



DIGITALISATION WORLD

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

ISSUE IX 2024

DIGITALISATIONWORLD.COM



**APT AND SCHNEIDER ELECTRIC
TRANSFORM
THE PIRBRIGHT INSTITUTE'S
DATA CENTRE TO FAST-TRACK
ADVANCED VIRAL RESEARCH**



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

APC[™]

40Years

Make greater

IMPACT

with an industry-leading network

Celebrate 40 years with APC.

Start leveraging four decades of uninterrupted protection, connectivity, and unparalleled reliability with the APC UPS family, a legacy marked by pioneering UPS technology and an unwavering commitment to innovation.



Life Is On

Schneider
Electric

VIEWPOINT

By Phil Alsop, Editor

The best of times, the worst of times

➤ The 2025 is likely to be a memorable year for any number of reasons. Whatever one's view of US politics, we can safely say that, once the new president is in office, life will not be dull...there are bits of evidence from his first time in office which support the most optimistic and pessimistic expectations as to what is in store for us in a Trumpian world.

Geopolitically, uncertainty remains, at least for now. If I remember my history correctly, the origins of the First World War tend not to cover any of the participants in particular glory – there seemed to be a collective complacency and lack of diplomacy that allowed the drift into war – all be it the Archduke's assassination was the apparent catalyst. Second time around, the final throes of global empire building were acted out, with a dictator hell bent on some kind of regional, if not global, domination. Right now, either of those scenarios could, depressingly, be repeated. There are individuals who fit the dictator mould, and there does seem to be a certain collective reluctance to engage with the trickier aspects of diplomacy in what's now a truly global economy. Then again, it would not take much for certain political tensions to ease and some kind of stability to return.

Climate-wise, such stability seems increasingly far off. The evidence for climate volatility seems overwhelming – such that, if a management consultant presented such a detailed document as to an emerging business trend to a client, it would be surprising to put it mildly if the client dismissed the report as scaremongering and did not adjust accordingly. Sustainability progress is being made – I'm just not sure whether at the right speed or right level. Until what might be called 'overconsumption' (how much of everything do we actually need?!!) is addressed, I am not sure that any plans to reach NetZero will be truly successful.

And talk of success brings us to the (continuing) story of the moment. On the face of it, AI can be an immense force for good in so many ways. Then again, it has the power, in the wrong hands, to do immense harm (and



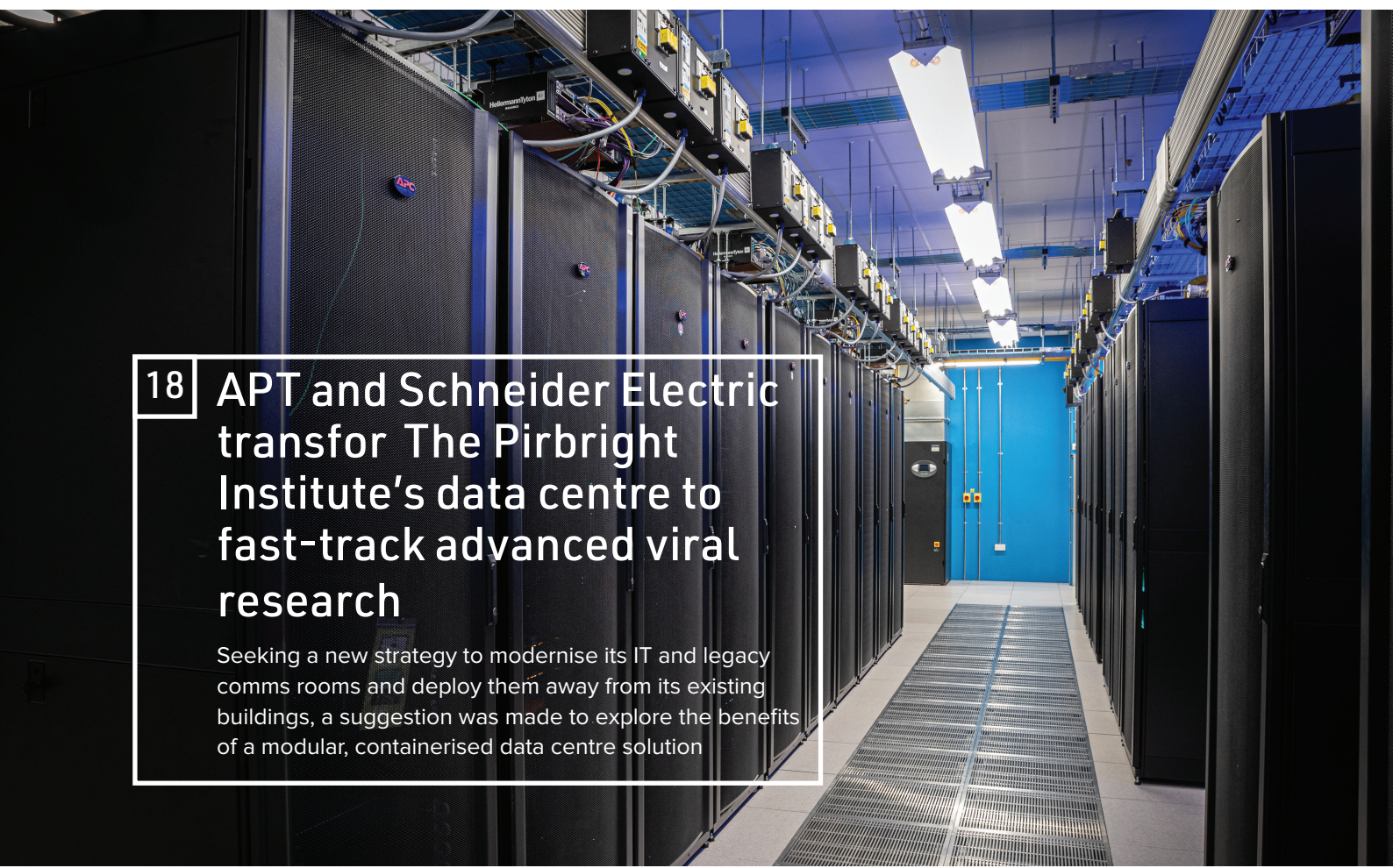
almost certainly already is). One thing is for sure, AI can't be ignored or shrugged off. It is here to stay. I'm fairly sceptical as to whether ethical AI can actually gain any traction – gearing in mind that ethical social media is already a comical concept.

All of which brings us to the very depressing fact that, increasingly, unelected individuals and the huge corporations they have built up and control seem to wield more power than most governments across the world. We all have the power to withdraw our support for many, if not all of them, yet choose not to do so. And here we are back to the apathy and complacency mentioned at the start of my comment.

My headline comes from the start of the Charles Dickens novel, *A Tale of Two Cities*, which is a powerful story set in and around the French Revolution. I shall leave folks to decide for themselves if we are rapidly heading for such another historical landmark, or whether the technology world in which we work can, somehow, enable the good and keep out the bad.

A Happy Festive Season to all!





18 APT and Schneider Electric transfer The Pirbright Institute's data centre to fast-track advanced viral research

Seeking a new strategy to modernise its IT and legacy comms rooms and deploy them away from its existing buildings, a suggestion was made to explore the benefits of a modular, containerised data centre solution

14 Only 48% of digital initiatives meet or exceed their business outcome targets

On average, only 48% of digital initiatives enterprise-wide meet or exceed their business outcome targets according to Gartner, Inc.'s annual global survey of more than 3,100 CIOs and technology executives, and more than 1,100 executive leaders outside of IT (CxOs)

22 The key steps business leaders must take to avoid AI projects failing

It's entirely understandable that business leaders have high expectations for artificial intelligence (AI) technology, and also that they should be impatient to get this technology to work

24 Data governance - laying the foundations for effective AI applications

While AI in one way or another has been integral to financial services for some time, it's now hard to think of any area of the industry the technology hasn't touched

26 Time to shine a light on shadow AI

Whilst companies are right to encourage their teams to find innovative usages of generative artificial intelligence (GenAI) to streamline workflows, many employees are using the technology in ways that are not being sanctioned by their employers

28 Navigating the surge of cyberthreats in healthcare

Malicious attacks on the healthcare industry have grown exponentially in recent years

30 Who are BISOs and what do they bring to the cybersecurity table?

The role of a Business Information Security Officer (BISO) is gaining traction in security communities and board conversations. But why do organisations need BISOs?

32 Who's responsible for digital trust?

Digital trust isn't merely a defence against the ever-present problems of privacy infringement, cybersecurity threats and technology failures - but a way to innovate and expand safely

34 Capitalising on your data with DataOps

Across every industry, companies continue to put increased focus on gathering data and finding innovative ways to garner actionable insights

36 A data-led approach to powering digital transformation

Digital transformation is already a reality for most organisations. But successful change management and a data-led approach can significantly enhance the chances of a smooth transition

38 Three-step strategy for making your tech investments work harder

By reassessing the role of technology in helping the business achieve its most pressing goals, IT decision-makers can ensure their investments make sense

40 A changing landscape for technology firms amidst the Ecodesign for Sustainable Product Regulation

The EU's initiative for a circular economy through the ESPR and mandating of DPPs marks a milestone commitment to lowering waste levels and provides hope for a more circular and sustainable economy

42 How insurgent financial services institutions are overtaking the giants of the sector

In a hyper-competitive environment, it is very often a company's ability to adopt new technology and turn it to profit quicker than their competitors which makes the key difference

44 Here's why nobody's really ready for NIS2

Despite being published in late 2022 and coming into effect in January 2023, the second Network and Information Security Directive (NIS2) is taking the European Union by surprise

NEWS

06 Human error is cybersecurity's weakest link

07 Ransomware survey reveals nearly a third of businesses suffered data loss in 2024

08 Research uncovers root causes of AI and automation implementation delays

09 Silos and inconsistency top list of data challenges for global IT leaders

10 Organisations are ramping up efforts to meet sustainability targets

11 One in three workers want AI banned from the workplace

12 Survey reveals CISO priorities for 2025



11

DW DIGITALISATION WORLD

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

Senior B2B Event & Media Executive
Mark Hinds
+44 (0)2476 718971
mark.hinds@angelbc.com

Marketing & Logistics Executive
Eve O'Sullivan
+44 (0)2476 823 123
eve.osullivan@angelbc.com

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

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

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

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

Directors
Scott Adams: CTO
Sukhi Bhadal: CEO

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

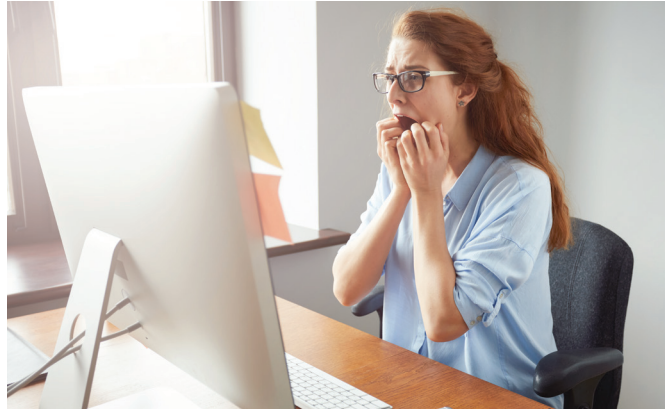
Angel 
BUSINESS COMMUNICATIONS

Digitalisation World is published 10 times a year on a controlled circulation basis in Europe, Middle East and Africa only. Subscription rates on request. All information herein is believed to be correct at time of going to press. The publisher does not accept responsibility for any errors and omissions. The views expressed in this publication are not necessarily those of the publisher. Every effort has been made to obtain copyright permission for the material contained in this publication. Angel Business Communications Ltd will be happy to acknowledge any copyright oversights in a subsequent issue of the publication. Angel Business Communications Ltd.
© Copyright 2024. All rights reserved. Contents may not be reproduced in whole or part without the written consent of the publishers. The paper used within this magazine is produced by chain of custody certified manufacturers, guaranteeing sustainable sourcing. ISSN 2396-9016 (Online)

Human error is cybersecurity's weakest link

Kaseya has released the results of its 2024 Kaseya Security Survey. IT professionals reported user behavior as their biggest cybersecurity challenge.

ANOTHER IMPORTANT finding relates to the widespread adoption of artificial intelligence by both threat actors and defenders. The survey found that feelings are mixed as IT professionals learn to navigate this new industry game-changer. The results of the survey are featured in the Cybersecurity Survey Report 2024: Navigating the New Frontier of Cyber Challenges.



“Cybersecurity attacks are widespread and more sophisticated, and as a result, are shaping business and IT strategies,” said Chris McKie, VP, Product Marketing-Security at Kaseya. “IT professionals are navigating this new frontier as they try to find a balance between cybersecurity needs against hybrid workforces, dependency on cloud-based applications and services, and the role of artificial intelligence in cyberattacks.”

People are the Problem

An alarming 89% of respondents cited a lack of training or bad user behavior as their main cybersecurity problem. User-related security issues cause the most distress for IT professionals with poor user practices and gullibility (45%) and lack of end-user cybersecurity training (44%) as the root causes for cybersecurity problems. When asked which cybersecurity issues have impacted their business, phishing ranked first at 58%, followed by computer viruses or malware at 44% and business email compromise at 34%.

AI – All Hype?

Cybercriminals are leveraging advances in AI technology to launch more sophisticated cyberattacks at a faster pace than ever before. However, its role

in cybersecurity is highly debated with critics questioning its current limitations and ever-evolving cybercriminal tactics. More than half of survey participants say they believe AI will help them be more secure. But one-third of the IT professionals surveyed said they're unsure about the impact AI may have on their company's security. More research and clarity around the benefits and limitations of AI as a cybersecurity tool is needed.

Ransomware Payouts Decline

The survey found that fewer companies are paying ransomware demands – with only 11% claiming to have done so. The reason? Increased investment in backup and recovery technologies have likely minimized the impact of attacks showing the importance of these tools as part of robust backup and disaster recovery strategies. A growing awareness that paying the ransom is poor practice may be another reason.

Tools to Fight Cybercrime

According to the survey, the most widely adopted cybersecurity frameworks are NIST (40%) and Zero Trust (36%). There is a trend in rising security maturity in response to increasingly sophisticated threats. Respondents have rigorously implemented an array of security solutions with antivirus software (87%),

email/spam protection (79%), and file backup (70%) topping the list. Three out of five respondents have an incident response (IR) plan in place – but follow-through is needed. Only 37% of those surveyed reported that they confirm the efficacy of their plan with periodic drills, down from 46% last year.

Another weapon in the fight against cybercrime is pentesting. More than two-

thirds of respondents test at least twice per year, and more than one-third test at least three times each year. The major challenges around pentest adoption are cost and lack of budget (58%), resource limitations (18%) and IT staffing issues (12%).

As cyberattacks have risen, so has the adoption of cyber insurance with coverage now at 61% compared to 27% in 2023. Moreover, 41% of organizations are planning to invest in cyber insurance in the next 12 months.

Investments in Cybersecurity

IT budgets are stable. Over 80% of respondents said that they believe their IT security budget will remain the same, or even grow, in the next year. Aside from cyber insurance, IT professionals anticipate investing in cybersecurity, specifically cloud security (33%), automated pentesting (27%), network security (26%), security awareness training (26%) and vulnerability assessment (26%). Endpoint detection and response (EDR) and managed SOC/MDR also were on the list.

The IT professionals surveyed had headquarters in North America (87%), UK & EU (9%) and APAC/NZ (3%). Most of their company's annual revenue ranged from \$1M to \$10M, and had 101- to 500 employees.

Ransomware survey reveals nearly a third of businesses suffered data loss in 2024

Number of ransomware victims paying a ransom more than doubles over past year.

