DIGITALISATION WORLD

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

ISSUE IV 2024

DIGITALISATIONWORLD.COM

WHY YOUR ENTERPRISE NEEDS AIOPS MORE THAN EVER

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

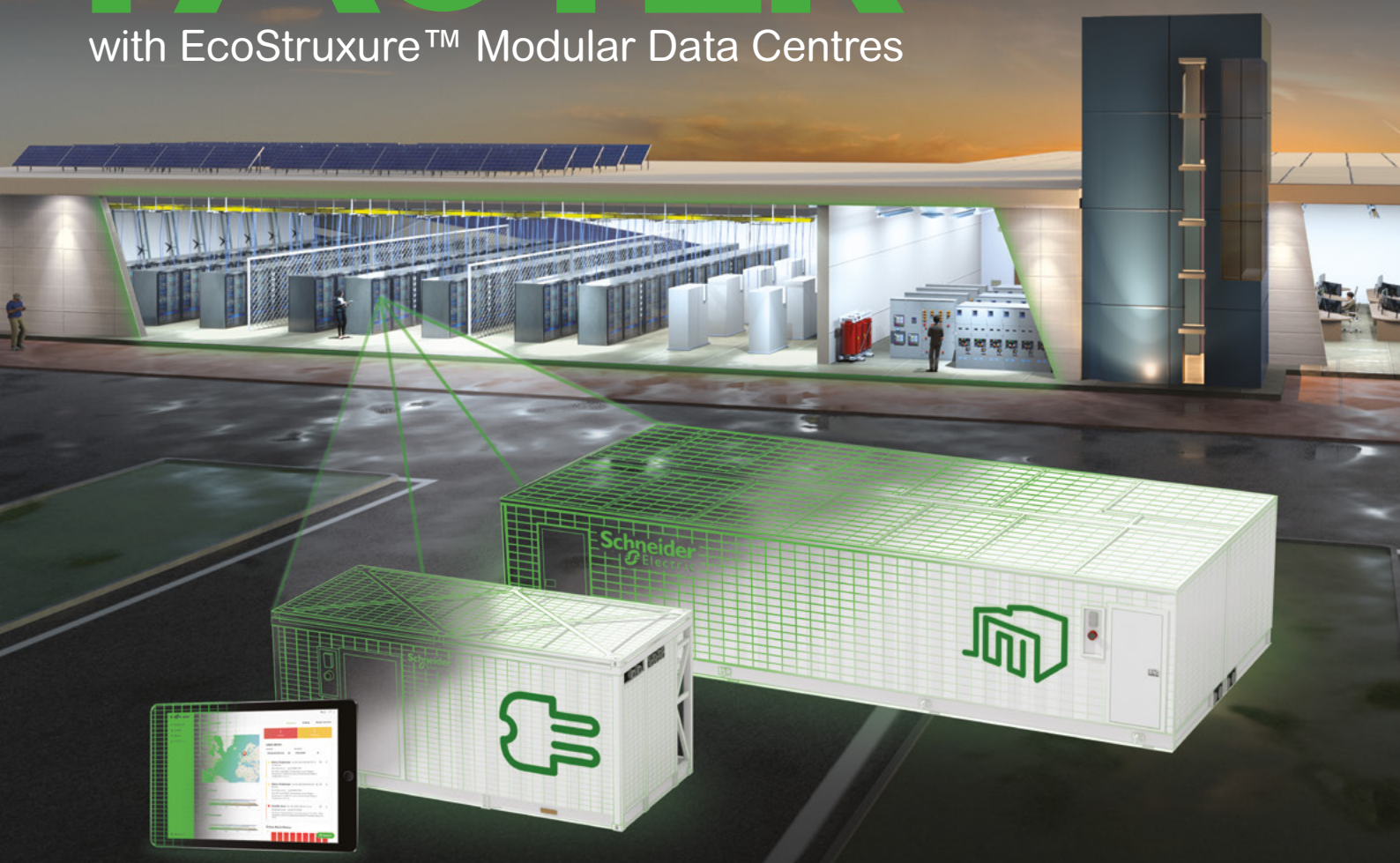
AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION

EcoStruxure™
Innovation At Every Level

Deploy your data centre

FASTER

with EcoStruxure™ Modular Data Centres



EcoStruxure Modular Data Centres are a smart alternative solution to overcome the traditional challenges of data centre builds.

Such as allocation of space, deployment in industrial environments, or the ability to scale capacity quickly - frees up other real estate or buildings to better support the organization's core function.

- Faster Deployment - Simplify the planning, construction, and implementation
- Flexibility to scale at a more granular level, resulting in less oversizing
- Prefabricated, pre-assembled and pre-tested in the factory prior to shipment.
- Delivered as functional building blocks of power, cooling, IT or all-in-one data centre
- Securely manage system from anywhere

Ready to get started with EcoStruxure Modular Data Centres?

se.com/datacentre

Life Is On | Schneider Electric

VIEWPOINT

By Phil Alsop, Editor

IT's all about building relationships

THERE'S A THEME running through several of the news stories in this issue of DW, which can broadly be summarised as 'understanding the importance of (good) relationships'. For many, this might seem rather obvious. However, with so much hostility, posturing and culture warfare pushed towards us by politicians and their compliant, complicit media outlets across the globe, joined by the anger and hatred which seems to be the fuel of so many social media platforms, the idea that we should seek out what brings us together, rather than what drives us apart, cannot be stated often enough.

Our first news story describes what happens when things go wrong – the finger pointing starts, with everyone trying to avoid the blame when things go wrong (back to our politicians here!), and pointing towards those who they want to take the blame. As most problem tend to be solved by some kind of collaboration, finger pointing is generally counter-productive.

