control to get into each data centre room, then possibly a cage depending on the data centre structure. However, it is at the rack level where data security and access control have the potential to fall short. If the servers are behind doors, there may not be physical locks securing those doors. And in older server farms, the server racks are wide open to all who have gained access to the cage that surrounds them. Thus, all of the physical layers of security can't prevent unauthorized or malicious attempts to access unsecured servers. And if there is an attack or data breach, it becomes more difficult to track down the "who, what, when and where" of the breach if there is no rack-level security and audit trail in place.

In response, data centre managers are focusing on extending physical security down to the rack level. Cabinet manufacturers are transitioning from traditional lock-and-key mechanisms to integrated solutions that combine electronic locking and monitoring capabilities for optimum security. These electronic access solutions (EAS) allow data centre managers to easily incorporate intelligent locking throughout the facility—from its perimeter down to its servers—using the data centre's existing security system integrating with newer DCIM systems or through a separate, fully-networked system.

The remote monitoring capabilities offered by electronic access solutions help data centre managers quickly identify a violation, enabling them to receive updates on their computer or via text or email on their personal devices. An electronic access solution is composed of three primary components: an access control reader or input device, an electromechanical lock and a controller system for restricting, monitoring and recording access. When designing an electronic access solution, it is important that the appropriate

Southco's Modular H3-EM Electronic Locking Swinghandle series provides the flexibility to accommodate any reader technology as an integral component of the electronic lock.

electronic lock is chosen for the specific enclosure and provides the intelligence, flexibility and security needed at the rack level. Electronic locks are actuated by external access control devices, which validate user credentials and produce a signal that initiates the unlocking cycle. Electronic locks can be combined with any access control device from keypads to radio frequency identification (RFID) card systems, biometrics or wireless systems. The access control device can also be integrated into the electronic lock for a streamlined, integrated solution that requires minimal installation preparations.

Each time an electronic lock is actuated, an electronic "signature" is created which is captured to monitor access–either locally with visual indicators or audible alarms, or remotely over a computer network. The electronic signatures can be stored to create audit trails that can be viewed at any time, whether on- or off-site, to forensically reconstruct a series of access events.

This electronic audit trail keeps track of cabinet access activity, including location, date, time, duration of access and specific user credentials. These audit trails provide data centre managers with an additional resource: They can track the amount of time a server rack door is opened in order to monitor maintenance and service activity. If a server rack is scheduled for activity that should take 30 minutes, but the audit trail shows the door was open for several hours, management can find out why the delay occurred and exercise better management of service personnel and costs for service.

This audit trail can be used to demonstrate compliance with data protection regulations and allows data centre managers to immediately identify and respond to security breaches or forensically reconstruct events leading to a violation. Remote management and real-time monitoring eliminates the

need for on-site staffing and reduces costs associated with managing data centre security. Support for Multifactor Authentication. When designing a new installation or retrofit, it is important to select an electronic lock based on the depth of intelligence and level of protection required.

Many EAS suppliers offer a range of electronic locking solutions designed to make implementing rack-level security relatively simple and cost-effective. These include robust cabinet locks integrated into locking door handles that are self-contained, modular devices designed to provide multifactor authentication in order to supply access to a server cabinet. Multifactor authentication is a growing requirement for many access control scenarios and more data centre managers are implementing it, particularly for server racks containing highly sensitive data. Common multifactor systems typically require the following factors:

- Something you know–such as a PIN
- Something you have–such as an RFID card
- Something you are–biometric data, such as a fingerprint or through facial recognition scans

With multifactor authentication, one piece of information alone does not grant access. An electronic lock can be designed to require the user to present an RFID card, and then enter a PIN code on a keypad. There are electronic locking systems that are designed to be modular, allowing different types of access controllers to be easily added to the lock and satisfying the specific level of security for a given server rack. The levels of safety can be further enhanced in a relatively simple manner. For example, there are electronic locking systems that combine RFID cards and fingerprint readers. Technicians assigned to access a server rack using this type of system have their fingerprint data loaded onto the card. To access the server, they

present their card which transmits their fingerprint data to the reader; they then provide their fingerprint to complete access.

Designing for Compliance

Electronic access solutions provide a strong level of physical access control for a variety of data centre security applications, whether providing storage for one organization or several housed in a colocation environment. Managers of colocation environments have started to adopt intelligent locking systems due to the challenges of protecting access to individual cabinets, rather than "caging" a cabinet or group of cabinets into separate areas of the data centre. Electronic access solutions are adaptable to both structural designs and control mechanisms that are already in place. Often, building access cards or ID badges are already part of an organization's access control system; using them for rack-level access eliminates the need to create new or separate credentials.

Conclusion

Expectations for data security and management have changed significantly. Regulations are driving facility managers to consider comprehensive security solutions with monitoring capabilities and digital audit trails to protect sensitive information from the threat of unauthorized access and theft. Regulatory requirements related to data security will continue to increase in response to the constantly changing tactics of data thieves. Data centre managers can prevent these situations from occurring by optimizing security down to the rack level with electronic access solutions. Electronic locks extend intelligent security from existing building security networks to data centre cabinets. As a result, data centre managers can ensure their facilities and equipment are protected against the risk of data breaches and any penalties associated with non-compliance.