THE NUMBER of ransomware victims who paid a ransom in 2024 (16.3%) more than doubled on the previous year (6.9%), according to new research from leading cybersecurity provider Hornetsecurity. Data loss has also increased dramatically, from 17.2% in 2023 to 30.2% in 2024. Alarmingly, 5% of organizations reported a complete loss of all affected data.

These worrying trends come as data recovery rates have hit a new low. The increasing sophistication of cyberattacks has meant that the data recovery rate for businesses hit by ransomware has dropped from 87.4% in 2021 to just 66.3% this year.

The survey also revealed that email and phishing attacks remain the most common vector of attack for ransomware, responsible for 52.3% of attacks. Despite a slight reduction in attack volume from 21.1% in 2021 to 18.6% in 2024, the severity of these criminal behaviours has increased.

Commenting on the findings, Hornetsecurity CEO Daniel Hofmann said: "The evolving landscape of ransomware threats highlights the need for constant vigilance. The data shows that while fewer attacks are being reported, the outcomes are far more damaging, with potentially devastating consequences for organizations that fall victim to them.

"Criminals are constantly shifting tactics, and organizations of all sizes must invest in comprehensive security measures and ongoing cybersecurity awareness training to stay protected." Generative AI: a double-edged sword.

The rise of generative AI technology has heightened fears of ransomware, with two-thirds (66.9%) of respondents indicating that AI has increased their

apprehension about potential attacks. This comes as general concerns about ransomware remain high, with nearly 85% of companies expressing moderate to extreme worry. While 89.4% of businesses acknowledge their senior leadership's awareness of ransomware risks, only 56.3% report that leadership is actively engaged in prevention strategies. Additionally, 39.2% are content to leave the issue primarily to IT departments.

The survey showed 84.1% of respondents view ransomware protection as a top IT priority, and 87% have established disaster recovery plans - and while this represents the majority, there are some concerns around the organizations that do not prioritize ransomware given its potentially ruinous consequences on a business's operations.

When it comes to the 'why', one reason might be that some people (13.1%) mistakenly believe reliance on platforms like Microsoft 365 or Google Workspace negates the need for a formal plan.

Training in cybersecurity: urgent refreshes required

Despite 95.8% of respondents acknowledging the value of cybersecurity training, several concerns and misconceptions persist. The main issue is the time commitment, with 17.8% of respondents believing it is too demanding.

Additional feedback includes the perception that users are 'untrainable' (14.4%), the high cost of training (12.3%), and the significant time burden on IT staff (10.6%). A smaller proportion (7.6%) view training as outdated.

Hornetsecurity's research shows just over half (52.3%) of ransomware



attacks stem from email and phishing attempts - and breaches of the human firewall. This shows the urgent need to overcome resistance to training, as employees are the first line of defence against cyber threats. To maintain effective security and adapt to evolving cybercriminal tactics, continuous and evolving training is essential.

Awareness and insurance trends
Awareness of the impact of ransomware on Microsoft 365 data has improved significantly, with only 9.8% of respondents now uncertain about its vulnerability, down from 25.3% in 2022.

In addition to this, the uptake of ransomware insurance has increased markedly, with 54.6% of organizations purchasing coverage in 2024, up from 37.9% in 2022.

Daniel Hofmann added: "Generative AI is a game-changer in ransomware, making attacks smarter and organizations understandably more nervous. It's promising to see more businesses taking up ransomware insurance, but awareness isn't enough. Next-gen, AI-powered cybersecurity solutions are a crucial step in the battle against cybercriminals, but it is clear that organizations also need strong leadership, robust and engaging training, and constant vigilance to stay one step ahead."

Research uncovers root causes of AI and automation implementation delays

99.7% of organizations recognize AI's potential to overcome IT challenges and drive efficiency, but gap between interest and execution persists.

SCIENCELOGIC has unveiled the results of comprehensive enterprise IT research with the publication of its whitepaper, "The Future of AI in IT Operations: Benefits and Challenges." Commissioned by ScienceLogic and conducted by Vanson Bourne, the study uncovers the driving factors behind the challenges to effective AI/ML deployments that create the data and observability infrastructure necessary to support generative AI (GenAI) capabilities.

The increasing complexity of IT environments and data proliferation is outpacing human capacity, necessitating a shift towards automated, intelligent capabilities that enhance visibility, streamline issue identification, and accelerate resolution times.

This automation allows IT teams to focus on delivering cutting-edge business services in a competitive landscape while paving the way for GenAI implementation. These

advanced AI systems provide context-aware insights and actionable recommendations, enabling proactive issue prevention and resource optimization. However, effective GenAI deployment relies on first successfully leveraging traditional AI/ML for IT operations (AIOps), forming a foundation for more advanced AI-driven innovations.

Key findings of "The Future of AI in IT Operations":

Benefits and Challenges" include:

- Effective IT monitoring, a foundational component of AIOps, remains a challenge across organizations.
- 50% of organizations use multiple, disparate tools to monitor resources, resulting in data silos, longer incident response times, and a fragmented user experience.
- 47% of surveyed organizations are unable to map all of their on-premises, cloud, and edge devices

into a single business view, despite monitoring a large range of IT systems and services.

- 39% of organizations are prioritizing the consolidation of IT monitoring tools, as creating a consolidated monitoring environment becomes a key strategic focus.

Organizations need comprehensive observability and clear data

management to automate using AI/ML.

- 38% cite inability to monitor all IT resources as a barrier to AIOps adoption, highlighting the importance of a holistic IT estate view for effective AI implementation.
- 39% struggle to automate complex repair workflows due to lack of critical context, exacerbating visibility challenges across the IT estate.
- 50% acknowledge security concerns as a barrier to AIOps adoption, potentially addressable through proper data management and governance policies.

Risk appetites have grown for 81% of CISOs

NETSKOPE has published a new report analyzing the evolution of the CISO role within the retail sector. 'The Retail CISO: Bringing Balance', is based on research with over 1,000 CISOs globally, and it explores the evolution of the retail sector CISO role as a strategic member of the executive team, comparing the sector to cross-sector averages to identify unique insights.

81% of retail CISOs say their appetite for risk has grown in recent years (much higher than the cross-sector average of 57%), but all (100%) believe conflicting risk appetites in the C-suite are a major issue.

Less than 2% of retail sector CISOs classify their risk appetite as low. However, nearly a quarter (23%) would

describe their CEOs' risk appetite as low. Retail CISOs see interactions with the C-suite and business as a constant balancing act, with 47% reporting that most interactions are about risk and 53% countering that most are about opportunity.

An overwhelming majority (98%) of retail CISOs now consider themselves to be business enablers (well above the cross-sector average of 59%), and more than four-fifths (87%) want to play a more active role as a business enabler going forward (compared to an average of 67%). 86% of retail CISOs increasingly see their role as improving business resilience, not just managing cyber risk. Retail CISOs are clear that they want to embrace more measured,

centralized decision-making processes knowing the high levels of governance involved.

This again contrasts with all other sectors who saw themselves moving the other way—drawn to a model described as "agile, fast decision-making with devolved responsibility".

One of the pathways identified by retail CISOs for achieving the sometimes conflicting goals of the C-suite is adopting a zero trust approach. More than two-thirds (72%) believe zero trust will help them balance conflicting priorities better (higher than cross-sector averages of 55%), enable their organizations to move faster (77%) and encourage more innovation (71%).

Silos and inconsistency top list of data challenges for global IT leaders

New research from Confluent sees IT leaders share their biggest data challenges.

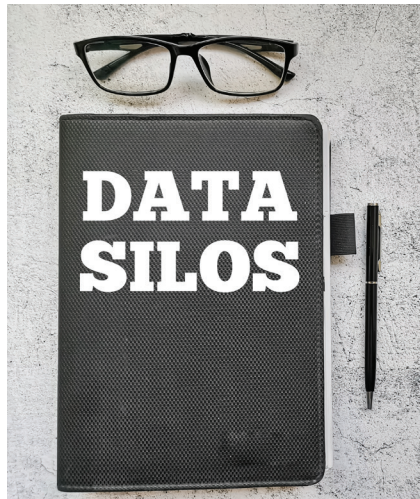
DATA SILOS are the #1 challenge currently facing global IT leaders when it comes to their data strategy and implementation. That's according to newly released research from Confluent, which surveyed 4000 global IT leaders on their biggest IT challenges.

It found that 69% of IT leaders believe "data spread across silos" is a major challenge for their organisations and a key focus area.

According to Confluent's data, the top three data challenges for IT leaders around the world include:

- Data spread across silos (69%)
- Inconsistency of data (68%)
- Timeliness and quality of data (62%)

As a result of these challenges, many IT leaders are rethinking their approach to data, switching from disjointed batch processing to real-time streaming. Half of leaders (50%) say data streaming



technologies are now a top strategic priority, while a further 34% say they are an important secondary priority.

Those already using data streaming confirm the benefits of this approach, with 60% saying this change in approach is already enabling more

data-driven operational decisions. A further 35% expect similar benefits in the next 12 months.

Commenting on the research, Richard Jones, data expert at Confluent said, "Most organisations struggle with the same data problems.

The complexity of maximising data's value is a constant challenge, whether it's accessing, analysing, or simply understanding it.

"Through data streaming, IT and data teams can tackle these challenges right across the organisation.

Real-time access to the right data exactly when it's needed will avoid and break down silos, promote visibility across the business, and enable better data governance. It's a data approach that's becoming critical as the use of AI continues to skyrocket and regulations evolve to protect the user, business, and consumer or customer data."

Stressed, anxious, excited – CIOs' state of mind in 2024

60% of global respondents say their focus on AI has boosted their personal reputation.

Technology leaders from large global enterprises are feeling the pressure as AI becomes a major force of innovation and disruption, according to the IDC InfoBrief, commissioned by Expereo, Enterprise Horizons 2024: Technology Leaders' Priorities on Their Digital Business Journey*, which reveals that 64% of global respondents find it challenging and/or stressful to meet the technology demands of the business, and that AI is a key source of both pressure and opportunity. The paper reveals that AI has raised the profile and expectations of technology leaders

at board level – a double-edged sword for many senior technology decision-makers. While 60% of global respondents say their focus on AI has boosted their personal reputation, 47% also say their board has unrealistic demands regarding the impact of AI on international business performance and 39% felt their job is more stressful or negative because of their added profile.

The perceived impact of AI on the workforce, both within and outside of IT, could be partly causing this 'AI-anxiety'. While the emergence of a Chief AI Officer role could bring businesses new opportunities, 40% of technology leaders say a CAIO role will take over

much of the CIO's responsibilities within two years, and 38% of them are worried that AI could replace their or their team's role. Moreover, 46% of global respondents believe increased automation will also result in some roles outside of IT being displaced.

CIOs remain excited, despite challenges. However, technology leaders are also excited about the pace of technology innovation. The survey shows that 68% of global respondents say this is the most exciting time to be a technology leader, and 71% of them are confident that they or their team can support growth and efficiency gains through their current technology strategy.

Organisations are ramping up efforts to meet sustainability targets

69% of executives say that anticipating stricter future regulations is a key driver of sustainability initiatives, up from 57% last year.

ORGANISATIONS continue to make progress in their sustainability initiatives, despite facing geopolitical challenges. Regulation and technology are proving to be a vital part of this progress, with two thirds of executives agreeing that their organisation will never be able to achieve its sustainability goals without climate tech.

This is according to the Capgemini Research Institute's latest report, 'A world in balance 2024: Accelerating sustainability amidst geopolitical challenges', which tracks advancements in organisations' environmental and social sustainability over the last three years. The third edition of the report highlights marked improvements in circularity, sustainable design, measurement, water stewardship, biodiversity, and sustainability skilling, despite shortfalls in tackling Scope 3 emissions and consumer skepticism.

Collectively, organisations are ramping up their efforts to meet their sustainability targets, and their maturity in adopting sustainable practices has increased steadily since 2022. 84% of executives this year say their organisation is on target to meet its carbon emissions goals; less than a tenth say they are behind. As organisations look to minimise their impact on the environment, progress is particularly visible in terms of circularity, sustainable product design, measurement, and water management. For instance, nearly three quarters of executives say that recycling products is a core aspect of their manufacturing strategy, up from 53% in 2022, while over two thirds said they were redesigning products to remove fossil fuel feedstock sources, up from less than half in 2022. In addition, three-quarters of executives have implemented a water-stewardship program, up from 55% in 2022.



In late 2023, executives were planning to increase investments in sustainability this year. However, companies have not followed through: average annual investment in sustainability initiatives and practices now stands at 0.82% of total revenue, down from 0.92% in 2023.

"This year's report shows sustainability projects continuing to build momentum in 2024 despite current headwinds," said Cyril Garcia, Capgemini's Head of Global Sustainability Services and Corporate Responsibility and Group Executive Board Member. "Business leaders have the power and the responsibility to steer us towards a more sustainable economy."

Water stewardship, biodiversity preservation, and circular practices are now established as key business imperatives. Executives are being very pragmatic, and CO2 reduction must now be translated into cost savings. We continue to see sustainability efforts bolstered by new climate tech innovations and regulations. The best way to build trust and credibility with consumers is by demonstrating tangible outcomes and planning for a future with sustainability at its heart."

Consumers unconvinced about progress

Consumers want to see corporations going even further and demand transparency. The report finds three-quarters of consumers expecting corporations to play a larger role in

reducing GHG emissions in 2024. Furthermore, even as organisations ramp up sustainability initiatives, consumers are more skeptical than ever about corporate sustainability, as more than half believe that organisations are greenwashing their sustainability initiatives, up from 33% in 2023. Geopolitics and regulations impacting corporate sustainability initiatives. Executives pointed to climate-related regulations as a key driver of sustainability projects. A full three-quarters of executives believe that sustainability regulation is necessary to achieve global climate goals, and nearly two thirds even agree that without regulation, their organisation would not have launched many environmental sustainability initiatives. Globally, 73% of executives agree that the EU's Corporate Sustainability Reporting Directive (CSRD) is honing sustainability measurement and tracking capabilities. However, organisations continue to fall short in terms of reporting on sustainability initiatives, especially on Scope 3 emissions.

Among organisations required to report for CSRD in 2025, just over a third say that they are prepared to report Scope 3 downstream emissions next year, while 86% are prepared for Scope 1. Meanwhile, tensions such as US-China relations, the wars in Ukraine and the Middle East, and the European energy crisis, are leading to disruption to supply chains and business operations, and uncertainty around government funding. This year, nearly two thirds of executives pointed to geopolitics as an increasing consideration in sustainability investments, and 69% are concerned about the impact of the uncertain US political scene. This is felt across countries, but Swedish executives are most concerned (75%), compared with 71% of US executives and 59% of executives in India.

One in three workers want AI banned from the workplace

New research from CYPHER Learning warns that women, over 55's, and clerical or manual workers believe the AI race puts them at risk.

CYPHER Learning has released a new study on workers' concerns and aspirations around using AI in the workplace. The study found that while AI is reshaping job roles in a positive way to remove repetitive tasks, workplace digital divides between ages, gender and seniority are deepening.

CYPHER Learning surveyed 4,543 workers aged 18 and above, from a cross-section of industries across the US, UK and Mexico, and found:

Reshaping of Roles: 63% of workers say the introduction of AI technologies has already impacted the skills required to perform their role, while over half (52%) believe it will either 'totally transform' or have a 'major impact' on their role within two years. Consequently, 38% expect they will need to retrain as their jobs will become obsolete and almost half (45%) are concerned about their future job security.