When it comes to the importance of establishing good relationships, with suppliers, employees and customers, the words of Dr. Charlotte Armitage, as found in our second news story ('Return on relationships') say it all: "To maintain our own psychological and physical safety in the world, we choose to interact with those that we feel safe and secure around. Therefore, creating secure and meaningful relationships with employees and customers positions an organisation as a place that both parties wish to remain a part of."

Right now, that last bit – 'wish to remain a part of' – is particularly important when it comes to attracting and, importantly, retaining skilled IT staff. Ignore requests for flexible work, fail to update the office environment – well, don't be surprised if your employees choose to work elsewhere.

The idea of human-centred software is a new one to me That's to say, the idea that the software experience for users should be optimised for as many different individuals and groups as possible seems like common sense. But the phrase 'human-centred software' is helpful in so far as it seeks to formalise what many organisations like to think they are already doing, but probably aren't on a consistent basis.

In summary, no extraordinary insights from me this (or any other!) month, just a reminder that the world tends to work better when we look for common ground, rather than disagreement. That's true whether we're talking politics, the office, or the politics of the business world.

CONTENTS

ISSUE IV 2024

DW DIGITALISATION WORLD

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.

ISSN 2396-9016 (Online)

Return on relationships: The metric every business leader should be tracking in 2024

New research from Gamma reveals the tactics successful businesses are using to stay ahead, with psychological insight as to why they make a difference.

RESEARCH commissioned by leading UCaaS provider, Gamma, has demonstrated that despite challenging market conditions, there is still room for businesses to thrive. Human factors are revealed to be central to commercial success; with almost three quarters (72%) of business leaders believing that good rapport is more important than price and capabilities when choosing a partner or supplier.

Most businesses recognise the importance of relationships, but not all are delivering on this. For those who practise what they preach, strong relationships are a key predictor of business success.

When comparing businesses whose revenue had grown in the last twelve months versus those whose revenue had declined, there was a clear gap in performance on the reported strength of relationships between customers and colleagues. Nearly three-quarters (73%) of leaders in growing companies felt they had strong relationships with clients, with 64% saying the same for colleagues, compared to 61% and 52% respectively in businesses experiencing declining revenues.

When evaluating business success, research revealed that businesses who reported a growth in revenue over the last 12 months were performing best across:

- Delivering effective problem resolution (74%)
- Providing consistent high-level products and services (70%)
- Building and maintaining good personal relationships with clients (69%)
- Offering valuable advice to businesses (68%)

Respondents whose revenue had declined in the last 12 months agreed that more client feedback (48%) and a greater focus on customer service over profit (37%) would help them to form better relationships with clients.

There was also clear connection between success and culture, with successful businesses more likely to rate their workplace's culture highly in comparison to those who had not performed well (67% vs 55%), and three-quarters (75%) agreeing that strong relationships with colleagues are equally key to business success.

With half of business leaders (51%) acknowledging that staff churn was a factor in losing clients, and over a third (37%) of total respondents admitting they are considering a career change in the coming year, greater emphasis on building positive working relationships should be a priority for businesses in 2024.

In response to these findings, Gamma has identified a metric which tracks this correlation between strong relationships and revenue growth; 'Return on Relationships' (RoR); and has built a calculator to help businesses evaluate their performance.

Dr. Charlotte Armitage, a business psychologist, explains the value in good business relationships from a psychological standpoint: "Relationships form the basis of our existence as humans, we are inherently social beings and require meaningful connections for survival. "

"To maintain our own psychological and physical safety in the world, we choose to interact with those that we feel safe and secure around. Therefore, creating secure and meaningful relationships with employees and customers positions an organisation as a place that both parties wish to remain a part of."

Psychology can also help us create better relationships. Dr Armitage explains why businesses should prioritise trust to maximise their RoR: "Trust is fundamental in any relationship and takes time to build. To develop trust, individuals need to feel safe, and that you are stable and predictable. If you can offer this predictability and remain consistent over time, demonstrating integrity when needed, it forms a good basis for a trusting relationship to be built."

Andrew Belshaw, CEO at Gamma, comments: "Connectivity isn't just about technology; it's about people. Successful businesses thrive when their communications have genuine human connections, leading to meaningful customer experiences. Our research clearly shows that success is closely tied to investing in strategies that build trust and confidence among colleagues and customers."

"It's an approach we have been living and breathing for years, in our own relationships with our customers and in the solutions we offer them. Return on Relationships (RoR) is something we take very seriously because we understand that good relationships make good business sense."

Critical operations at risk

War room style incident management is driving IT teams in nearly 50% of organisations to experience burnout.

DYNATRACE has warned that organisations are putting their critical operations at risk by enabling the widespread continuation of a "blame game" culture between their IT teams and third-party service providers. A new survey found that 91% of organisations are still playing the "blame game" with IT service providers when problems occur. This increases the reliance on war-room-style meetings to identify and resolve the cause of problems, which extends the duration of incidents and creates tense workplace environments that heighten the risk of losing skilled talent.

Nearly half (49%) of IT teams have been left feeling burned out by war rooms, 46% have missed personal time during evenings and weekends, and one in five (21%) have considered a change in job role or career due to added stress. If these trends continue, organisations could be putting their critical operations at risk, as they find themselves with a shortage of skilled developers and operations professionals to deliver digital services and accelerate innovation.

"War rooms are an extremely negative approach to resolving problems, and against the backdrop of continued skills shortages, can significantly deepen resourcing challenges for many organisations," said Rob Van Lubek, Vice President, EMEA at Dynatrace. "What looked like 'business as usual' five years ago is no longer acceptable for many IT professionals, who reassessed their work-life balance during the shift to hybrid working. The high-stress environment of war rooms and the looming threat of emergency conference calls at any hour of the day can lead to a disenfranchised and disengaged workforce that is constantly on the lookout for their next employer."