> Each time an electronic lock is actuated, an electronic "signature" is created which is captured to monitor access–either locally with visual indicators or audible alarms, or remotely over a computer network

Top design considerations for the most secure data centre lighting solution

By Graeme Shaw, Technical Application Manager, Zumtobel

CLOUD, COLO, HYBRIDS – every data centre is unique, and as such, each facility will have its own layouts and requirements. Although specifications inevitably vary, there are often more similarities than differences when it comes to the equipment operators choose for their facility.

Data centre operators have come to expect that the products installed within their data hall meet certain criteria. Equipment should save power, be sustainably sourced, but most of all, it must be safe and secure. Operators are becoming increasingly more selective about the kind of products they allow in to their facilities. However, making a data centre campus as secure as possible does not necessarily begin and end with antivirus software and firewalls. Data centres face many threats besides cyber-attacks – theft, natural disasters, vandalism, man-made disasters and other incidents which can lead to lengthy repairs and potential downtime.

As a leading, global lighting manufacturer, we have partnered with a number of operators around the world to deliver best in class lighting within their data centres. For this reason, we understand the unique design challenges operators and specifiers face on a day to day basis. These challenges are exactly why we have channelled our experiences in to what we believe to be best practice, steering key design considerations and making the next design as futureproof as possible.

External lighting

High precision external lighting can help to fortify a facility's defences against such threats. Only by illuminating an outdoor space are you able to provide that feeling of reassurance that the grounds are safe and secure. This can also help with wayfinding as the lighting design works to shape and define the perimeter of a space, whilst providing guidance from one part of a campus to another. Conversely, data centres in urban locations can often be perceived as an eye sore. The right lighting can allow data centres to blend seamlessly with their surroundings making its appearance subtle or even unnoticeable. Like other businesses, data centre operators welcome their clients for tours around their facilities to showcase what they can offer. When you enter in to any corporate headquarters, you get a sense of that company's self-image. Why should a data centre be any different? By incorporating luminaires which are specifically designed to be used for that application, it provides an opportunity to project your brand's identity. This could be by lighting up a façade in your corporate colours or simply changing the finish of a fitting to suit your logo.

Emergency lighting

Emergency lighting systems are a critical part of any commercial building, data centres are no exception and must have a proven emergency lighting scheme. Along with a consistent and reliable power stream, your emergency lighting back-up system needs to provide power to the emergency luminaires for between 1 and 3 hours depending on the geographical location.

Central battery systems are often preferred as the system can be located in a battery or plant room where temperatures are either naturally lower or cooled to an ambient of around 20c. There is also the added advantage of being able to monitor and record any faults with a single point of contact. Since these batteries are located away from excess heat build-up, the lifetime often exceeds that of self-contained, local

DATA CENTRE ALLIANCE

systems. Not only does this present the operator with a longer battery life, it also reduces maintenance time and costs.

Ambient air temperature

The ambient air temperature of a facility is often considered one of the most important aspects of data centre design. Hot and cold aisles result in fluctuating temperatures and increasing pressure on any hardware found within a data hall. The first step is to determine if the luminaires being considered have been fully tested and have an appropriate ambient temperature rating for the environment. By opting for a fitting with the correct ambient temperature rating backed by independent test certification, it reduces the risk of system failures, unplanned maintenance costs and potential downtime.

Task lighting

Although data centres do not have the same occupation rate as traditional commercial businesses, technical

engineers need to monitor and work in close proximity to the servers. A well-lit working plane is crucial so that engineers can accurately record information and clearly see the task at hand. It is vital that the lighting system is designed to light the face of the servers, similar to a library where you are illuminating the spines of books to 500lux, for ease of identification. Advanced lens technology can be used to achieve vertical illumination which means light is positioned exactly where it is needed whilst avoiding unnecessary light spillage and conserving precious energy.

Modularity

The Data Centre Industry is growing fast and one of the key challenges facing Developers and Operators is how to build and scale at speed to meet client demand. Products which offer modular construction allow for greater design flexibility and enable

the build to progress piece by piece, increasing data storage capacity without compromising on time or value. Prefabricated sections constructed within off-site controlled manufacturing facilities has many advantages. It improves build consistency, decreases on-site install time as well as the amount of multi-skilled, site-based install teams in comparison to traditional methods of construction.

Lighting Control

Lighting control should be the rule rather than the exception as the right choice of highly efficient lighting coupled with an intelligent lighting control system will enable consistent monitoring of the installation and report any potential faults remotely. In addition, energy savings linked to the facility lighting can be reduced by a further 10% – 15% when LED luminaires are used in conjunction with sensors to manage when and where light is deployed, reducing operating time and unwanted heat gain.