Cautious Optimism: Despite the upheaval, many workers felt positive about the changes. 67% of workers view AI as a 'friend' rather than a foe. Moreover, 41% of workers use GenAI for their work, with 46% saying that AI as a whole is making their jobs easier, and 43% noting that it's taking away boring administrative tasks so they can focus on more high-value work.

AI Digital Divides: Yet not all workers are equally benefiting from AI. Younger workers, men, and senior management are more likely to use AI at work and enjoy experimenting with AI, compared to women, over 55, and manual or clerical workers. Similarly, fewer women, older workers and manual or clerical workers felt technology is changing their roles for the better.

Lack of Guidance: Workers also felt clearer guidance is needed around use of AI in the workplace, with 69% feeling

clear AI policies are still needed – while one in three (33%) think the use of AI in the workplace should be banned entirely. Interestingly, one in four (25%) workers admit to using AI without their boss's knowledge.

"Each technological leap – such as we are currently experiencing with AI – does change the workplace," explains Graham Glass, Founder and CEO, CYPHER Learning. "Trade-offs have had to be made throughout history as jobs and roles shift. But over the long term these changes generally prove to be for the better."

Michael Rochelle, Chief Strategy Officer and Principal HCM Analyst at Brandon Hall Group adds: "Artificial intelligence is not just about automation—it's about augmentation. Brandon Hall Group research underscores AI's ability to enhance the workforce by freeing employees from mundane tasks and empowering them to focus on more strategic, creative endeavors. The true value of AI lies in its ability to enrich the employee experience and provide actionable insights that elevate organizational performance. CYPHER Learning's report highlights a key issue: all employees should have the opportunity to benefit from training and support to maximize AI's value in the workforce." With the influence of AI on the workforce expected to grow in the coming years, 73% of workers believe AI skills will be important to their role within five years – with 45% believing such skills will be 'essential' or 'very important'. However, only 25% have had training in this area. Again, workforce divides were apparent:

- Only 11% of workers over 55 have had AI training, compared to 30% of those aged 18 to 44.
- More men than women report exposure to AI training – 36% compared to 18%.



- Senior management have had more training than anyone else – 58%, compared to 11% of clerical or manual workers.

The survey also revealed frustrations and concerns around how technology training is delivered at present. Nearly half of workers (48%) worry about their company's future due to a lack of leadership investment in new technology skills. Moreover, 46% of workers said they find it impossible to keep up with the tech and digital skills required for their roles, and 53% say their tech training quickly becomes outdated.

"As AI increasingly permeates the workplace, fostering a culture of continuous learning through training and education will be essential to boost worker confidence," Glass concludes. "Some workers may feel overwhelmed by technology when training is not delivered in a way that is relevant to them and their role. For example, helping people understand the purpose of AI, and how to assess and validate outputs, will be more useful to some workers than extensive training in prompt engineering. When training is delivered in ways applicable to each individual and their role, at the right time in the right context, it's more likely to help them progress."

Survey reveals CISO priorities for 2025

CISOs around the world acknowledge waning confidence in securing today's hybrid cloud infrastructure, shifting focus toward gaining visibility into all data-in-motion.

Gigamon has unveiled priorities for global CISOs going into the new year, highlighting the challenges that come with today's tightening budgets and increasingly sophisticated cyber threats.

The Gigamon "CISO Insights: Closing the Cybersecurity Preparedness Gap" report, based on the company's 2024 Hybrid Cloud Security Survey, highlights the current state of cybersecurity based on responses from 234 CISOs in Australia, France, Germany, Singapore, UK, and the USA.

The Gigamon report data reveals a widening security gap, with CISOs falling behind as cybercriminals outpace their organization's cybersecurity defenses. Despite global information security spending projected to reach \$215 billion in 2024, nearly half (44 percent) of CISOs surveyed reported they were unable to detect a data breach in the last 12 months using existing security tools. CISOs identified blind spots as a key issue, with 70 percent of CISOs stating their existing security tools are not as effective as they could be when it comes to detecting breaches due to limited visibility.

"Modern cybersecurity is about differentiating between acceptable and unacceptable risk," says Chaim Mazal, CSO at Gigamon. "Our research shows where CISOs are drawing that line, highlighting the critical importance of visibility into all data-in-motion to secure complex hybrid cloud infrastructure against today's emerging threats. It's clear current approaches aren't keeping pace, which is why CISOs must reevaluate tool stacks and reprioritize investments and resources to more confidently secure their infrastructure."

As organizations revisit security strategies this Cybersecurity Awareness Month, the Gigamon survey data highlights the following focus areas



CISOs are prioritizing as they plan for 2025:

Gain Visibility into Data-in-Motion

Blind spots across hybrid cloud infrastructure are a top concern for 8 out of 10 CISOs, with 81 percent agreeing that cloud security is dependent upon gaining complete visibility into all data-in-motion. This includes visibility into lateral (East West) traffic and encrypted traffic, where 93 percent of malware hides today, creating a perfect opportunity for cyber criminals to breach a network. As a result, gaining visibility into encrypted traffic was listed as a priority for 84 percent of CISOs.

Optimize Existing Security Investments

Overinvestment in new security tools has led security teams to struggle with sprawling tool stacks. Coupled with the growing costs associated with data storage and management, CISOs are under immense pressure to optimize their existing security investments. Three-quarters of CISOs (76 percent) report being overwhelmed by the increasing volume of threats detected from a growing number of tools on an increasing number of assets. As a result, 6 in 10 CISOs listed tool consolidation and optimization as their number one priority for remediating blind spots.

Support AI Investments to Counter Growing AI Cyber Threats

CISOs are increasingly concerned about the potential for AI to fuel the growth of global ransomware threats, with 83 percent expecting a

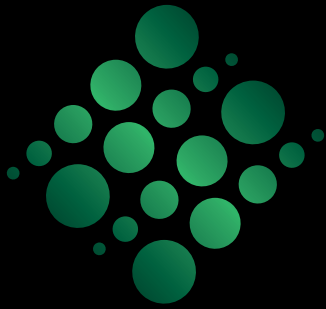
significant impact in the coming year. While deepfakes have garnered much attention, the more pressing threat is the volume and quality of cyberattacks that AI can enable. AI is empowering novice attackers with advanced capabilities and accelerating the discovery of exploitation techniques, underscoring the need for greater, more comprehensive visibility. Nearly half (46 percent) of CISOs will use security automation and implement AI to remediate visibility gaps.

Achieve Deep Observability Across Cloud Infrastructure

As CISOs evaluate increasingly complex hybrid cloud environments, greater visibility is the common goal, with 82 percent agreeing that deep observability – the ability to deliver network-derived intelligence and analysis to cloud, security, and observability tools – is a foundational element of cloud security. Deep observability goes beyond traditional monitoring, providing real-time insights into all network traffic based on network telemetry, including encrypted data and lateral traffic. This comprehensive view is crucial for identifying and mitigating cyber threats in real-time, which is why 85 percent of CISOs agree that having access to packet-level data and rich application metadata can unlock deeper insights, strengthening security posture.

The importance of this comprehensive visibility is also reaching the boardroom, with 81 percent of CISOs reporting that their boards are discussing deep observability as a priority to better secure and manage hybrid cloud infrastructure, reinforcing its importance for 2025 budget planning.

"Today's CISOs recognize that security and observability are intrinsically connected," said Stephen Elliott, group vice president, IT Operations, Observability, and CloudOps at IDC.



DCS AWARDS 2025

22 MAY

Leonardo Royal Hotel
London St Pauls

CELEBRATING 15 YEARS OF SUCCESS
The DCS Awards: 38 Categories across 5 Themes



KEY DATES:

14 FEBRUARY: NOMINATIONS CLOSE

21 MARCH: SHORTLIST ANNOUNCED

24 MARCH: VOTING OPENS

23 APRIL: VOTING CLOSES

22 MAY: AWARDS CEREMONY

NOMINATE NOW!

SPONSORSHIP PACKAGES

The DCS Awards offer extensive branding and sponsorship opportunities through online advertising in our Datacentre Solutions & Digitalisation World publications, and of course at the awards ceremony itself.



For sponsorship opportunities and/or to book your awards table please contact: awards@dcsawards.com or call +44 (0)2476 718970

NOMINATE: <https://dcsawards.com/nominate>

Supported by



The
data centre
trade association

Only 48% of digital initiatives meet or exceed their business outcome targets

On average, only 48% of digital initiatives enterprise-wide meet or exceed their business outcome targets according to Gartner, Inc.'s annual global survey of more than 3,100 CIOs and technology executives, and more than 1,100 executive leaders outside of IT (CxOs). A small cohort of CIOs and CxOs, known as the "Digital Vanguard," has the highest achievement rate, where 71% of their digital initiatives meet or exceed outcome targets.



"THIS DIGITAL VANGUARD distinguishes themselves from the rest of CIOs and CxOs because they co-own digital delivery," said Raf Gelders, VP, Research at Gartner. "CIOs and CxOs are equally responsible, accountable and involved in delivering the digital solutions their enterprises need. This is a radical departure from the traditional paradigm of IT delivery and business 'project sponsorship' that predominates in most enterprises."

Gartner analysts presented the survey findings during the recent Gartner IT Symposium/Xpo. The 2025 Gartner CIO and Technology Executive Survey gathered data from 3,186 CIOs and technology executives in 88 countries and all major industries, representing approximately \$17.6 trillion in revenue/public-sector budgets and \$351 billion in IT spending. This survey was supplemented with insights from 1,126 executive leaders outside of IT (CXOs).

Digital vanguard CxOs distinguish themselves from other CxOs because they dedicate more of their personal time and resources to digital delivery. They co-own digital delivery end to end with their CIOs, as well as dedicate 35% of their business area staff to do technology work (vs 21% of the rest of CxOs). They also work very closely with IT, meeting with

their CIOs four times more often than the rest of CxOs.

"Behind every digital vanguard CxO, a digital vanguard CIO is guiding and enabling CxOs and their teams to co-lead and co-build digital delivery with IT," said Jaime Capella, Distinguished VP, Research at Gartner. "Digital vanguard CIOs nurture their peers to become digital vanguard CxOs. Those CIOs make it easier for their CxOs to lead digital with them and for business area staff to build digital solutions together with IT.

"CIOs' success now depends on their CxOs' success," continued Capella. "To succeed at the next phase of digital initiatives, CIOs need their CxOs to work together and co-lead with them. So their fortunes are intertwined: one cannot succeed without the other."

CIOs Seek Compelling, Easy-to-Use Platforms for All Technologists

Over 80% of CIOs polled in the 2025 CIO and Technology Executive Survey said they expect to increase their investments in 2025 in strong foundational capabilities and technologies such as cybersecurity, AI/GenAI, business intelligence and data analytics, or integration technologies/APIs (see Figure 1).

“Digital vanguard CIOs do not invest in these technologies to be used by their IT staff only. They also make them easy to use for potential or actual technologists outside of IT,” said Gelders. “On average, there is 26% of business/corporate area staff outside of IT dedicated to building, implementing or managing technology. Many of these technologies naturally lend themselves to easing the burden of work enterprise-wide, accelerating time-to-market and time-to-value, and fostering the accountability of CxOs.”

At the other end of the spectrum, 43% of CIOs said they expect to decrease their investment in legacy infrastructure and data center technologies. This is a trend that has become more common in recent years, mainly due to migrating to cloud-based solutions. That compares with 33% who said they expect to increase it, which can be attributed, in part, to those organizations that acquired on-premise infrastructure to experiment and produce GenAI solutions.

CIOs Look to Develop Tech and Digital Leadership Skills for All Technologists Across the Enterprise Only 16% of CIOs surveyed prioritize building a technology workforce enterprise-wide (beyond their own IT departments) in 2025. That will limit the enterprise’s ability to get the most from their digital investments. It condemns them to perpetuate the low number (48%) of digital initiatives that meet or exceed their business outcome targets. Furthermore, just 18% of CIOs said they will prioritize sharing technology leadership with other business areas, a paramount must-have to grow the digital vanguard (see Figure 2).

“Digital vanguard CIOs plan the needs of digital skills not just for IT staff but also for all potential and actual technologists across the enterprise,” said Gelders.

Two-thirds of digital vanguard CIOs (vs 22% of the rest of CIOs) go beyond that and help business areas forecast their own needs of digital skills among business staff.

Worldwide IT spending to grow 9.3% in 2025

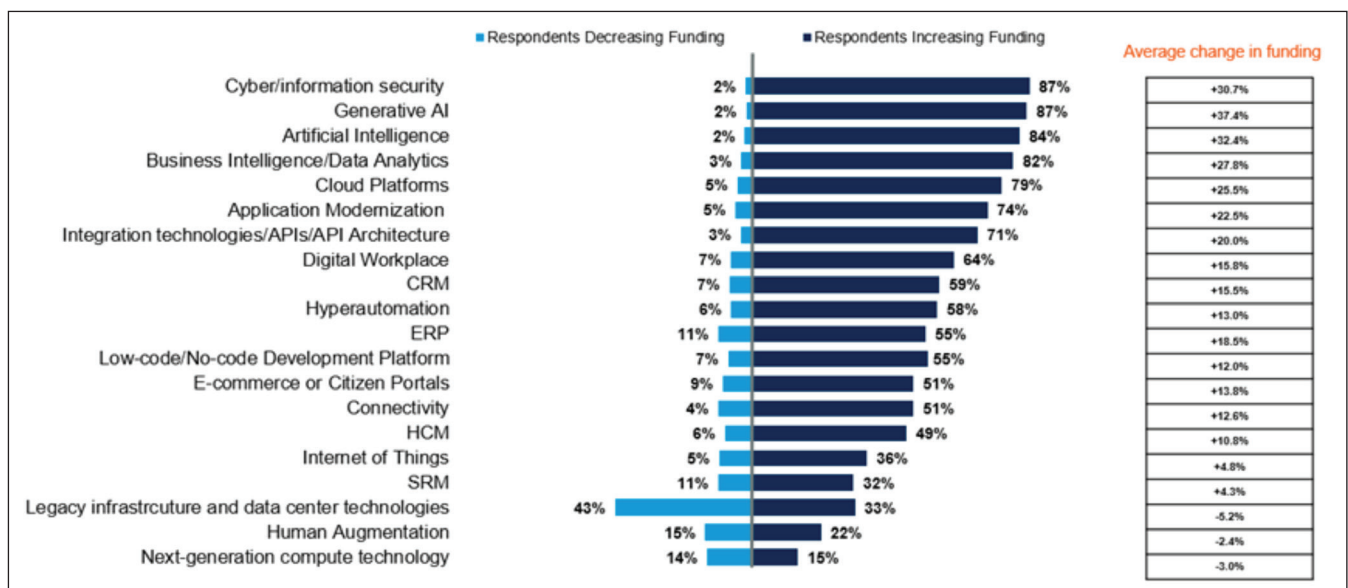
Worldwide IT spending is expected to total \$5.74 trillion in 2025, an increase of 9.3% from 2024, according to the latest forecast by Gartner, Inc. “Current spending on generative AI (GenAI) has been predominantly from technology companies building the supply-side infrastructure for GenAI,” said John-David Lovelock, Distinguished VP Analyst at Gartner. “CIOs will begin to spend on GenAI, beyond proof-of-concept work, starting in 2025. More money will be spent, but the expectations that CIOs have for the capabilities of GenAI will drop. The reality of what can be accomplished with current GenAI models, and the state of CIO’s data will not meet today’s lofty expectations.”