Reliance on siloed monitoring tools and manual processes within many organisations amplifies the challenges inherent to war rooms. Less than a third (29%) of organisations say teams use a single platform and the same data to monitor and manage digital services. This means everyone is working from their version of the truth, which fuels the cycle of blame between teams. As a result, these teams are more reluctant to take ownership of problems, which increases the risk that incidents take longer to resolve or, worse, are ignored entirely.

"Organisations need to transform the way their teams work and collaborate, both internally as well as with third parties," continued Van Lubek. "The best way of enabling a culture of collaboration across IT, business, development, and security teams is to adopt a unified observability strategy that provides a single source of truth that teams can use to make decisions and work cross-functionally. This approach helps teams become more proactive in their incident response. In addition, embracing advanced AI and automation as part of this approach helps streamline processes by eliminating manual triaging and equipping teams with solutions to diagnose and resolve problems before they become crises. This significantly reduces stress, eliminates wasted spending, and boosts productivity, allowing teams to spend less time in war rooms and more time innovating."

Organisations need to transform the way their teams work and collaborate, both internally as well as with third parties. The best way of enabling a culture of collaboration across IT, business, development, and security teams is to adopt a unified observability strategy that provides a single source of truth that teams can use to make decisions and work cross-functionally

Average of 90 AI-apps built per day in 2023

Snowflake report unearths Python as the programming language of choice for AI development, while the processing of unstructured data has increased by 123 percent in the past year.

LARGE LANGUAGE MODELS (LLMs) are increasingly being used to create chatbots, according to Data Cloud company Snowflake. As generative AI continues to revolutionize the industry, chatbots have grown from being approximately 18 percent of the total LLM apps available, to now encompassing 46 percent as of May 2023 — and that metric is only climbing.

In addition, after surveying Streamlit's developer community, it was found that nearly 65 percent of respondents noted that their LLM projects were for work purposes, signaling a shift in the importance of harnessing generative AI to improve workforce productivity, efficiency, and insights.

These results are based on usage data from more than 9,000 Snowflake customers, and summarized in Snowflake's new "Data Trends 2024" report. The report focuses on how global enterprise business and technology leaders are leveraging resources such as AI to build their data foundation and transform future business operations. The new data shows a shift from LLM applications with text-based input (2023: 82%, 2024: 54%) to chatbots with iterative text input, offering the ability to have a natural conversation.

"Conversational apps are on the rise, because that's the way humans are programmed to interact. And now it is even easier to interact conversationally with an application," explains Jennifer Belissent, Principal Data Strategist at Snowflake.

"We expect to see this trend continue as it becomes easier to build and deploy conversational LLM applications, particularly knowing that the underlying data remains well governed and protected. With that peace of mind, these new interactive and highly versatile chatbots will meet both business needs and user expectations."

Over 33,000 LLM applications in nine months

The report also shows that 20,076 developers from Snowflake's Streamlit community of developers have built over 33,143 LLM apps in the past nine months. When it comes to developing AI projects, Python is the programming language of choice due to its ease of use, active community of developers, and vast ecosystem of libraries and frameworks.

In Snowpark, which enables developers to build apps quickly and cost-effectively, the use of Python grew significantly faster than that of Java and Scala (in the past year)— Python grew by 571 percent, Scala by 387 percent, and Java by 131 percent. With Python, developers can work faster, accelerating prototyping and experimentation—and therefore overall learnings as developer teams make early forays into cutting-edge AI projects.

In terms of where application development is taking place, the trend is towards programming LLM applications directly on the platform on which the data is also managed. This is indicated by a 311 percent increase in Snowflake Native Apps – which enables the development of apps directly on Snowflake's platform – between July 2023 and January 2024. Developing applications on a single data platform eliminates the need to export data copies to third-party technologies, helping develop and deploy applications faster, while reducing operational maintenance costs.

Data governance in companies is growing in importance

With the adoption of AI, companies are increasing analysis and processing of their unstructured data. This is enabling companies to discover untapped data sources, making a modern approach to data governance more crucial than ever to protect sensitive and private data.

The report found that enterprises have increased the processing of unstructured data by 123 percent in the past year. IDC estimates that up to 90 percent of the world's data is unstructured video, images, and documents. Clean data gives language models a head start, so unlocking this untapped 90 percent opens up a number of business benefits.

"Data governance is not about locking down data, but ultimately about unlocking the value of data," said Belissent. "We break governance into three pillars: knowing data, securing data and using data to deliver that value. Our customers are using new features to tag and classify data so that the appropriate access and usage policies can be applied. The use of all data governance functions has increased by 70 to 100 percent. As a result, the number of queries of protected objects has increased by 142 percent. When the data is protected, it can be used securely. That delivers peace of mind."

Modernising offices key to enhancing hybrid work and productivity

72% of employees are positive about returning to the office, but want better-equipped spaces for collaboration and brainstorming.

CISCO has unveiled findings from a survey that details how the reality of the in-office experience compares to employee expectations around the globe, and how employers are investing in AI as a transformative tool for workplace collaboration and productivity.

The report shows that while employees are positive about the return to the office, they find that the spaces are too focused on individual work, rather than environments that foster collaboration and creativity.

As global companies transition to hybrid models, employers and employees alike recognize the need for office spaces that encourage collaboration and innovation.

Employers agree that technology and AI investments are essential to enhancing productivity and attracting top talent, but few have strategies to implement the technology throughout their organization.

“Making the office a magnet means creating experiences that employees value,” said Cisco Executive Vice President and General Manager of Security and Collaboration, Jeetu Patel. “To achieve this, organizations must embed hybrid work solutions, infused with AI, into office spaces to foster collaborative experiences for everyone.”

Key survey findings from 14,050 employees and 3,800 employers in 19 countries include:

- **Employees seek in-office collaboration:**
  The report reveals a surprising truth: employees feel positively about returning to the office, provided the spaces support seamless collaboration, social interaction and creative brainstorming. While 72% of employees are positive about returning to the office, only 47% believe their work environments are equipped for this new era of hybrid work. It’s time to advocate for and design office spaces that truly support the ways employees want to work together.

- **Office tech needs to change to enable collaboration:**
  85% of employers say that most of their office space is allocated to personal working spaces, creating individual working environments and encouraging individual working habits. Technology infrastructure and integration is a major area of concern across the globe, with ineffective meeting rooms due to inadequate audio and video technology hindering productivity and collaborative efforts. Among employers who find meeting rooms ineffective in boosting in-office productivity, the main reason is insufficient audio and video endpoints, with 41% in the Americas, 52% in Asia Pacific and 42% around Europe.

- **Employers will invest in office design and tech to attract top talent:**
  81% of employers have already or plan to redesign workspaces in the next 24 months. But these enhancements are not just cosmetic; 90% of employers in the Americas, 94% in Asia Pacific and 85% in European countries report that collaboration-driven workspace enhancements are highly or moderately effective at attracting and retaining top talent. This is a testament to the belief that the right environment can be a powerful draw for a skilled workforce.

- **Organizations realize the value of AI to increase productivity:**
  Employers are making a strong commitment to integrating AI into the workplace. By 2025, 73% will invest in AI-powered collaboration software, with 68% planning to enhance their workspaces with AI technologies. 80% of employers plan to invest in AI for workspaces and collaboration by the end of 2025, recognizing the potential of AI to revolutionize the working environment. This underscores the need to accelerate AI adoption within the workplace to enhance productivity and create a future-ready office environment.

- **Employers must focus on closing the AI skills gap:**
  While 43% of employees have access to AI technologies, less than half feel proficient in using them. With 1 in 4 employees not well prepared to use AI, this highlights the need for training and that businesses must select AI that meets both the organization and individual team’s needs.

Warning that carbon offsets market fosters greenwashing, not sustainability

Energy efficiency experts from Exergio expose the pitfalls of the carbon offsets market, showcasing how it allows greenwashing rather than sustainability. They propose that independent entities should be able to certify companies' sustainability efforts and emission reductions according to set standards.

IN A WORLD increasingly concerned with environmental impact, the carbon offsets market - which allows companies to compensate for their carbon emissions by investing in projects that reduce or remove greenhouse gases elsewhere - has seemingly emerged as a pivotal player in mitigating climate change. However, recent developments indicate a troubling trend: the potential for greenwashing, rather than genuine sustainability, to dominate the landscape.

For instance, according to some energy and sustainability experts, when companies fail to address their own CO2 emissions from producing cosmetics or cars and instead opt to plant trees, it does not render them or their products truly "climate neutral" or "eco-friendly.

With the EU's directive to ban misleading environmental claims on the horizon, experts are sounding the alarm on the urgent need for independent sustainability certification in the carbon offsets market.

"While we appreciate the forthcoming directive, sustainability advocates are facing a pressing dilemma. The current trajectory suggests that waiting for two more years is a luxury we cannot afford. Originally intended to advocate for nature and sustainability, carbon emission offsets have instead become a tool for creating a false facade of corporate sustainability, often without substantive action. The unregulated nature of the market only exacerbates these concerns, leaving many frustrated with its misleading results in terms of reducing CO2 emissions," explains Donatas Karčiauskas, CEO of Exergio, a company dedicated to providing sustainable solutions for commercial buildings to combat energy waste. The carbon offsets market, once seen as a symbol of environmental sustainability, is also under scrutiny for becoming more profit-oriented. With its current valuation surpassing $2 billion and growing rapidly, concerns arise that this expansion prioritizes financial gain over genuine environmental stewardship.

Initially designed to offset greenhouse gas emissions by investing in projects such as reforestation and renewable energy, the market has failed to significantly impact the environment as intended. Reports indicate that up to 90% of rainforest carbon offsets may be ineffective, highlighting the urgent need for standardized parameters to quantify reductions in CO2 emissions accurately. "The solution is to have independent entities that could certify a business's sustainability efforts and emission reductions based on preset rules or parameters. At Exergio, we address this challenge by installing an AI-based solution in commercial buildings. These systems continuously monitor various building systems and devices, providing real-time data analysis. With this approach, we can accurately quantify energy savings and demonstrate tangible contributions to sustainability," elaborated Karčiauskas.

There is no universally recognized official certification for carbon emissions in the real estate sector. The market remains largely unregulated, leading to concerns about the effectiveness and reliability of some offset projects. As a result, there is an ongoing debate and calls for more stringent regulation and oversight to address issues such as double-counting and the effectiveness of offset projects.

"Unfortunately, the current state of affairs allows anyone to obtain a certification document from an unregulated market, claiming they are climate neutral. For a building to become a green asset, a self-bought BREEAM certificate is enough. This loophole may persist in the EU for at least the next two years. This approach fails to address the global challenge, as comprehensive regulations are not yet in place worldwide," Karčiauskas concluded.

Report reveals IM helps with AI benefits

Findings suggest a comprehensive IM strategy may also help overcome top challenges organisations faced during AI implementation, including unintended data exposure and data quality issues.

AvePOINT has published the results of its inaugural AI and Information Management Report in collaboration with the Association for Intelligent Information Management (AIIM) and the Centre for Information Policy Leadership (CIPL). AvePoint surveyed over 750 digital workplace leaders across the world and industries and found that nearly every organization experiences challenges when implementing artificial intelligence (AI), with the top challenge being issues with data quality. However, organizations with more mature information management (IM) strategies are 1.5x more likely to realize benefits from AI than those with less mature strategies.