Server Sales Continue to Drive the Data Center Systems Segment

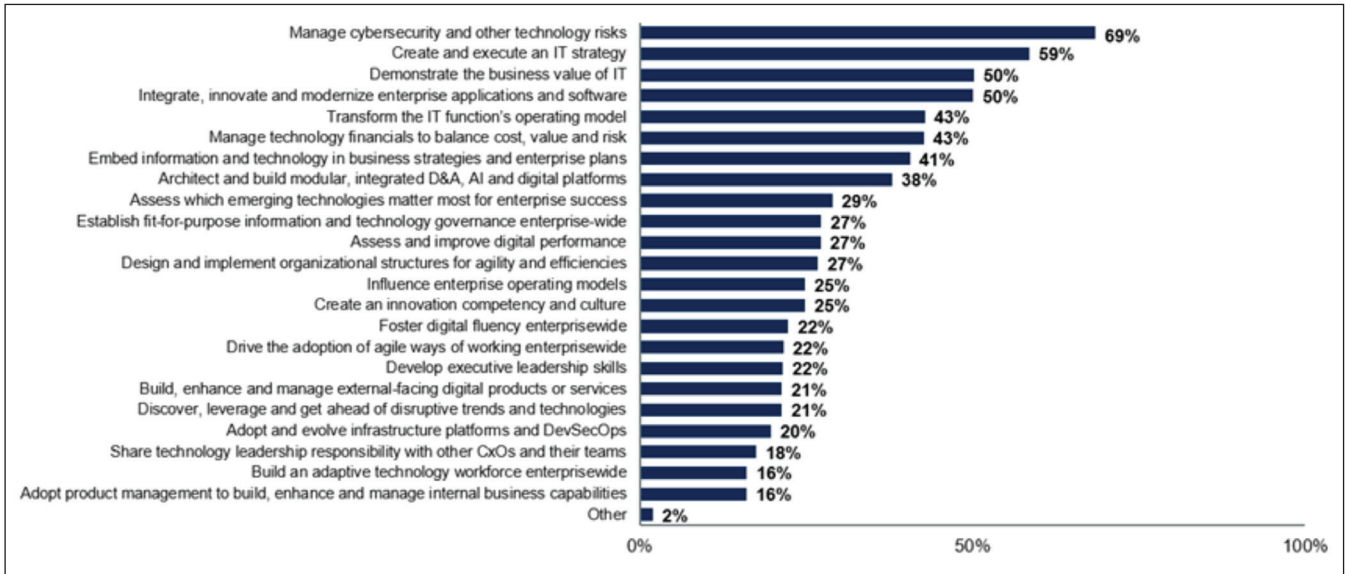
Data center systems spending grew by nearly 35% in 2024. While the segment will not see a jump equal to that in 2025, it is still set to grow by almost \$50 billion in 2025 (See Table 1). This is led by server sales, which are set to almost triple from more than \$134 billion in 2023 to \$332 billion by 2028, including more than \$257 billion in 2025. “GenAI will easily eclipse the effects that cloud and outsourcing vendors had on previous years regarding data center systems,” said Lovelock. “It took 20 years for the cloud and outsourcing vendors to build up spending to \$67 billion a year on servers. The demand of GenAI will help nearly triple server sales from 2023 to 2028.”

Software and IT Services Drive Growth

Spending on software is expected to increase 14%



➤ Figure 1: Changes in Technology Funding, from 2024 to 2025 (Percentage of Respondents). Source: Gartner (October 2024)



► Figure 2: CIO Focus Areas for 2025 (Percentage of Respondents). Source: Gartner (October 2024)

to \$1.23 billion in 2025, up from 11.7% growth in 2024. Meanwhile, IT services is expected to grow 9.4% to \$1.73 billion in 2025, up from 5.6% in 2024. “Software and IT services are a large driver of IT growth,” said Lovelock. “Spending on these segments is expected to be on AI-related projects, including email and authoring.

This was a market that, despite its age and having been consolidated down to a small number of players, will add \$6.6 billion to global spending in 2024 and \$7.4 billion 2025 due in part to GenAI products and services.

“Our forecast projects that \$500 billion will be added in spending every year in terms of growth rates. With this in mind, IT spending should cross the \$7 trillion mark in 2028.”

Top predictions for IT organizations and users in 2025 and beyond

Gartner, Inc. has revealed its top strategic predictions for 2025 and beyond. Gartner’s top predictions explore how generative AI (GenAI) is affecting areas where most would assume only humans can have lasting impact.

“It is clear that no matter where we go, we cannot avoid the impact of AI,” said Daryl Plummer, Distinguished VP Analyst, Chief of Research and Gartner Fellow. “AI is evolving as human use of AI evolves. Before we reach the point where humans can no longer keep up, we must embrace how much better AI can make us.”

Through 2026, 20% of organizations will use AI to flatten their organizational structure, eliminating more than half of current middle management positions.

Organizations that deploy AI to eliminate middle management human workers will be able to

capitalize on reduced labor costs in the short-term and long-term benefits savings. AI deployment will also allow for enhanced productivity and increased span of control by automating and scheduling tasks, reporting and performance monitoring for the remaining workforce which allows remaining managers to focus on more strategic, scalable and value-added activities.

AI implementation will present challenges for organizations, such as the wider workforce feeling concerned over job security, managers feeling overwhelmed with additional direct reports and remaining employees being reluctant to change or adopt AI-driver interaction. Additionally, mentoring and learning pathways may become broken, and more junior workers could suffer from a lack of development opportunities.

By 2028, technological immersion will impact populations with digital addiction and social isolation, prompting 70% of organizations to implement anti-digital policies.

Gartner predicts that by 2028, about one billion people will be affected by digital addiction, which will lead to decreased productivity, increased stress and a spike in mental health disorders such as anxiety and depression. Additionally digital immersion will also negatively impact social skills, especially among younger generations that are more susceptible to these trends.

“The isolating effects of digital immersion will lead to a disjointed workforce causing enterprises to see a significant drop in productivity from their employees and associates,” said Plummer. “Organizations must make digital detox periods mandatory for their employees, banning after-hour communication and bring back compulsory analog tools and techniques like screen free meetings, email free Fridays, and off-desk lunch breaks.”

By 2029, 10% of global boards will use AI guidance to challenge executive decisions that are material to their business.

AI-generated insights will have far-reaching impacts on executive decision making and will empower board members to challenge executive decisions. This will end the era of maverick CEOs whose decisions cannot be fully defended.

“Impactful AI insights will at first seem like a minority report that doesn’t reflect the majority view of board members,” said Plummer. “However, as AI insights prove effective, they will gain acceptance among executives competing for decision support data to improve business results.”

By 2028, 40% of large enterprises will deploy AI to manipulate and measure employee mood and behaviors, all in the name of profit.

AI has the capability to perform sentiment analysis on workplace interactions and communications. This provides feedback to ensure that the overall sentiment aligns with desired behaviors which will allow for a motivated and engaged workforce.

“Employees may feel their autonomy and privacy are compromised, leading to dissatisfaction and eroded trust,” said Plummer. “While the potential benefits of AI-driven behavioral technologies are substantial, companies must balance efficiency gains with genuine care for employee well-being to avoid long-term damage to morale and loyalty.”

By 2027, 70% of new contracts for employees will include licensing and fair usage clauses for AI representations of their personas.

Large language models (LLMs) that emerge have no set end date which means employees’ personal data that is captured by enterprise LLMs will remain part of the LLM not only during their employment, but after their employment.

This will lead to a public debate that will question whether the employee or employer has the right of ownership of such digital personas, which may ultimately lead to lawsuits. Fair use clauses will be used to protect enterprises from immediate lawsuits but will prove to be controversial.

By 2027, 70% of healthcare providers will include emotional-AI-related terms and conditions in technology contracts or risk billions in financial harm.

The increased workload of healthcare workers has resulted in workers leaving, an increase in patient demand and clinician burnout rates which is creating an empathy crisis. Using emotional AI on tasks such as collecting patient data can free up healthcare workers’ time to alleviate some of the burnout and frustration they experience with increased workload.

By 2028, 30% of S&P companies will use GenAI labeling, such as “xxGPT,” to reshape their branding while chasing new revenue.

CMOs view GenAI as a tool that can launch both new products and business models. GenAI also allows for new revenue streams by bringing products to market faster while delivering better customer experiences and automating processes. As the GenAI landscape becomes more competitive, companies are differentiating themselves by developing specialized models tailored to their industry.

By 2028, 25% of enterprise breaches will be traced back to AI agent abuse, from both external and malicious internal actors.

New security and risk solutions will be necessary as AI agents significantly increase the already invisible attack surface at enterprises. This increase will force enterprises to protect their businesses from savvy external actors and disgruntled employees to create AI agents to carry out nefarious activities.

“Enterprises cannot wait to implement mitigating controls for AI agent threats,” said Plummer. “It’s much easier to build risk and security mitigation into products and software than it is to add them after a breach.”

By 2028, 40% of CIOs will demand “Guardian Agents” be available to autonomously track, oversee, or contain the results of AI agent actions.

Enterprises’ interest in AI agents is growing, but as a new level of intelligence is added, new GenAI agents are poised to expand rapidly in strategic planning for product leaders. “Guardian Agents” build on the notions of security monitoring, observability, compliance assurance, ethics, data filtering, log reviews and a host of other mechanisms of AI agents. Through 2025, the number of product releases featuring multiple agents will rise steadily with more complex use cases.

“In the near-term, security-related attacks of AI agents will be a new threat surface,” said Plummer. “The implementation of guardrails, security filters, human oversight, or even security observability are not sufficient to ensure consistently appropriate agent use.”

Through 2027, Fortune 500 companies will shift \$500 billion from energy opex to microgrids to mitigate chronic energy risks and AI demand. Microgrids are power networks that connect generation, storage and loads in an independent energy system that can operate on its own or with the main grid to meet the energy needs of a specific area or facility.

This will create competitive advantage for day-to-day operations and derisk energy in the future. Fortune 500 companies who spend some of their operating expenses on energy should consider investing in microgrids which will offer a better return than continuing to pay rising utility bills.

APT and Schneider Electric transform The Pirbright Institute's data centre to fast-track advanced viral research

Seeking a new strategy to modernise its IT and legacy comms rooms and deploy them away from its existing buildings, a suggestion was made to explore the benefits of a modular, containerised data centre solution. The containerised data centre also includes complete monitoring and management systems, delivered via Schneider Electric EcoStruxure IT Expert data centre infrastructure management (DCIM) software. This is supported by Netbotz environmental monitoring, with over 60 data parameters measured and managed.

THE PIRBRIGHT INSTITUTE is at the forefront of global viral research, operating as one of the UK's leading virus diagnostics and surveillance centres. Pirbright is a worldleading centre of excellence for research into the control and surveillance of virus diseases of farm animals, and viruses that spread from animals to humans. It plays a pivotal role in controlling and preventing some of the world's most destructive diseases through the development of new and improved diagnostics and vaccines.

Recently, the Institute's campus has undergone significant development and investment, incorporating a state-of-the-art high containment (SAPO 4) laboratory – the BBSRC National Virology Centre: The Plowright Building and the low containment facility, The BBSRC National Vaccinology Centre, The Jenner Building. These facilities have enabled a unique combination of fundamental and applied research into pathogenic diseases with potentially devastating impact, enabling the Institute to maintain its cutting edge viral research.

Challenges

Pirbright has embarked on an exciting journey, modernising its campus to maintain high standard of infrastructure and research. In fact, its distributed and legacy IT facilities have played an essential role in housing its critical research applications, helping to ensure that the UK maintains its ability to monitor epizootic viral diseases of farm animals and control unexpected outbreaks.

Developing its campus was, therefore, imperative for maintaining its Reference Laboratory status - enabling the Institute to provide a world-leading

facility for research and training, while making its data available to researchers from other institutions around the world.

Its campus also provides laboratories with facilities capable of identifying and meeting the future demands of diseases which have not yet become a problem here in the UK, but with the advent of climate change, could soon become more widespread.

A critical part of its campus modernisation strategy has been the Institute's IT and data centre infrastructure systems, which not only provide a home for the massive amounts of data generated by its researchers, but deliver the processing power to analyse and turn it into actionable intelligence. Due to the mission-critical nature of its research applications, and the need to provide continuity of service during any modernisation, the Institute had to identify a new strategy to build out its infrastructure to support future technological requirements within high performance computing (HPC) and artificial intelligence (AI).

To deliver its new modernisation strategy it had to look beyond its legacy facilities, which had not been specifically designed for modern data storage requirements, and build a scalable, advanced and dedicated data centre environment for its research applications.

Once completed, the site would provide a unique and vital diagnosis and research facility within the UK, and one which will have international significance for the future.

Tim Haywood, IT infrastructure manager at The Pirbright Institute, a veteran of decades with multinationals, said "A host of new resources were available from the expansive investment, and there was a need to modernise our infrastructure to meet evolving needs."

"The challenge for IT was to find suitable accommodation for the data centre, while modernising to provide services such as secure backup, and Virtual Desktop Infrastructure (VDI) computing for the researchers and scientists using both our high and low containment laboratories. Some existing space was available in older buildings, but these spaces were designated for scientific usage, and could not be changed." "Furthermore, some of the buildings were scheduled for demolition in five to 10 years, meaning it made little sense to house the newly modernised infrastructure there," Tim Haywood observed, reflecting on the importance of value for taxpayers."

The Solution

Seeking a new strategy to modernise its IT and legacy comms rooms and deploy them away from its existing buildings, a suggestion was made to explore the benefits of a modular, containerised

data centre solution. With no prior relationship, Tim Haywood engaged with Advanced Power Technology (APT), an EcoXpert Partner and former Elite Data Centre Partner to Schneider Electric. APT has established a leading reputation as an independent supplier of energy efficient, critical power and cooling systems, and as a specialist in designing, building and maintaining data centres, server rooms and comms rooms.

Followed by a visit to an existing customer site not far from Pirbright's campus, the company quickly established a fruitful relationship and identified for what became known as the CDC – the Institute's new 'Containerised Data Centre'.

Built using key components from Schneider Electric's EcoStruxure for Data Centers solutions portfolio, including its EcoStruxure Row Data Center solution, formerly a Hot Aisle Containment System, APC NetShelter racks, cooling, Galaxy range UPSs, specifically the Symmetra UPSs, and APC NetBotz environmental monitoring, APT was quickly able to preconfigure its modular units with Schneider Electric equipment, enabling the solution to be pre-tested for faster deployment, installation, and greater predictability. Seeing the benefits immediately, Tim Haywood worked with his team to build out a strong business case for the solution. This was a significant process, as there had been a growing realisation that the Institutes IT infrastructure needed to evolve beyond network and storage into a centralised solution housed in a fully-secure and customised data centre.

"After engaging with APT and undertaking a detailed site survey, we were able to build the business case and the costs together quickly," said Tim. "Looking back, the approval to proceed went through with very little friction because it presented a valuable solution, and because it was fully customised."





Once the modular solution was selected, the project was delivered in three phases to meet a strict timeline of 12-weeks, ensuring minimal impact on the Institute's business or its critical applications. Phase 1 of the project, for example, required detailed site preparation and connection of utilities, and new foundations were laid to support the data centre modules.

Phase 2 required the data centre to be built, pre-configured and pre-integrated off-site, and migrating the existing infrastructure and IT systems which were to be retained by the Institute. Phase 3 was deployment, and with tight physical access, the containerised modules were delivered to site via low-loader, and craned into position in June 2023. By the end of July, the project was completed and commissioned well ahead of schedule. The new data centre delivered 80kW of scalable, optimised



and future-proofed capacity in an N+1 configuration, allowing the Institute to increase the resiliency and availability of its critical systems.

The new infrastructure, with the containerised data centre at its core, now supports high-tech research equipment such as sequencers, and diamond-light processes for virus analysis, that can generate data sets of 700GB each. It also allows the Institute to leverage new advancements in HPC, AI and GPU-powered computing, allowing them to identify breakthroughs in viral research at a far faster rate. This, in turn, drove the need for greater bandwidth, low latency data transfer, increased capacity and more secure storage. As such, its network connectivity was expanded to two 10Gb links, and it uses 1 petabyte storage arrays for onsite back up, with additional redundancy offsite.