According to the survey, fewer than half of organizations are confident they can use AI safely today. In addtion:
Before implementing AI, 71% of organizations were concerned about data privacy and security, while 61% were concerned about quality and categorization of internal data.
Fewer than half have an AI Acceptable Use Policy, despite widespread use of publicly available generative AI tools (65% of organizations use ChatGPT and 40% use Google Gemini today).

When implementing AI, 45% of organizations encountered unintended data exposure, meaning one of their biggest concerns became reality.
Said Chris Shaw, UKI&SA Country Channel Manager at AvePoint, “Our survey reveals that many organisations struggle with information management and data privacy, and these problems are only going to get worse as reliance on AI increases and more data is produced,” said Chris Shaw, AvePoint.

“Working with AvePoint, channel partners can provide a comprehensive data privacy and management strategy to their customers so they can continue to thrive in the digital workplace.”
“Unsurprisingly, data privacy and security were among the top concerns for organizations before implementing AI,” said Dana Simberkoff, Chief Risk, Privacy and Information Security Officer, AvePoint. “The reality is that not enough organizations have the proper policies in place today, which exposes them to risks that could be mitigated, if they better protect and govern their data and educate their employees on the safe usage of this technology.”

The survey exposed contradictions in organizations’ perception of readiness for AI compared to their reality. Many companies experience gaps in data readiness and information management that have already or will pose significant obstacles to safe and successful AI implementation.

88% of organizations report they have an IM strategy in place, but 44% lack basic measures such as archiving and retention policies and lifecycle management solutions. Just 29% of organizations use automation in most aspects of their IM strategy. But data volume is growing, with 64% of organizations managing at least 1 petabyte of data and 41% managing at least 500 petabytes of data.

When implementing AI, 52% of organizations faced challenges with internal data quality.

“The amount of data companies are generating and must manage is growing rapidly, and this will only accelerate as more organizations utilize AI technology,” said Alyssa Blackburn, Director of Information Management, AvePoint. “If organizations don’t establish or adapt their information management strategies, the challenges they are already facing will be exacerbated by AI. The good news is, 77% of organizations recognize they must implement additional strategies to keep pace with AI, which is a promising step in the right direction.”

Additionally, effective IM strategies can lead to a meaningful return on AI investments, according to the survey. Organizations with mature IM strategies are 1.5x more likely to realize benefits from AI than those with less mature strategies.

Despite this correlation, not enough organizations acknowledge the value of information management in AI success, with only 17% recognizing a robust IM strategy as the most effective way to ensure ROI on their AI investments.

“We are pleased to support this important study, which confirms the importance of an information management strategy to successful AI implementation and operationalization,” said Tori Miller Liu, CIP, President & CEO, Association for Intelligent Information Management (AIIM). “The data shows that organizations who invest in their information management strategy can realize the benefits of AI faster than organizations who lack a comprehensive information management strategy.”

This year, organizations are significantly increasing their investments in AI, with 83% planning to increase their AI spending and 79% investing in licensed AI such as Copilot for Microsoft 365.
In addition, 60% of organizations plan to allocate at least a quarter of their technology budget to AI in the next 5 years. However, less than half of organizations (46%) offer AI-specific training, hindering their employees from safely using and optimizing this technology.

“As organizations increase their investment in AI, a comprehensive and holistic accountability program for both data privacy management and AI governance is even more critical,” said Bojana Bellamy, President, Centre for Information Policy Leadership (CIPL).

IT professionals list shortage of skilled workers as their top challenge in 2024

Compared to 2023, 24% more IT professionals reported planned investment in automation in 2024, and 96% are using at least one AI or ML tool to improve efficiency.

AUVIK has released the results of its IT Trends 2024: Industry Report, an annual report in which 2,100 internal IT and MSP professionals are surveyed on top trends and challenges impacting IT teams. The 2024 report reveals a lack of skilled workers is the top challenge for IT teams. As a result, teams are prioritizing automation, outsourcing to managed service providers (MSPs), and adopting new tools to seek improved productivity and reduce the burden on front-line technicians handling an onslaught of end-user requests.

Automation is Key Amid Challenges
One of the report's key findings is an increased focus on adopting automation, including AI and ML tools, to address the needs of overworked and understaffed IT teams. Driven by persistent talent shortages, resource constraints, and the complexity of managing numerous tools, automation is emerging as a critical solution for enhancing end-user experiences and bridging the gap for both MSPs and internal IT departments.

Compared to the results of the 2023 report, 24% more IT professionals reported planned investments in automation in 2024, and almost all (96%) of IT professionals are using at least one AI or ML tool today. However, on average, 29% of network and SaaS related tasks are still done mostly or completely manually. With the majority (64%) of internal IT departments spending up to 50% of their working hours resolving end user requests, the use of automation can alleviate workload and allow them to focus on other priorities. Many IT professionals are also outsourcing network-related tasks or functions to address workforce shortages, with nearly three out of four respondents sharing that at least some of these tasks are being delegated to external entities such as MSPs.

"The trends toward automation and outsourcing when it comes to network management echoes what we are hearing from our customers—a desire for frictionless IT," said Doug Murray, CEO, Auvik. "IT professionals and MSPs want to be able to embrace change, introduce innovative technology into their environments, and reduce the huge amount of time their teams are currently spending on menial tasks. Automation allows them to do more with less and free up time and resources to focus on more strategic projects, while ensuring the day-to-day runs smoothly and employees still enjoy a seamless user experience."

Discrepancies between C-suite and IT perceptions

The strain on frontline IT workers is also creating significant gaps between how upper management and practitioners view current IT struggles. For example, nearly 58% of C-suite respondents indicated they were highly confident that their organization's network toolset meets the needs of remote workers, while only 35% of IT technicians reported this same confidence.

"So many IT technicians are understaffed and overburdened, and this is causing a rift within organizations of how end-user satisfaction is prioritized," continued Murray. "46% of C-suite executives list customer satisfaction as the most important metric, while only 26% of technicians echoed this sentiment. The data around configuration management indicates a similar discrepancy when it comes to prioritizing security and compliance. We interpret this as a clear call for help from IT teams for better resources and tooling, to allow full alignment within organizations on the issues that matter most."

Growing investment in IT

Another top trend is a focus on investments in IT, particularly in the areas of cloud security, network security, and cloud management. The majority (86%) of respondents reported increased budgets in 2024, with nearly 50% saying they expect to see an increase of at least 20% from 2023. In terms of specific investments, 48% of survey respondents shared that they are investing most heavily in SaaS monitoring and management tools, 46% shared that they are investing in Wi-Fi management, and another 46% shared they are investing in cloud monitoring and management. The number of respondents with planned investments has grown in every area surveyed since 2023, but network automation has seen the largest growth; compared to 2023, 24% more IT professionals are reporting planned investments in this area.

MANAGED SERVICES SUMMIT BENELUX

2 JULY 2024

NOVOTEL AMSTERDAM CITY
AMSTERDAM NETHERLANDS

THE MANAGED SERVICES SUMMIT EUROPE is the leading managed services event for the European IT channel.

The event features conference session presentations by specialists in the sector and leading independent industry speakers from the region, as well as a range of sessions exploring technical and operational issues.

The panel discussions and keynotes are supported by extensive networking time for delegates to meet with potential business partners.

This C-suite event will examine the latest trends and developments in managed services and how they have influenced customer requirements and the ability to create value through managed services for your organisation and customers.

THEMES, TOPICS & TRENDS

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

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

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

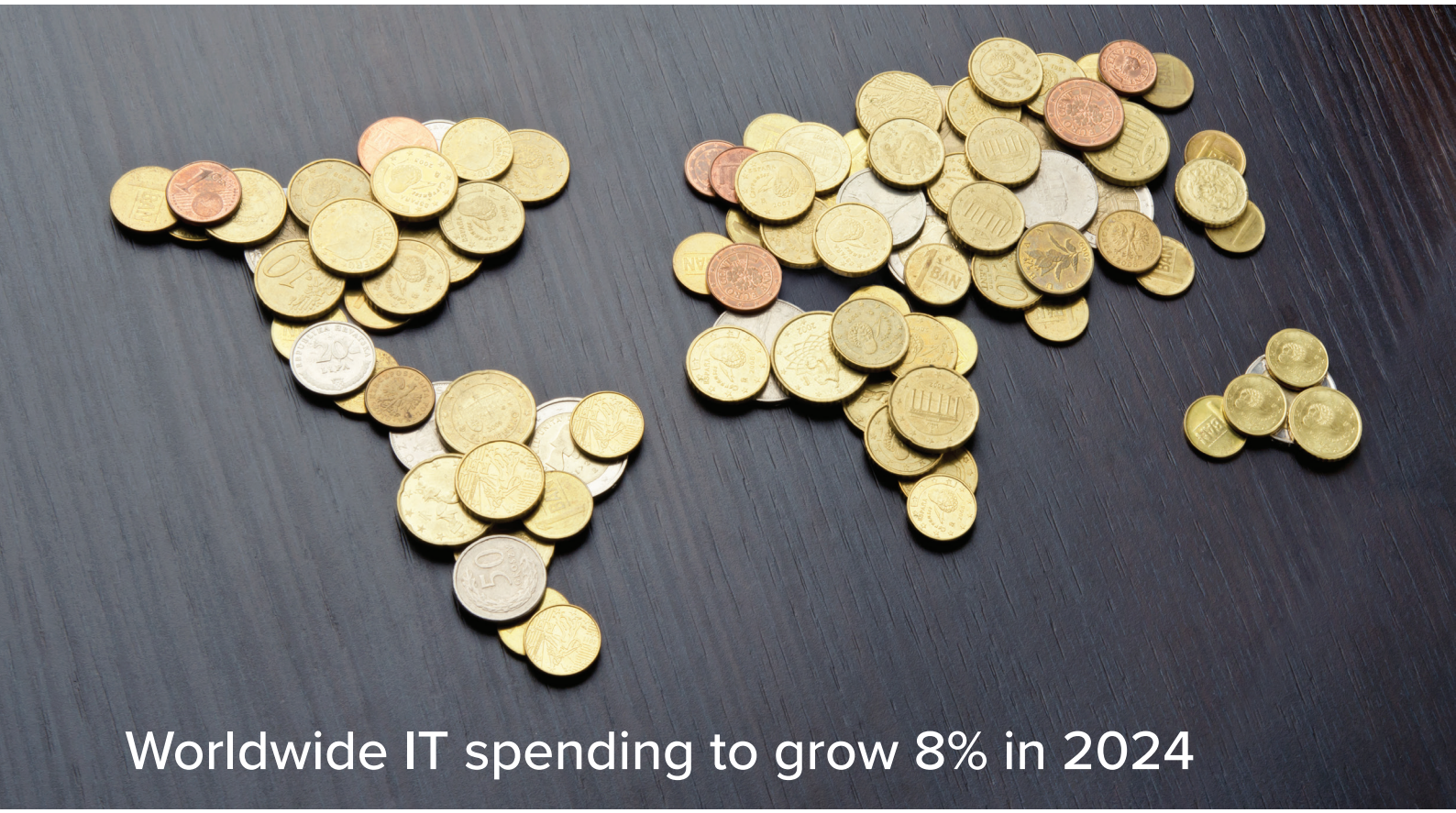
Sukhi Bhadal
sukhi.bhadal@angelbc.com
+44 (0)2476 718970

Peter Davies
peter.davies@angelbc.com
+44 (0) 1923 690211

Mark Hinds
mark.hinds@angelbc.com
+44 (0)2476 718971

https://europe.managedservicessummit.com

Angel BUSINESS COMMUNICATIONS · IT EUROPA · ANGEL EVENTS



Worldwide IT spending to grow 8% in 2024

Worldwide IT spending is expected to total $5.06 trillion in 2024, an increase of 8% from 2023, according to the latest forecast by Gartner, Inc. This is an increase from the previous quarter's forecast of 6.8% growth and puts worldwide IT spending on track to surpass $8 trillion well before the end of the decade.