The containerised, modular data centre also provides the flexibility needed for the Institute's researchers and supporting services, while delivering key advantages in areas such as physical security. For example, parts of the cooling equipment were elevated and installed on top of its modular architecture, allowing APT to deploy a highly effective, heavy-duty enclosure outside the facility, which prevents unwanted access and physical intrusion.

Employing an EcoStruxure Row Data Center solution also ensured the Institute would benefit from a highly efficient and scalable system that facilitates future growth. This approach, coupled with Schneider Electric InRow cooling units, means cooling efficiency is maintained even at lower rack densities.

The new ata centre now hosts a high-performance computing (HPC) cluster, used by scientists on a regular basis. Virtual desktop infrastructure (VDI) allows researchers and scientists to log onto their work whether they are inside the high containment (SAPO 4) laboratory, or sitting at a desk in the office. From a power perspective, Schneider Electric's Galaxy (the Symmetra) range of Uninterruptible Power Supplies (UPS) were deployed in an N+1 configuration, delivering leading levels of resilience and efficiency.

"High availability and business continuity are vital to the Institute, and outages whether scheduled or unscheduled, are undesirable. All maintenance and development, therefore, is undertaken with this need at the forefront of our strategy, and everything is dual connected with twice the power protection for high availability, which is our mantra," said Tim. The containerised data centre also includes complete monitoring and management systems, delivered via Schneider Electric EcoStruxure IT Expert data centre infrastructure management (DCIM) software. This is supported by Netbotz environmental monitoring, with over 60 data parameters measured and managed, including

temperature, humidity, leak detection, and multiple cameras providing real-time information via one complete platform.

“Cyber and physical security is paramount to the work of the Institute and it’s essential that we have continuous and proactive protection against phishing, malware, ransomware, and more. In fact, security is one of the biggest drivers we have, after science,” said Tim. “The investments we’ve made in EcoStruxure IT Expert DCIM and in data centre physical security have paid dividends - allowing us to leverage automation and remote monitoring to help protect against a host of threats.”

The results

The new data centre provides a dedicated, and world-class IT function that allows The Pirbright Institute to compete for groundbreaking research projects on a global basis. Its scalable, modular architecture, and its N+1 configuration also provides the highest levels of availability, resiliency and efficiency.

“One result of the new data centre and IT systems is the flexibility it provides for new research projects,” said Tim Haywood. “If a researcher has an urgent requirement, we’ve got the space to spin up more servers and have populated the system with the equipment from our previous data centre, so there’s plenty of potential.”

Tim Haywood said that the new capability, both in terms of capacity and flexibility, has allowed the Institute to contemplate new projects and ambitions, and further supports collaborations vital to its ethos, with active links to facilities in Guildford, Scotland, and around the world.

Furthermore, the new and futureproofed data centre environment enables the Institute to deploy new HPC and GPU technologies in line with the latest technological advancements, and its extended life cycle will help to deliver a 50 year life span.

“The unique set of challenges we encountered at The Pirbright Institute required a customised and tailor-made data centre, meeting its requirements for fast deployment, increased security, availability and efficiency,” said John Thompson, managing director of APT. “As such, it will provide a long-term, collaborative and scalable solution, which enables its endusers to deliver the highest standards of research, while meeting future demands for security and sustainability.”

“The scalable, sustainable and futureproofed solution, managed using Schneider Electric EcoStruxure IT Expert and bolstered by Netbotz environmental monitoring, also gives Pirbright the foundation to be even more ambitious with their future IT infrastructure and research demands,” he continued.



The data centre has allowed The Pirbright Institute to bring its IT infrastructure in line with its development master plans, ensuring it retains its place as the UK’s foremost centre of excellence in research and surveillance of viral diseases.

Future plans include new laboratories, scientific and administrative facilities that will see three centres of computing, comprising the two main mirror sites and a third, smaller control facility. Furthermore, the Institute now has the flexibility and capacity to support scientists and researchers as they leverage the state-of-the-art laboratories, and the specialised requirements of high-tech virology, HPC, and the vast data it produces.

What’s more, the Institute can further fast-track its knowledge and contributions to global health and welfare for animals, building on a solid IT foundation on which to develop ground-breaking research for decades to come.



➤ Caption here



The key steps business leaders must take to avoid AI projects failing

It's entirely understandable that business leaders have high expectations for artificial intelligence (AI) technology, and also that they should be impatient to get this technology to work.

BY NICHOLAS BORSOTTO, WW AI BUSINESS LEAD AND HEAD OF LENOVO AI INNOVATORS PROGRAM

WE HAVE SEEN two years with a near-unprecedented level of hype around the technology, in particular around generative AI. AI spending is rising, with 61% of tech leaders planning to increase their spend this year, according to the latest research. But it's best to tread very carefully, and to ensure that the organisation approaches AI not with blind enthusiasm, but with a grounded view of what AI is expected to deliver. Over the past couple of years, too many companies have invested in AI, then found that their proof-of-concepts have failed to deliver. It is very possible to get the right results from AI, but it requires not only careful thought beforehand, but also attention to detail throughout the project.

In the wake of the global frenzy around ChatGPT, some business leaders have become carried away with the hype around AI and challenged their IT teams to find ways to use generative AI right away,

without waiting. But there's a big problem with this approach. In those businesses, neither the leaders nor their IT teams have thought about how AI can really deliver a business advantage. Business leaders need to be certain they are using AI for the right reasons, rather than simply doing it out of the fear their competitors might get ahead.

Many technologies look exciting in the laboratory, but the gulf between such technology and the day-to-day reality of business applications is vast. Above all, business leaders need to avoid getting over-excited about technology that is at the 'exciting' stage, but has yet to become really useful. This sort of short-sighted view leads to AI investments being wasted.

Beyond the laboratory

Even the very best technology is just a science experiment if it cannot be adopted and used



in the real world. The single biggest reason AI 'doesn't work' for businesses is that people try to 'do AI' rather than identifying where problems or inefficiencies exist. To find such problems, business leaders should first talk to partners, and listen to consumers and front-line employees. Does the business lack staff to talk to customers? Does the business need to find a way to cut fuel emissions? Beyond the hype, the real excitement of this technology comes not from thinking about AI as a standalone solution, but by adding AI into the solution to a real business problem.

Communicating success

All too often, the approach to AI is to have a specific 'AI team', rather than applying the technology across the whole business. This siloed approach is a key mistake. AI must be integrated with a holistic approach, and a view to scaling it across every part of the business. Business leaders must connect multiple teams together to initially implement the technology, and avoid cutting corners to ensure seamless integration.

Business leaders need to design an effective proof-of-concept solution that includes AI appropriately in order to mitigate a business problem, and then scale it accordingly. For example, a generative AI chatbot that can answer niche questions could be made available to a small subset of customers initially, but rolled out to larger groups thereafter. Internal communication is also key as the business benefits of the proof-of-concept must be effectively communicated within the organisation, as AI projects often fail to be exciting to leadership until they grow to a certain size.

The right kind of AI

Even experts who have worked in the field for many years were caught by surprise at how the launch of ChatGPT made the pinnacle of AI technology so easy to adopt. This, in turn, made it easy for business leaders to imagine that generative AI should be adopted universally. But they should pause to think about whether such technology is the right choice, or if other forms of AI might do the job better.

The enthusiasm around generative AI has meant that it's sometimes used in areas which don't play to its natural strengths. Generative AI is great for conversational user interfaces such as chatbots, knowledge discovery and content generation. It's also highly useful in segmentation and intelligent automation and anomaly detection. For example, Smartia, a leading UK Industrial AI & IoT technology company, worked with Lenovo to harness machine learning and computer vision AI technologies to enable its composite manufacturing process to be smoother and greatly reduce anomalies. This demonstrates how AI is already improving manufacturing quality control through various systems that accurately detect defects.

Reaping rewards

All too often, the approach to AI is to have a specific 'AI team', rather than applying the technology across the whole business. This siloed approach is a key mistake. AI must be integrated with a holistic approach, and a view to scaling it across every part of the business

Artificial intelligence is already helping organisations to solve real problems in sectors such as retail and manufacturing. AI helps to streamline and speed up processes, eliminating the amount of time spent by employees on mundane tasks. In both retail and manufacturing, computer vision is emerging as an interesting and successful use of AI, linking the physical and digital worlds, and helping to spot defects on production lines and offering valuable insight in retail settings.

Signatrix's AI solution uses computer vision to draw important insights from cameras in retail stores, far beyond simply dealing with theft or similar incidents. The system is able to offer insights into important trends around what customers are looking at and buying, and to validate the success of promotions. The system can identify everything from misplaced products to how retail media (advertising) within the store is performing in terms of views.

In manufacturing, Graymatics' LabVista software uses computer vision to help make factories and laboratories more efficient and also safer for employees. LabVista conducts quality control checks on products, ensuring they are not missing any components, and monitors the number of products coming off a production line in any time period, also scanning for defects. But even more importantly, the LabVista system helps to make factories safer: the system scans for smoke and fire, while also detecting accident-prone machinery.

Preparing for success

The rewards of a successful AI project are very real, but business leaders need to ensure that they take the right approach to the technology. This entails remaining focused on the real, tangible problems that AI can solve, and how to deliver solutions that work for the business. It's also key to ensure that as many employees and parts of the business are 'hands on' with AI during the project. Taking this sort of balanced, holistic approach will help to ensure that AI projects survive from the drawing board through the tricky early stages, to become solutions which can deliver real and lasting value for the organisation as a whole.

Data governance - laying the foundations for effective AI applications

While AI in one way or another has been integral to financial services for some time, it's now hard to think of any area of the industry the technology hasn't touched. AI algorithms have evolved from simple rule-based fraud alerts to influencing everything from billion-dollar investment strategies to customer service interactions.

BY YIANNIS ANTONIOU, HEAD OF DATA, AI, AND ANALYTICS AT LAB49



ALTHOUGH AI holds significant promise for boosting efficiency and scaling operations, its increasing use comes with a rising demand for high-quality, well-governed data that is easy to discover and is reliable. Such data is integral in developing accurate, reliable, and fair AI models. Without it, organisations risk deploying AI applications that may have serious negative implications for financial institutions and their customers.

Building on solid foundations

AI systems are only as good as the data they have been trained on - their pattern identification and prediction capabilities rely on curated, high-quality data, ideally at very large sizes. Unfortunately,

data can be flawed in many ways – inaccuracy, incompleteness, bias, discrimination, and many other ethical factors are all concerns that need to be systematically addressed. AI models will produce outputs that reflect and amplify these data flaws.

This is because AI models don't inherently understand truth – they simplify, spot, and magnify patterns in the data without assessing whether those patterns are fair or accurately represent reality. If an AI model is trained on a dataset that disproportionately represents one demographic, it could unfairly favour that group in its decisions. These models naturally generalise the patterns they see, unaware of biases hidden in the data.



But poor data quality isn't just a technical concern – it can have real-world consequences on fairness. For example, an AI system used for credit scoring might unjustly deny loans to qualified applicants if it's trained on biased historical data. The controversy surrounding the Apple Card issued by Goldman Sachs is one notable example where an algorithm was accused of gender bias, allegedly offering lower credit limits to women with higher credit scores. Although Apple and Goldman were cleared by the New York Department of Financial Services, the companies still faced criticism for lack of transparency, and the regulators called for laws to be tightened. Clearly, the potential for biased algorithms may expose a financial institution to potential regulatory scrutiny and reputational harm.

Challenges in achieving high-quality data

Data fragmentation is a big challenge for large organizations, especially financial institutions. Even though they hold vast volumes of proprietary data, this information is spread across different systems and departments, locked behind silos that prevent the creation of the unified, high-quality datasets that AI models need to perform well. This data also usually lacks clear definitions, ownership and overall governance. This makes it difficult for financial institutions to quickly find, assess and use the right data to feed AI models.

And Generative AI comes with its own set of hurdles. The Large Language Models in use today are typically trained on vast amounts of unstructured data sourced from web scraping and public sources which can be low quality, skewed, or contain prejudiced content. This can lead to “hallucinations” where the AI produces outputs that sound convincing but are factually incorrect. Add in the positive feedback loops inherent in generative AI systems, where outputs influence future inputs, and small biases can quickly spiral out of control, scaling up to potentially result in poor outcomes in financial services use cases such as investment research or wealth management. The advent of generative AI has heightened existing concerns regarding algorithmic risks in financial systems. A salient historical precedent is the 2012 Knight Capital incident, where a solitary algorithmic error resulted in a \$440 million loss within a mere 45 minutes. Contemporary financial markets exhibit significantly greater complexity, and the integration of generative AI – characterized by its inherent unpredictability and non-deterministic nature – further amplifies potential risks.

In light of these evolving challenges, financial institutions must prioritize robust data governance frameworks and stringent data quality processes. These measures are critical to ensure the reliability, accuracy, and intended functionality of AI systems deployed in high-stakes financial environments.

Establishing robust data governance

To address these concerns, financial institutions



must make data governance an organisational priority. In practical terms, this means defining clear roles, responsibilities, and processes for data management, ownership, usage, and sharing across the organisation. Establishing clarity in these areas can encourage the necessary cross-functional collaboration to break down internal silos impeding the use of data for AI systems.

What's more, accountability and clear ethical guidelines can help mitigate the risk of generative AI systems becoming polluted by irrelevant or incorrect data. On a structural level, financial institutions that deploy secure and private AI models can be more confident that their AI systems are based on relevant and high-quality client data. By building in a way that aligns with responsible and ethical AI principles, they can also bolster the trustworthiness and credibility of their offerings to clients. On an ongoing basis, investing in regular cleansing, curating, and reviewing of data – regular assessments and audits with human oversight – goes a long way toward combating hallucinations. As the volume and variety of data increase, identifying and correcting data quality issues can become more challenging. Human experts, who are closer to their clients than algorithms, can naturally sense-check for relevance. In this way, human intervention can make judgment calls that automated systems might miss. Complete reliance on automated processes without humans in the loop may allow errors and biases to go unnoticed.

The integration of AI in finance therefore necessitates a fundamental shift in how financial organizations manage their data estate. Robust data governance is now critical for operational success, not just a technical requirement, and the performance of AI systems is directly tied to data quality. By implementing strong data governance, financial institutions can improve the accuracy, reliability, and fairness of their AI systems. This approach aligns with ethical standards and regulations while building client trust.

Ultimately, effective data governance forms the foundation for AI systems that enhance strategic decision-making and mitigate risks. It's not just a safeguard, but a strategic imperative for financial institutions navigating the AI landscape.

Time to shine a light on shadow AI

Whilst companies are right to encourage their teams to find innovative usages of generative artificial intelligence (GenAI) to streamline workflows, many employees are using the technology in ways that are not being sanctioned by their employers.

**BY TIM FREESTONE, CHIEF STRATEGY AND MARKETING OFFICER
AT KITEWORKS**

THIS SO CALLED “shadow AI” is a problem that is not going to go away any time soon. A recent study from Deloitte found that only 23% of those who have used GenAI at work believe their manager would approve of how they’ve used it. This unsanctioned use of AI should not be encouraged. After all, it could put an organisation in serious legal, financial, or reputational risk.

Something needs to change. Nearly one-third of employees admit to placing sensitive data into public GenAI tools. Yet, in the same study, 39% of respondents say that the potential leak of sensitive data is a top risk to their organisation’s use of public GenAI tools.



A tool for all

But how did we get here? The step change in AI adoption happened with the launch of ChatGPT. From that point forth it wasn’t just a tool for

technologists, but a tool for all. It was a collective ‘aha’ moment. Now, the use of AI has become almost as ubiquitous in our everyday lives as brushing our teeth in the morning.

In the past 12 months, we have seen organisations across nearly every industry deriving business value from AI. In fact, in a recent McKinsey Global Survey, 65% of respondents reported that their organisations are now regularly using the technology, nearly double the percentage ten months previous.

Respondents’ expectations for GenAI’s impact were highly positive, with three-quarters predicting that it would lead to significant or disruptive change in their industries in the years ahead.

Applying zero trust principles into the data layer
Most of the enterprise GenAI solutions being built

Businesses need to apply zero trust principles into this data layer. A zero trust model operates on the principle of maintaining rigorous verification, never assuming trust, but rather confirming every access attempt and transaction. This shift away from implicit trust is crucial. By embedding zero trust principles throughout generative architectures will offer a proactive path to enabling accountability, safety, and control

are being designed to leverage already available data. However, with much of this data being sensitive in nature, it is important that organisations take no chances. It is time for a shift in thinking and for businesses to think of GenAI solutions as a machine that moves data.

The top priority should, therefore, be how the data is being controlled both going into the system and when it comes out the other side.

Businesses need to apply zero trust principles into this data layer. A zero trust model operates on the principle of maintaining rigorous verification, never assuming trust, but rather confirming every access attempt and transaction. This shift away from implicit trust is crucial. By embedding zero trust principles throughout generative architectures will offer a proactive path to enabling accountability, safety, and control.

The democratisation of data

Part of the reason for the shadow IT epidemic is that the technology has thus far outpaced the need to secure it. Whilst some organisations know the risks, the knowledge has not yet percolated out. AI has been the democratisation of data leverage. Before GenAI, a business had to have technology sitting in front of a database to get to the data held within. Plus, someone who knew how to use it. Now, the only barriers to leveraging data is whether you know the alphabet. Because of this, the likelihood of data

going outside of the business markedly increases. Whilst a business can take steps to secure the technology and the data, there are always human beings in the loop. Training and education help, but we as a species remain incredibly flawed.

Brining AI out of the shadows

As long as GenAI is a tool that staff can use to help them reach their goals they will take advantage of it. The use of AI is not going to go away. And nor should it. AI is great for automating tasks, handling big data, facilitate decision-making, reducing human error, and further our understanding of the world around us. However, education of best practices and how to responsibly use AI is needed.

Least privilege access, always on monitoring, and never trust, always verify have been in place at the technology layer for some time. It is now the time to bring these principles down to the data itself. Thankfully, help is at hand. With a Private Content Network, organisations can protect their sensitive content more effectively in this era or AI. The best solutions provide content-defined zero trust controls, featuring least-privilege access defined at the content layer and next-gen DRM capabilities that block downloads from AI ingestion. They also themselves employ AI to detect anomalous activity – for example, sudden spikes in access, edits, sends, and shares of sensitive content. This will help shine a light on any unsanctioned activity going on in the shadows so that a business can remain compliant.

DW DIGITALISATION WORLD

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

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

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





Navigating the surge of cyberthreats in healthcare

Malicious attacks on the healthcare industry have grown exponentially in recent years. A survey of cybersecurity managers in the UK health sector found that 81% of organisations in the UK had been hit by ransomware in the previous year. Healthcare, in particular, is a prime target for threat actors, given how valuable patient information can be for identity theft and blackmail. Many health systems still operate with legacy technologies, making it easier for cybercriminals to gain unauthorised access.

BY SCOTT MCKINNON, CHIEF SECURITY OFFICER (CSO), UK&I AT PALO ALTO NETWORKS



HEALTHCARE is undergoing rapid modernisation. New technologies in the field can dramatically improve outcomes, while new care delivery models make the experience of receiving care much more pleasant for patients. And telemedicine, here, is a game-changer. It allows our already-stretched legions of doctors and nurses to “see,” diagnose and treat patients in a digital environment rather than forcing a patient to come into a physical office, clinic or emergency room. And while in-person care is obviously essential for many health issues, telemedicine is ideal for many other scenarios.

However, this also introduces a new level of risk that must be addressed: an ever-expanding attack surface in healthcare. Understanding the largest drivers of healthcare transformation today is key to securing digital transformation and providing the quality of care patients deserve.

The emergence of telehealth

Telehealth and remote patient monitoring are revolutionising the care delivery experience. Patients enjoy better access to care, especially those with disabilities or those who live in

underserved communities. In 2022, NHS England's experimental statistics showed that an average of 41.2% of appointments were by telephone, highlighting an increase in telemedicine.

While innovations, like remote care, optimise patient-centric care delivery, they also introduce new cybersecurity challenges. Remote care requires access to Emergency Medical Retrieval Service (EMRS), Protected health information (PHI), virtual visits and remote patient monitoring devices delivered from multiple channels: data centres, cloud providers and SaaS providers. Security teams must also manage the IT infrastructure and connectivity between hospitals and patients. Ultimately, this shift toward decentralised care delivery models expands the attack surface and makes securing the entire network much more painstaking.

The rise of connected devices

Connected medical and non-medical devices now make up a sizable portion of a hospital's network. MRI machines, IV pumps, blood pressure monitors, laptops and security cameras, and even Heating, Ventilation, and Air Conditioning (HVAC) systems, just to name a few. Preventing data compromise and risks to patient safety requires securing these connected devices from end to end.

Complete visibility among the diversity of devices can be extremely challenging, especially among providers practising distributed-care delivery models. Devices are often connected to complex medical IT environments while located in medical centres, remote clinics and patient homes. This widens the endpoint sprawl, making every device a potential target for cybercriminals. To further complicate this problem, many IoT and IoMT devices are both critical to provider operations and highly insecure due to design for functionality and cost and not secure-by-design across the expected lifecycle.

The growing complexity of Healthcare IT systems

Applications and services are now hosted in data centres and the cloud, or they're delivered by SaaS providers, while clinicians deliver care from anywhere using an array of connected medical devices. Many of these run on antiquated operating systems and often cannot be patched or secured effectively. Security teams are tasked with managing these increasingly complex IT environments, which require significant technical resources.

Healthcare organisations often attempt to secure this digital landscape by tackling on point product solutions that provide a single security function. These products typically lack integration and cohesiveness, only adding to the complex challenge.

Making digital transformation secure for healthcare

Addressing the surge of cyberthreats in healthcare requires a multifaceted approach that combines technology, policy, and education so they don't run on multiple disjointed products. A first step for healthcare organisations would be to invest in robust cybersecurity measures to protect patient data and critical infrastructure. This includes implementing advanced encryption protocols, multi-factor authentication, and network segmentation to limit the impact of potential breaches. Regular security audits and vulnerability assessments can also help identify and mitigate potential weaknesses in the system.

Secondly, collaboration and information sharing among healthcare providers, government agencies, and cybersecurity experts are essential for staying ahead of evolving threats. For example, NHS England's Data Security and Protection (DSPT) Toolkit is a good starting point to help promote consistency and ensure security standards are met. However, these systems require continual development and potential expansion, as well as encouraged adoption by the public and private sectors. Equally, consolidating the cybersecurity arsenal into a unified platform eliminates the complexity of managing multiple tools and offers a holistic view that enhances operational efficiency and effectiveness. In addition, fostering a culture of cybersecurity awareness and training regularly among healthcare staff is crucial for mitigating human error, which remains a significant vulnerability in many organisations.

Finally, leveraging emerging technologies such as AI and machine learning capabilities securely can enhance threat detection and response capabilities. These technologies can analyse vast amounts of data in real-time to identify anomalous behaviour and proactively defend against cyberattacks. By taking a proactive and collaborative approach to cybersecurity, the healthcare sector can stay ahead of new and emerging threats, ensuring patient data and the integrity of their systems are protected in an increasingly digital world.





Who are BISOs and what do they bring to the cybersecurity table?

The role of a Business Information Security Officer (BISO) is gaining traction in security communities and board conversations. But why do organisations need BISOs? What are the main business drivers? What is their relationship with security leaders and what traits are ideally suited for the role?

BY STEVE DURBIN, CHIEF EXECUTIVE, INFORMATION SECURITY FORUM



The Main Drivers for a BISO

COLLABORATING with information technology has been around since its inception, when it started as a transactional order-taking department. Over time a partnership emerged with business because technology soon assumed a central role across every process. Along similar lines, cybersecurity too has come of age, with the understanding that security requires better alignment with the business.

In large organisations, the chief information security officer (CISO) is expected to apply risk management and oversight of every department, something nearly impossible to achieve, especially in a distributed environment. If CISOs become too involved in daily security and compliance

operations, they run the risk of spreading themselves too thin.

Additionally, there's always been a disconnect between business leaders and security leaders driven by a perception that cybersecurity is a necessary expense that does little to further the business. Security leaders may have previously seen themselves as the most urgent voice in the room, leaving little room for collaboration on security matters — a problem exacerbated by technical jargon and complexity.

BISOs deliver the much-needed headspace CISOs need to strategise and to lead. By delegating day-to-day security issues, CISOs can focus on developing

a security strategy aligned with the larger business goals.

The Key Objectives of a BISO

A BISO role has primarily two objectives:

Enrich the value of security for the business: A closer relationship with the consumer – the business – can make security more alluring and demonstrate its value by understanding the motivations and needs of the business and mapping the security proposition to those needs. The goal is to reach a point where the business ‘wants’ security as a line of investment, rather than security being seen as something it must have.

At a high-level, the role of a BISO is to build enduring relationships across the organisation; find solutions to specific business risk challenges; support the delivery of corporate security strategies; earn trust and confidence of both technical and non-technical stakeholders; nurture security culture by factoring in local and demographic considerations; and enable risk-based decision making at a more granular level across the organisation.

Support the strategic ambitions of enterprise security leadership: While the CISO owns the organisation’s overall security strategy and ensures that the strategy protects the overarching values of the organisation, a BISO is responsible for executing strategy at a more granular, functional, and departmental level. A BISO is basically the arms and legs of a CISO, serving as a mediator between central and local security functions. For instance, they can recommend optimisations that reduce the burden on business teams.

Does Every Organisation Need a BISO?


Small organisations will likely not have a need for a BISO. However, this doesn’t mean that the security leader or CISO will not require some sort of business partnership arrangement. Smaller

organisations could lean on “security champions” to achieve similar outcomes. For larger organisations, the decision to onboard a BISO will depend on the scale, maturity, geographic location and future goals of the security function. Some organisations may want to consider a hybrid approach, splitting the BISO responsibility 50-50 with an additional responsibility such as leading a specific security function (e.g., supply chain risk management) or geography.

What Skills and Characteristics Must Organisations Look for in a BISO?

A key requirement of the BISO role is bringing security, technical, and business stakeholders together in partnership to exploit the strength of all parties – a challenge to achieve without a balance of business and technical knowledge. Someone with deep technical experience could present an unconscious bias towards technology, potentially limiting the BISO’s capacity to think more broadly and implement practices that meet the needs of the business. Although having a technical skillset isn’t always necessary, someone with deep technical experience can be helpful when striving to earn the respect of technical staff. Along with business and technical acumen, a BISO is expected to have familiarity with a wide range of applications and systems, an understanding of business risks and mediation skills – a problem solver, active listener, and analytical thinker.

The position of a BISO is still in its formative stage, much like other security leadership roles including the CISO, which initially struggled with role clarity (and still struggles today to some extent). Adopting a business partnering approach by appointing a BISO can be a profitable strategy for fostering inclusive cultures, proactively addressing security risks, and positioning security as a valuable business opportunity rather than a mere compliance requirement.



DW **ROUNDTABLE**
Modern Enterprise IT - From The Edge To The Core To The Cloud

Not every discussion
is a **battle...**

- Based around a hot topic for your company, this 60-minute recorded, moderated zoom roundtable would be a platform for debate and discussion
- Moderated by an editor, Phil Alsop, this can include 3 speakers
- Questions prepared and shared in advance

Cost: €5995

Contact: Jackie Cannon
jackie.cannon@angelbc.com

**ANGEL
EVENTS**

Who's responsible for **digital trust**?

Digital trust isn't merely a defence against the ever-present problems of privacy infringement, cybersecurity threats and technology failures - but a way to innovate and expand safely.

BY BRIAN TRZUPEK, SENIOR VICE PRESIDENT, PRODUCT, DIGICERT



DIGITAL TRUST is the measure of confidence that we have in the digital products and services that we rely on every day. It's built of the industry and technological standards, systems of operations and compliance, software that manages the delivery of that trust within an organisation and the efforts to extend trust across lifecycles, through software supply chains and everywhere else.

As such, it is now an irrevocable business priority. As an idea which helps protect the baseline connections and technologies which we use every day - it is absolutely fundamental to police the complex web of transactions that define modern

business. Businesses have begun to understand its importance, but, according to a new survey from DigiCert - these efforts are not without their own problems and inconsistencies.

In fact, digital trust efforts seem to be spread inconsistently across many organisations, resulting in silos which ultimately mitigate their broader value.

Surveying companies around the world - DigiCert's 2023 Digital Trust Survey found exactly this. Most organisations - 87% - believe that their digital trust efforts are too siloed. The typical enterprise has 5 or fewer departments that issue certificates and most believe that more departments should issue them.



Drilling down further, over half of our respondents - 52% - told us that the IT department manages their certificates, while certificates are managed outside of IT in 37% of certificates and in 11% of organisations no one manages certificates at all. It's an uneven, siloed arrangement which leaves digital trust efforts fractured and in turn, can lead to all manner of problems and risks. In fact, digital trust is only as good as its scope - and the minute data passes from a department which employs digital trust to a department that doesn't, it loses that crucial quality. Ultimately, only 1% believe that their digital trust practices are "extremely mature."

They're not wrong - digital trust efforts need to address the whole enterprise. Not doing so risks mismanagement, certificate outages and data breaches. The consequences of that mismanagement in this case are clear - 98% of respondents reported outages and brownouts, 92% reported data breaches and 74% compliance issues all stemming from digital trust issues.

Digital trust is for the whole organisation

The reality is that digital trust is the responsibility of the whole organisation. Perhaps the defining thing one can say about modern business is that it is digitally driven and connected. Technologies and IT assets touch most - if not all - parts of the business. Digital trust is all about securing those basic technical connections which allow us to do our jobs and live our lives. As such, it needs to be everywhere those connections lead.

There are three foundational elements to digital trust. The first is identity, required for individuals, workloads, services, devices, or technology. The second is integrity - the assurance that an object remains whole and has not been tampered with. The final is encryption, which secures data in transit. These three steps are increasingly a fundamental layer of security, protecting the dense webs of transactions that define modern business.

Digital trust is heavily associated with Public Key Infrastructures (PKI) and certificates - and rightly so - but must be viewed as a more holistic concept for a business. Principally, digital trust needs to be made a strategic imperative from the top down. This means that organisational leaders and executives need to take responsibility and put digital trust at the centre of their management concerns. Similarly, it also means adopting digital trust as a designing principle for an entire business, which involves the wide deployment of PKIs (Public Key Infrastructures) and certificates but has also found expression in things like Zero Trust architectures.

From there, those digital trust efforts must maintain compliance with policies and be updated to adapt to changing threats, architectural shifts, and regulatory concerns. Looking ahead, businesses will need to find ways to enable connected trust, expanding trust into complex supply chains and ecosystems such as

across software supply chains or to establish digital rights provenance in a content community.