"WITH SPENDING ON IT services on track to grow by 9.7% to eclipse $1.52 trillion, this category is on pace to become the largest market that Gartner tracks," said John-David Lovelock, Distinguished VP Analyst at Gartner. "Enterprises are quickly falling behind IT service firms in terms of attracting talent with key IT skill sets. This creates a greater need for investment in consulting spend compared to internal staff. We are at an inflection year for this trend, with more money being spent on consulting than internal staff for the first time."

Data center systems investment illustrates shift in focus to GenAI spending

Spending on data center systems is expected to see a notable jump in growth from 2023 (4%) to 2024 (10%), in large part due to planning for generative AI (GenAI) (See Table 1).

"We are seeing a cycle of story, plan, execution when it comes to GenAI. In 2023, enterprises were telling the story of GenAI and in 2024 we are seeing most of them planning for eventual execution in

	2023 Spending	2023 Growth (%)	2024 Spending	2024 Growth (%)
Data Center Systems	236,179	4.0	259,680	10.0
Devices	664,028	-9.1	687,943	3.6
Software	914,689	12.6	1,042,174	13.9
IT Services	1,385,120	6.1	1,519,928	9.7
Communications Services	1,487,161	3.3	1,551,288	4.3
Overall IT	4,687,177	3.8	5,061,013	8.0

Source: Gartner (April 2024)

Table 1. Worldwide IT Spending Forecast (Millions of U.S. Dollars)

2025," said Lovelock. "Technology providers are required to be a step ahead of this cycle and are already in the execution phase. They are bringing GenAI capabilities to existing products and services, as well as to use cases being identified by their enterprise clients.

"There is also gold rush level spending by service providers in markets supporting large scale GenAI projects, such as servers and semiconductors," said Lovelock. "In 2024, AI servers will account for close to 60% of hyperscalers total server spending."

Devices expected to bounce back in 2024

The average lifespan for mobile phones is shortening and consumers and enterprises are replacing mobile phones earlier. This change allows device spending to achieve $688 billion during 2024, up from 2023 spending lows of $664 billion, which will represent a 3.6% growth rate. The integration of GenAI capabilities in premium and basic phones sustains, more than drives, this change.

AI code assistants on the rise

By 2028, 75% of enterprise software engineers will use AI code assistants, up from less than 10% in early 2023, according to Gartner, Inc. Sixty-three percent of organizations are currently piloting, deploying or have already deployed AI code assistants, according to a Gartner survey of 598 global respondents in the third quarter of 2023. AI code assistants enable more capabilities that go beyond code generation and completion.

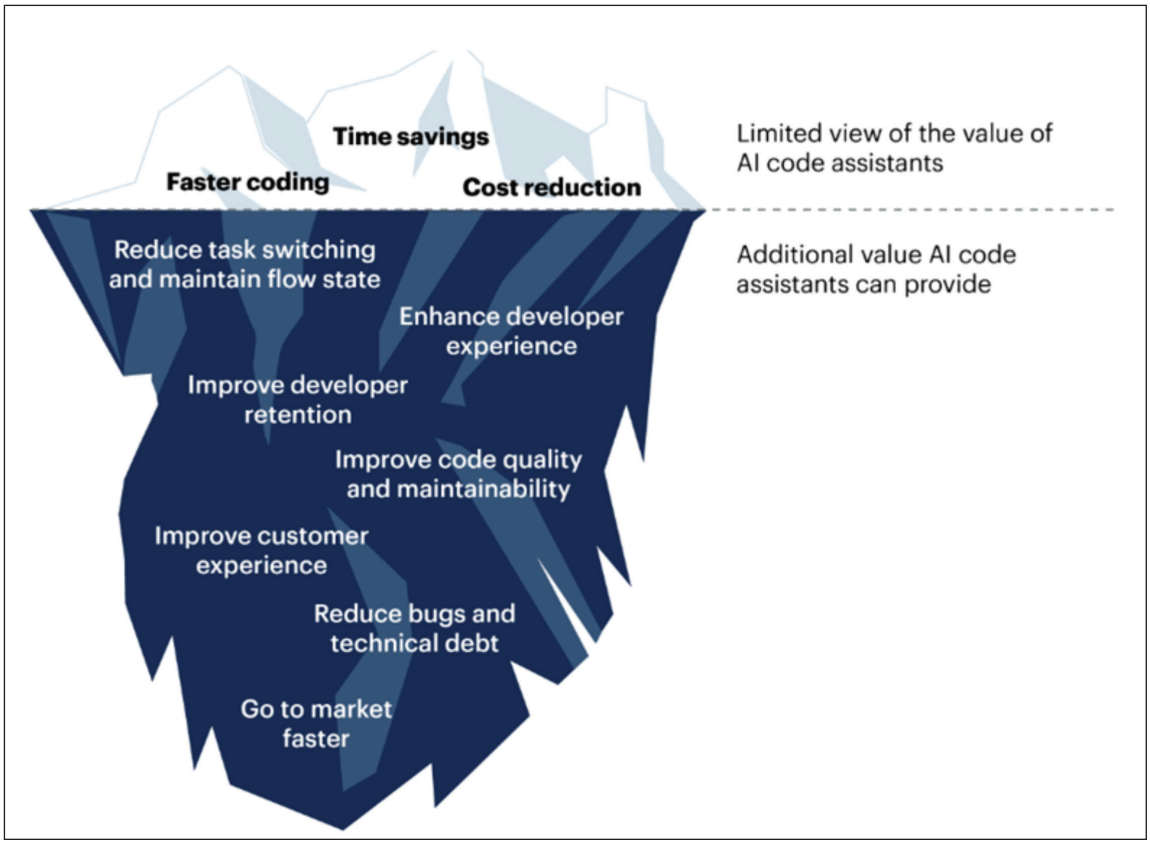
They are collaborative assistants that improve developers' efficiency by stimulating brainstorming and increasing code quality enhancements which empower developers to continuously upskill and build proficiency across programming frameworks. The enablers offered by AI code assistants lead to increased job satisfaction and retention, thereby saving the costs associated with turnover.