Digital Trust Officers

To make digital trust a driving concept in business strategy, some organisations are introducing Digital Trust Officers (DTO). These positions intend to oversee all digital trust efforts across the organisation, changing digital trust from a narrow tactic to an overall business strategy. Within that position, these trust officers will create, and oversee the policies and processes that centrally govern the digital trust and risk issues that are so crucial in modern business. But digital trust efforts can become complex, at least as complex as the dense networks of connections, devices, and data that they protect, and what a DTO does is offer a single centralised point of accountability and oversight for that whole complex operation.

Digital trust as a baseline for digital expansion
There are myriad reasons that digital trust is becoming a key driving force behind technical change in the enterprise. A mature digital trust infrastructure is not merely a reactive, defensive asset to have but one that sets the path for innovation. DigiCert's 2023 State of Digital Trust survey found that high levels of digital trust maturity often led to better outcomes in terms of revenue, security, and innovation.

In fact, 96% of those trust-mature organisations reported that digital trust helped them to digitally innovate, 93% said it helped with brand reputation, another 93% reported higher revenues, 74% reported high employee productivity and 56% reported higher profits.

The difference between those who used digital trust to their advantage against those who didn't are clear: 100% reported more mature trust practices, 97% reported more centralised management of trust services and 57% were more likely to manage certificates in IT.

In a 2022 Keynote, Forrester's VP and Principal Analyst simply announced that "Technology trust equals brand trust." DigiCert's 2022 State of Digital Trust survey showed that two thirds of companies have switched vendors after they lost trust in their previous vendor. Similarly, research from Deloitte has shown the potential for trust-led growth. According to one Deloitte survey, 88% of consumers who trust a brand become repeat customers and as such, trustworthy companies beat out competitors by four-fold.

Digital trust isn't merely a defence against the ever-present problems of privacy infringement, cybersecurity threats and technology failures - but a way to innovate and expand safely. But it cannot do that when constricted to silos and needs to have a wide scope, expanding holistically across organisations to fulfill those grand promises.

Capitalising on your data with DataOps

Across every industry, companies continue to put increased focus on gathering data and finding innovative ways to garner actionable insights. Organisations are willing to invest significant time and money to make that happen.

BY GUY EDEN, VP PRODUCT MANAGEMENT, BMC



ACCORDING TO IDC, the data and analytics software and cloud services market reached \$90 billion in 2021 and is expected to more than double by 2026 as companies continue to invest in artificial intelligence and machine learning (AI/ML) and modern data initiatives.

However, despite high levels of investment, data projects can often yield lacklustre results. A survey of advanced major analytics programmes by McKinsey found that companies spend 80 percent of their time doing repetitive tasks such as preparing data, where limited value-added work occurs. Additionally, they found that only 10 percent of companies feel they have this issue under control.

So why are data project failure rates so high despite increased investment and focus?

Many variables can impact project success. Often cited factors include project complexity and limited talent pools. Data scientists, cloud architects, and data engineers are in short supply globally. Companies are also recognising that many of their data projects are failing because they struggle to operationalise the data initiatives at scale in production.

This has led to the emergence of DataOps as a new framework to overcoming common challenges.

DataOps is the application of agile engineering and DevOps best practices to the field of data management to help organisations rapidly turn new insights into fully operationalised production deliverables that unlock business value from data. DataOps tools and methodologies can help you make the best use of your data investment. But if you want to succeed in your DataOps journey, you must be able to operationalise the data.

The obstacles to data orchestration

Most data pipeline workflows are immensely complex and run across many disparate applications, data sources, and infrastructure technologies that need to work together. While the goal is to automate these processes in production, the reality is that without a powerful workflow orchestration platform, delivering these projects at enterprise scale can be expensive and often requires significant time spent doing manual work.

Data workflow orchestration projects have four key stages:

Ingestion involves collecting data from traditional sources like enterprise resource planning (ERP) and customer resource management (CRM) solutions, financial systems, and many other systems of record in addition to data from modern sources like devices, Internet of Things (IoT) sensors, and social media.



Storage increases the complexity with numerous different tools and technologies that are part of the data pipeline. Where and how you store data depends a lot on persistence, the relative value of the data sets, the refresh rate of your analytics models, and the speed at which you can move the data to processing.

Processing has many of the same challenges. How much pure processing is needed? Is it constant or variable? Is it scheduled, event-driven, or ad hoc? How do you minimise costs? The list goes on and on.

Delivering insights requires moving the data output to analytics systems. This layer is also complex, with a growing number of tools representing the last mile in the data pipeline.

With new data and cloud technologies being frequently introduced, companies are constantly reevaluating their tech stacks. This evolving innovation creates pressure and churn that can be challenging because companies need to easily adopt new technologies and scale them in production. Ultimately, if a new data analytics service is not in production at scale, companies are not getting actionable insights or achieving value.

Executing business-critical workflows at scale

Successfully running business-critical workflows at scale in production doesn't happen by accident. The right workflow orchestration platform can help you streamline your data pipelines and get the actionable insights you need.

With that in mind, here are eight essential capabilities to look for in your workflow orchestration platform:

Support heterogeneous workflows: companies are rapidly moving to the cloud, and for the foreseeable future will have workflows across a highly complex mix of hybrid environments. For many, this will include supporting the mainframe and distributed systems across the data centre and multiple private and/or public clouds. If your orchestration platform cannot handle the diversity of applications and underlying infrastructure, you will have a highly fragmented automation strategy with many silos of automation that require cumbersome custom integrations to handle cross-platform workflow dependencies.

Service level agreement (SLA) management: business workflows, ranging from ML models predicting risk to financial close and payment settlements, all have completion SLAs that are sometimes governed by guidelines set by regulatory agencies. Your orchestration platform must be able to understand and notify you of task failures and delays in complex workflows, and it needs to be able to map issues to broader business impacts.

Error handling and notifications: when running in production, even the best-designed workflows will have failures and delays. It is vital that the right teams are notified so that lengthy war room discussions just to figure out who needs to work on a problem can be avoided. Your orchestration platform must automatically send notifications to the right teams at the right time.

Self-healing and remediation: when teams respond to job failures within business workflows, they take corrective action, such as restarting a job, deleting a file, or flushing a cache or temp table. Your orchestration platform should enable automation engineers to configure such actions to happen automatically the next time the same problem occurs.

End-to-end visibility: workflows execute interconnected business processes across hybrid tech stacks. Your orchestration platform should be able to clearly show the lineage of your workflows. This is integral to helping you understand the relationships between applications and the business processes they support. This is also important for change management. When making changes, it is vital to see what happens upstream and downstream from a process.

Self-service user experience (UX) for multiple personas: workflow orchestration is a team sport with many stakeholders such as data teams, developers, operations, business process owners, and more. Each team has different use cases and preferences for how they want to interact with the orchestration tools. This means your orchestration platform must offer the right user interface (UI) and UX for each team so they can benefit from the technology.

Production standards: running workflows in production requires adherence to standards, which means using correct naming conventions, error-handling patterns, etc. Your orchestration platform should have a mechanism that provides a very simple way to define such standards and guide users to the appropriate standards when they are building workflows.

Support DevOps practices: as companies adopt DevOps practices such as continuous integration and continuous deployment (CI/CD) pipelines, the workflow development, modification, and even infrastructure deployment of workflows, your orchestration platform should be able to fit into modern release practices.

The need for data is on the rise and shows no signs of abating, which means that having the ability to store, process, and operationalise that data will remain crucial to the success of any organisation. DataOps practices coupled with powerful orchestration capabilities can help enterprises orchestrate data pipelines, streamline the data delivery process, and improve business outcomes.



A data-led approach to powering digital transformation

Digital transformation is already a reality for most organisations. But successful change management and a data-led approach can significantly enhance the chances of a smooth transition. The common obstacles organisations face during digital change and how business leaders can harness data to ensure effective digital transformation.

JAMES YOUNG, CTO AT CANTIUM BUSINESS SOLUTIONS

Mapping processes and data flow

THERE'S A LOT OF PRESSURE to get digital transformations right. It's suggested that while 89% of large companies globally have a digital and AI transformation underway, they've only captured 31% of the expected revenue lift and 25% of expected cost savings from their programmes. More often than not, efforts falter because organisations have failed to understand their operations in the context of digital change.

Change isn't easy, and companies frequently have complex, layered processes that have been developed organically, over time. These processes can be elaborate and digitising them requires a thorough understanding of how information flows through the business. It's these disjointed processes that need to be scrutinised and mapping them out is essential to identify where complexity has been added along the way.



It's a crucial step, as it lays the foundation for identifying inefficiencies and areas where digital tools can be most beneficially applied. Effective change management is about understanding the true cost of delivery and the impact of changes on the organisation. A data-led approach helps, as it provides a clear picture of the existing processes and the data generated. By understanding the data flow and lifecycle within the business, leaders can make informed decisions about where to implement changes and how to measure their impact.

Saying that, it can be difficult to know where to start. For organisations with an established business change function, this team can be instrumental in leading the charge on digital transformation projects. As they have access to the information and possess knowledge of the organisations processes, people and workflows. However, when integrating new technologies, you need expertise to transform

the way data moves through the business lifecycle – and that might not be available in-house. That’s why it’s important to call on both internal capabilities and external perspectives to fully realise the potential of digital transformation.

Crafting an effective strategy

Assessing current processes and data flows, is the foundation of a data-led approach. Organisations must map out the lifecycle of data within their operations, understanding where data is generated, how it flows through different systems, and where it ends up. Identifying critical data points is essential for measuring performance and driving decision-making. It will form the basis of your strategy and should align with your organisation’s overall digital transformation goals.

The organisational strategy needs to drive the right cultural behaviours and attitudes. It’s estimated that 70% of digital transformations fail because of employee resistance. Leaders must articulate the benefits of digital transformation clearly, translating them into actionable, real-life examples to gain buy-in from employees. A clear strategic direction, supported by senior management and key stakeholders, helps align the organisation with the aims and objectives of the transformation. It should also outline how data will be captured, processed, and analysed. Establishing data governance policies ensures data quality, security, and compliance, as well as defining data ownership, access controls, and data standards.

Time waits for no one

The timing of digital transformation can significantly impact its success. Key trigger points include the end-of-life of critical technologies like ERP or CRM systems or the need to support business maturity. Starting early allows organisations to explore alternatives, understand their processes better, and make well-informed decisions. Delaying

A data-led approach is about understanding the cost of delivery, the data dependencies of workflows, and structuring the data in a way that aligns to key performance indicators

transformation can result in missed opportunities for efficiency and innovation. When organisations wait until technology contracts are up for renewal, they are often forced into making hasty decisions that don’t align with their long-term goals. This can railroad the transformation process, making it reactive rather than proactive.

A data-led approach is about understanding the cost of delivery, the data dependencies of workflows, and structuring the data in a way that aligns to key performance indicators (KPIs). It’s an approach that requires a holistic view of the data architecture across the entire business. By joining up data meaningfully, organisations can avoid the pitfall of having various data silos that fail to deliver true value.

Ultimately, digital transformation is a complex but necessary journey for modern organisations. By adopting a data-led approach, organisations can navigate the challenges of change management more effectively. Understanding and mapping data flows, aligning organisational strategy, and leveraging technology are crucial steps to ensure a smooth transition. Business leaders play a vital role in articulating the benefits and driving the cultural shift needed for successful digital transformation. A well-executed digital transformation not only improves efficiency but also positions an organisation for sustained future growth and innovation.

DW

ROUNDTABLE


Modern Enterprise It - From The Edge To The Core To The Cloud


- Based around a hot topic for your company, this 60-minute recorded, moderated zoom roundtable would be a platform for debate and discussion
- Moderated by an editor, Phil Alsop, this can include 3 speakers
- Questions prepared and shared in advance

Cost: €5995

Contact: Jackie Cannon
jackie.cannon@angelbc.com

Not every discussion is a battle...





Three-step strategy for making your tech investments work harder

By reassessing the role of technology in helping the business achieve its most pressing goals, IT decision-makers can ensure their investments make the most sense. Step back, and take the time to address these three key questions that will help get your tech investment strategy in a better position.

BY JOE BAGULEY, CTO EMEA AT BROADCOM



REMAINING COMPETITIVE as an IT organisation is a task made more challenging when navigating a complex cloud environment. Speed is mission-critical when trying to keep up with new demand. However, the tech investments made intermittently along the way can become siloed and won't always make financial sense. A convincing business case might be presented to you or the latest hype in the market may catch your eye, but sporadic artefacts accumulated over time usually results in IT budgets being stretched thin. Some gains might be made, but ultimately even a coherent investment strategy becomes sidelined.

In a down market, it is essential that investment in technology solutions produces digital transformation that helps users, reduces pressure on IT teams and achieves more agility than what was had before. That's how a significant competitive advantage will form, and re-introducing a holistic strategy is one way to get there. By reassessing the role of technology in helping the business achieve its most pressing goals, IT decision-makers can ensure their investments make the most sense. Step back, and take the time to address these three key questions that will help get your tech investment strategy in a better position.

Is my IT infrastructure more complex than it needs to be?

With the various IT platforms and solutions adopted by organisations come a string of tools that are also integrated along the way. Even though those tools aren't essential to the performance of the platforms, they're added on through iterations and updates which complicate the IT infrastructure

unnecessarily. IT professionals will have a hard time of distinguishing what tech is adding value, what's causing inefficiencies and realising the extent of the services they can deploy. As a result, organisations can find themselves purchasing additional software for multiple versions of the same product that was already providing the functionality they needed.

I have a real-life example of this in a recent conversation with a customer. A well-recognised media firm was looking to build a sustainability dashboard for their IT operations, but what they didn't know was that their existing VMware dashboard was capable of executing that work at the same cost. After having an active tender out for a year, they then learned how their current solution could work to get the most out of it. Don't underestimate your existing IT infrastructure – the solution is often already in your tech stack. It just requires you to regularly look at your IT investments and view them holistically as one, integrated system. You may be surprised at how many tools you already own and how seamlessly they can operate.

Is a tailored tech stack necessary?

Technologist may be led to believe that building a bespoke tech stack is key to becoming differentiated. What they might not realise is that the tech investments made to become fully bespoke become siloed. These investments are focused on specific tools and products that are then joined together to make something completely different – which often don't all work well together and require constant work from considerable-sized teams just to maintain.

Oftentimes simplification is the most effective way forward. You can capitalise on the solutions and platforms that are ready to be bought off the shelf - solutions that are industrialised, reliable and easily deployable. This route will help you to create a centralised development environment that quickly responds to customer needs and delivers on new requirements based on what customers ask for, in turn delivering greater value.

What is innovation truly defined by in my business? Innovation can be associated with adopting the latest and greatest solutions, but are those technologies adding value and making a difference where it matters or simply keeping the lights on? Organisations might race to invest in public cloud networks or more recently generative AI tools, but why does innovation on-premises or a private cloud environment get underestimated? The latter options can produce the same level of agility but a better focus on cost, data sovereignty and security. The right solution for your organisation might not require building your own cloud platforms. Rather it can involve adding layers of innovation and finding solutions with built-in resilience for continuous operations, threat prevention, and fast recovery from cyber threats. That's where the real differentiation can be found.

Avoid getting swept up by what competitors are revealing and market trends are convincing you of.



Getting the most from your tech investment starts by shifting to an innovation mindset. Use the questions we've covered above to understand your IT infrastructure and align your investments with your broader business objectives.

You don't need to create a tailored IT solution or acquire every new technology, instead, focus on building an environment that offers flexibility and agility through scalable and ready-to-go solutions. That's how you can enable your business to deliver impactful innovation and revitalise your tech investment strategy.

DW DIGITALISATION WORLD

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

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

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

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





A changing landscape for technology firms amidst the Ecodesign for Sustainable Product Regulation

The EU's initiative for a circular economy through the ESPR and mandating of DPPs marks a milestone commitment to lowering waste levels and provides hope for a more circular and sustainable economy.

BY LARS RENSING, CEO OF PROTOKOL

IT IS NO NEWS that waste is a growing problem in modern society. As technology evolves at such a rapid pace, our desire for new devices and gadgets continues to lead to rising waste levels. In particular, for technology companies, e-waste is a prominent issue that must be tackled. To put this into context, 'there are almost 350 million tonnes of unrecycled e-waste on earth'.

On this, as countries globally start to take note of the detrimental effects waste is having on the planet, the 'need to act now to avoid the worst scenario' is becoming a poignant narrative. Regarding the EU's efforts to tackle such issues, it has recently championed a number of initiatives to encourage more sustainable business practices and ensure all parties are playing their role in supporting a circular economy. One of these is the Ecodesign for Sustainable Products Regulation (ESPR), which came into force on July 18th and stands as part of the EU's greater Circular Economy Action Plan (CEAP).



The ESPR aims to 'significantly improve the circularity, energy performance, and other environmental sustainability aspects' of products placed on the EU market by ensuring that the product groups within these specified industries have greater sustainability and recyclability attributes. These industries don't just include ICT, the regulation will apply to a range including - but not limited to - furniture and chemicals. The deadline for compliance is 2030 for many of the designated industries and product groups, however for some - including ICT and electronics - it may be as soon as 2027. On this, it is worth noting any business placing products within these groups on the EU market will have to comply—including businesses who have manufactured their items elsewhere.

As part of this legislative move toward greater product sustainability, the implementation of Digital Product Passports (DPPs) will be mandated across all specified product groups. However, although the

information on the delegated acts (specific guidance pertinent to each industry and product group) is yet to be announced, tech businesses should begin considering their road to compliance to ensure a smooth transition amidst the changing landscape

Digital Product Passports and their helping hand in ensuring company compliance

In simple terms, DPPs are a transparent tool used to collect and provide data concerning the lifecycle of a product. They will prove vastly significant in supporting the EU's sustainability efforts as they can provide insight into product information such as composition, recyclability attributes, and details pertaining to the carbon footprint of a product's lifecycle. They can even provide product disposal information.

These characteristics of DPPs are largely what made them the chosen tool to support the EU's circularity efforts. Moreover, by mandating DPPs the EU hopes to empower technology businesses with greater levels of transparency into the products they use to encourage more sustainable practices surrounding design, sourcing, and end-of-life. Furthermore, DPPs also provide end-users with valuable information on a range of fronts. For example, providing end-users with guidance on how to dispose of an item responsibly when it reaches the end of its lifecycle, is expected to prompt consumers to act more sustainably in their day-to-day considerations.

Moreover, DPPs will also prove particularly beneficial when concerning Western society's issues with hazardous materials, such as those found in some electronic items, and hold the potential to transform e-waste management. To put this problem into perspective, 'The UK currently produces around 3 million tons of hazardous waste annually, with almost half coming from commercial and industrial waste.' Therefore, through DPPs and their ability to identify pertinent details regarding product makeup, e-waste could become an issue of the past. Regarding the composition of DPPs, they would be accessible via a data carrier, such as QR code or barcode, placed somewhere on the product. The data can then be obtained by scanning with a smartphone. The accessibility that DPPs provide through the compact data carrier, enables all individuals active in a product's life-cycle to access a range of data on demand and play a key role in ensuring the item's circularity journey.

What can technology companies do now to ensure compliance?

Although the ESPR came into force on the 18th of July, information on delegated acts is yet to be announced. Only here will companies be able to truly understand how this legislation will directly affect them and start creating a comprehensive strategy.

However, whilst these details aren't yet confirmed,

tech companies who want to thrive alongside the changing landscape should start preparing themselves now and consider their roadmap to compliance to ensure a smooth transition when the time comes.

As a first step, this can be assigning one lead or a team that will familiarise themselves with what we know about the business today, and starting to make note of all aspects of the supply chain and current operators that may be impacted by the legislation. Knowing where different types of data that may be part of the DPP requirement are held puts companies in a good place to create a strategy once the delegated acts are published. Having a view of partners that will support your DPP integration and existing partners that will support relevant data collection would be a useful set-up activity to consider before a strategy stage.

By companies being proactive early on and preparing for the mandating of DPPs, a culture of collaboration, transparency, and environmental responsibility will be fostered amongst colleagues and consumers as all parties are provided with more pertinent information.

Looking to a future of eco-conscious practices The EU's initiative for a circular economy through the ESPR and mandating of DPPs marks a milestone commitment to lowering waste levels and provides hope for a more circular and sustainable economy. Understandably, this will prove disconcerting at first to companies placing products in the EU marketplace. However, the potential it holds for businesses to play an active role in supporting a more sustainable economy is an opportunity to grab with both hands. On this, businesses should look forward to the positive outcomes of their efforts, such as contributing to a sustainable future, validating their sustainability credentials, and optimizing supply chain efficiency.

By companies acting promptly and embracing the change now, through understanding the legislation and beginning their journey to compliance, there are numerous long-term gains for companies to become eco-conscious practices that play a pivotal role in ensuring a sustainable economy.



How insurgent financial services institutions are overtaking the giants of the sector

In a hyper-competitive environment, it is very often a company's ability to adopt new technology and turn it to profit quicker than their competitors which makes the key difference. A company's ability to deploy blockchain, migrate to the cloud, and develop effective Machine Learning (ML) or Artificial Intelligence (AI) models often indicates who succeeds and who falls behind. Financial Services are now in the midst of just such a struggle.

BY ALEKSI HELAKARI, HEAD OF TECHNICAL OFFICE, EMEA, SPIRENT



FINANCIAL SERVICES have long been early adopters and pioneers of new technology. It's a sector which combines the voluminous budgets, tight regulation and high intensity competition that often forces them to the forefront of innovation. They were among the first to really seize hold of technologies like Mainframe computers in the 50s and 60s to handle their oceans of transaction data. Moving ahead, they pioneered customer and data analytics to gain competitive edges in serving their customers. Technologies like Blockchain, mobile banking and digital wallets have marked recent years in the sector. It should be expected then, that automation and AI would be pioneered quickly and adeptly. Yet many financial services firms are

struggling to do so. That's not the case across the board. In fact, its larger well-established firms are struggling, while smaller organisations are leading innovation efforts in the sector.

Size and success is a double edged sword. The main cleavage in financial services between those that can successfully make use of AI and automation and those that can't is sheer size. The reality is that larger financial services are loaded with age-old processes, departmental silos, backdated data and legacy technologies which make automation and AI development exceedingly difficult for many. That unwieldy size creates a whole range of downstream problems which prevent many



larger financial services institutions from rolling out projects.

Really big data

Financial services live off of data - actuarial data, customer data, personally identifiable details, market projections and so on. In larger firms, different kinds of data will be used for different metrics, collected across different departments - and possibly geographical regions - for different purposes. It was likely collected at different times and stored in different places with different technologies, for different time periods. This is the first major problem that many will come to understand in developing their own AI and automation deployments. AI and automation require good, reliable and consistent data in order to perform and the fragmented operations and practices that characterise larger firms make that significantly more difficult.

Legacy technology

That fragmentation acquires yet another aspect when we start thinking about the legacy technologies which collect and use it. Despite their reputation, as pioneering early adopters, larger financial services firms still deal with a lot of legacy. This could be because these are load bearing legacy tools which many other parts of the organisation depend on, or it could merely be the favorite piece of kit of a particular specialist or department. In any case, this furthers the fragmentation that is hobbling AI or automation. These pieces of technology will have their own dependencies and metrics and often don't integrate with other technologies, much less the frameworks and models that automation and AI consist of. This ultimately has the effect of forcing "small pocket implementations" and deepening the silos which hold larger financial services companies back.

This just leads to a situation where you have a large organisation, with multiple different departments, collecting different kinds of data with different tools and technologies. On top of that those tools will often not integrate together and the department will often not share data. It will be prohibitively difficult to build an automated system on top of that, much less comprehensive AI systems.

Compliance

Ironically, one of the key reasons financial services want to start using AI and automation is to help them comply with regulation. The financial services industry is closely watched by all manner of regulations which cover fraud, insider trading, data privacy, market fairness and more. There are national regulations set by individual governments - such as the UK's Financial Services and Markets Act - along with sectoral regulations like PCI DSS. Given the international nature of financial services, it's likely that any sizable firm has to comply with regulations in multiple jurisdictions and across multiple borders. These requirements are both wide-ranging and thorough, threatening heavy penalties



for non-compliance. Not only do these regulations have to be complied with but efforts and records have to be extensively documented which is both yet another difficulty that financial services firms have in complying with regulations, and another reason they want to start using automation and AI.

On top of all of that, larger companies have to deal with both the regimes they're already compliant with as well as those which they'll have to in the future, paying special attention to those which look at AI such as the EU's forthcoming Artificial Intelligence Act.

Clearing house

The difference between larger, old financial services institutions and smaller, faster ones isn't hard to imagine. They are essentially dealing with brownfield sites in which they have to fundamentally restructure some of their most basic processes. Smaller counterparts - on the other hand - have greenfields to build on top of - allowing them to build faster and leaner. This doesn't just go for AI and automation, but all kinds of innovations too. Online banking and digital wallets were first rolled out by smaller start-up firms because they could do so without the incredible overhead that accumulates with time and, ironically, long-standing success.

Larger financial services firms will have a much bigger job ahead of them than their smaller counterparts, but they also need it more. They need to compete with a new generation of firms who can move with an agility that's currently hard for them and regulations are bearing down on them which are forcing them to innovate. That's going to involve tearing out and replacing some of the most basic systems, processes and technologies that they rely on. From the root, those larger firms will need to change some of the most basic ways they automatically collect, validate and manage data from across their organisation. This will be especially important for compliance, which often has to be thoroughly documented to prove that compliance. Technologies like automation and AI can't just be bolted on to pre-existing systems and processes. They offer profound benefits and they'll require profound restructuring in order to realise.



Here's why nobody's really ready for NIS2

Despite being published in late 2022 and coming into effect in January 2023, the second Network and Information Security Directive (NIS2) is taking the European Union by surprise. Weeks after the 17 October deadline, the majority of member states haven't transposed it into their written laws — a necessary step for organisations in those countries to know the expectations and penalties. The story of NIS2 is, in some ways, the story of all compliance regulations — and in some ways, it's completely unique.

OUTLINING wide-reaching measures from system hardening to reporting, training, and more, NIS2 isn't likely to be either simple or clean for member states or their constituent organisations; as the deadline for legislation shrinks in the rearview, companies are scrambling to get ready for whatever their member state has in store (with most IT departments pulling funds from other areas of the business to cover). The NIS2 Directive was published in November 2022; member states have had since January 2023 to figure out how to require it by law; now, most EU companies are left in the lurch, waiting to find out their exposure and risk. How does that happen?

Three reasons NIS2 compliance is taking the EU by surprise

1. NIS2 is not an instruction booklet

Like most compliance regulations, directives, and even some frameworks, NIS2 is not instructional in nature. Rather than outlining the specific configurations, tools, and steps organisations can use to get compliant, NIS2 seeks to define a secure end state for IT systems.

That's largely because every IT system (and team) is different, providing instructions for bringing

and keeping every component into compliance would be impractically complex. It's also partially by design: The more specific the requirements for compliance, the faster they become obsolete. The end result is that every stakeholder along the line is doing some degree of interpretation before they can action anything. This includes member states that need to decide how to work NIS2 into their laws, organisations in those member states that need to become compliant, and teams in those organisations responsible for putting compliant tools and practices in place.

2. Nobody wants another NIS1 — so nobody wants to rush into NIS2

The first NIS Directive (sometimes referred to with the retronym "NIS1") went ignored for so long by so many member states (and the companies operating within them) that the European Commission ensured that NIS2 made up for the deficiency.

To address the increasing risk level associated with critical systems and data, NIS2 regulators baked in recommendations for hefty fines and personal liability in noncompliant organisations. Ernst & Young



expects Ireland to impose a bevy of penalties, up to and including imprisonment for negligent C-level figures if their organisation fails a NIS2 audit.

Unlike NIS1, regulators also set expectations for the entire supply chain in NIS2, fostering a culture of cybersecurity through collaboration, vulnerability handling, training, and information sharing – not unlike some of the core tenets of the NIS2 contemporary Digital Operational Resilience Act (DORA). But NIS2 doesn't exist solely to punish. It was built with room for teeth to inspire long-term adherence to IT security standards in a world where cybersecurity is primarily reactive. As pointed out by my German colleague Marc Martin, EU regulators feel an increasing sense of social responsibility for mitigating cyber risk in critical industries which they govern. That's one reason why all EU countries have already agreed to a minimum baseline expectation for compliance that includes ramifications not found in NIS1.

3. Getting compliant could take months. Staying compliant will take forever

To be frank, no single individual requirement, control, or component of NIS2 compliance is likely to be truly groundbreaking. But the fact that NIS1 compliance is and was so inconsistent means that when laws enforcing NIS2 are passed by each member state, companies will likely still be scrambling to catch up. It also means that using proven, standardised tools now can get them much closer later.

Additionally, regulators are likely expecting companies to put system hardening measures in place, but not continuously maintain them. That's why audits never happen the same day you configure everything just right – they look for evidence of long-term security policy enforcement as well as repeatable, scalable processes for demonstrating compliance. (Consider that compliance percentage rates with some of the most well-known compliance regulations, like GDPR and PCI-DSS, remain abysmal, even decades after their introduction). Again, that's the point of regular audits: to ensure that once you've gotten secure and compliant, you can keep it up over time. Longevity is the true test of a GRC framework – and the one most organisations fail.

How to settle in for the long haul of NIS2 Build your GRC framework with proven standards

Where directives fail to provide instructions, IT security standards like CIS Benchmarks and Frameworks like NIST pick up the slack and can help you choose the right tools, processes, and configurations you need to enforce. Plus, many of these prescriptive resources are free, internationally recognised, and peer-reviewed for an added layer of reliability. With specific configurations for hardening software, hardware, and network components – down to the configuration level – they're your bridge from "not compliant" to "compliant." Additionally, seek common threads across regulations. If you've already used the controls outlined in one regulation



or framework, you might have already accomplished key controls of another (like NIS2).

Focus on the long term

If you create a NIS2-compliant GRC framework without a solid foundation of repeatable configurations built with proven standards, you're building a house on sand. Even if you pick the right tools and institute the right processes, don't assume you can just pass every NIS2 audit for years. Drift, employee turnover, knowledge gaps, and tech debt will pile up over time. Even if it were possible to prevent every single active, malicious attack, that continuous passive risk exposes you to the teeth of NIS2. Choosing tools you can manage and processes you can maintain in the long term also saves time down the road, when member states enter the perpetual 'auditing and enforcement' phase of NIS2.

Don't forget about scalability

Use the above recommendations to define and enforce a secure, compliant desired state – no matter how much you diversify or scale your critical IT infrastructure.

For example, when you roll out an automated patch two days before someone uncovers a new vulnerability in it, can you run a line of code and roll it back on every server running that version of the software? When someone inserts a backdoor into the latest version of the open source tool your infrastructure uses every day, how long will you let it cripple your NIS2 compliance posture?

If you've got some production workloads in AWS, some in a data centre, and some private cloud, can you keep the bolts tight on all of them from one infrastructure codebase? Or will you be forever configuring, tweaking, and chasing down configuration drift? And how do you expect to manage compliance for them all if each platform is controlled by a different vendor?

For all its enhanced penalties, potential implications, and years of hype, NIS2 compliance largely comes down to fundamentals. Organisations across the EU would do well to bear the weight of NIS2 with patience, persistence, and strategic investments that reduce the toil of maintaining a compliant state.