"Software engineering leaders must determine ROI and build a business case as they scale their rollouts of AI code assistants," said Philip Walsh, Sr Principal Analyst at Gartner. "However, traditional ROI frameworks steer engineering leaders toward metrics centered on cost reduction. This narrow perspective fails to capture the full value of AI code assistants."

Reframing ROI conversations is critical to capture the full value of AI code assistants

Traditional ROI frameworks fail to capture the full value of AI code assistants. To build an effective value story extending beyond traditional ROI metrics, software engineering leaders must reframe the ROI conversation from cost reduction to value generations (see Figure 1).

"Calculating time savings on code generation is a good place to begin building a more robust value story," said Walsh. "To convey the full enterprise value story for AI code assistants, software engineering leaders should connect value enablers to impacts, and then analyze the overall return to the organization."



➤ Figure 1. Value of AI code assistants. Source: Gartner (April 2024)

Spending on GenAI solutions in Europe to exceed $30 billion in 2027

According to the latest release of the Worldwide AI and Generative AI Spending Guide (v1 2024) published by International Data Corporation (IDC), the European AI and generative AI (GenAI) market will reach almost $47.6 billion in 2024 and record a compound annual growth rate (CAGR) of 33.7% over the 2022-2027 forecast period. Europe represents around one-fifth of the global AI market.

WHILE THE SHARE of GenAI reached only 9.6% of the total European AI market in 2023, it is increasing rapidly. Spending on GenAI will grow more than three times as fast as spending on the rest of the artificial intelligence market, and as a result, GenAI will represent more than a quarter of the total European AI market in 2027.

Software will be the largest technology segment in 2024, with a market value higher than hardware and services combined. Furthermore, it is expected to present the fastest growth in the 2022-2027 period, driven by demand for AI applications and platforms. The share of hardware technologies will decrease during the period in favor of software technologies, with the exception of the software and information services industry, in which the hardware component remains the largest, due to specific AI infrastructure provisioning use cases that characterize this industry.

AI adoption is already widespread, and companies are demonstrating their willingness to expand that adoption to GenAI. According to the IDC EMEA Cross-Industry Acceleration Survey run in December 2023, one out of three companies are already using or are planning to use AI solutions in the following 24 months. The maturity of adoption is the result of a need to optimize business processes with a clear focus on customers and employees. Indeed, AI solutions proved to be successful in boosting customer experience as well as improving employee productivity. On the other hand, adoption is facing challenges primarily related to the broad integration of AI into the organization and their ethical use.

“Artificial Intelligence, as well as generative AI applications, should become fully integrated into the business, accompanied by responsible use,” says Carla La Croce, research manager, Customer Insights and Analysis, IDC. “Realizing the full

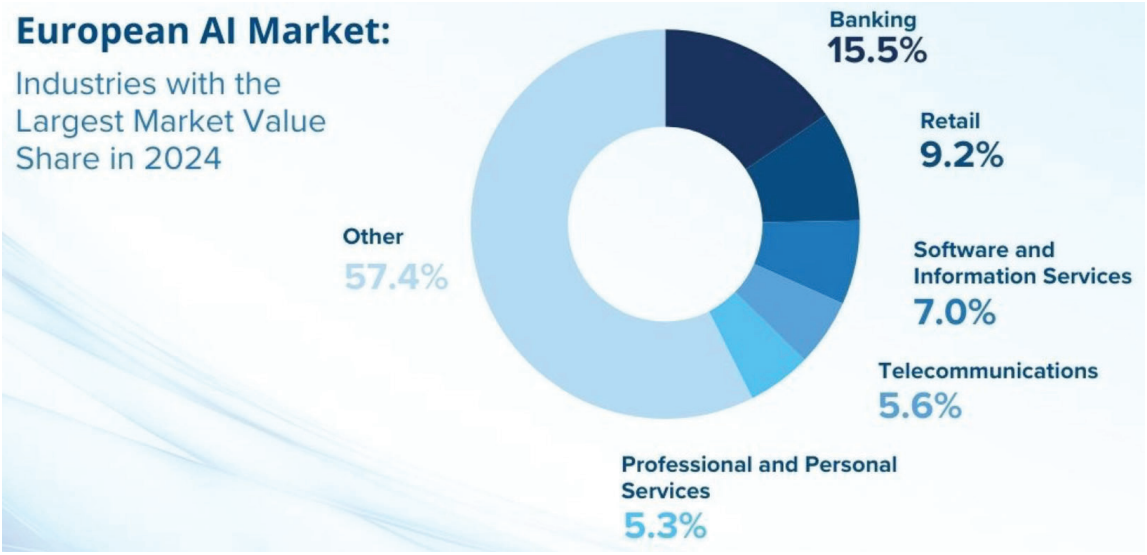


Figure 1

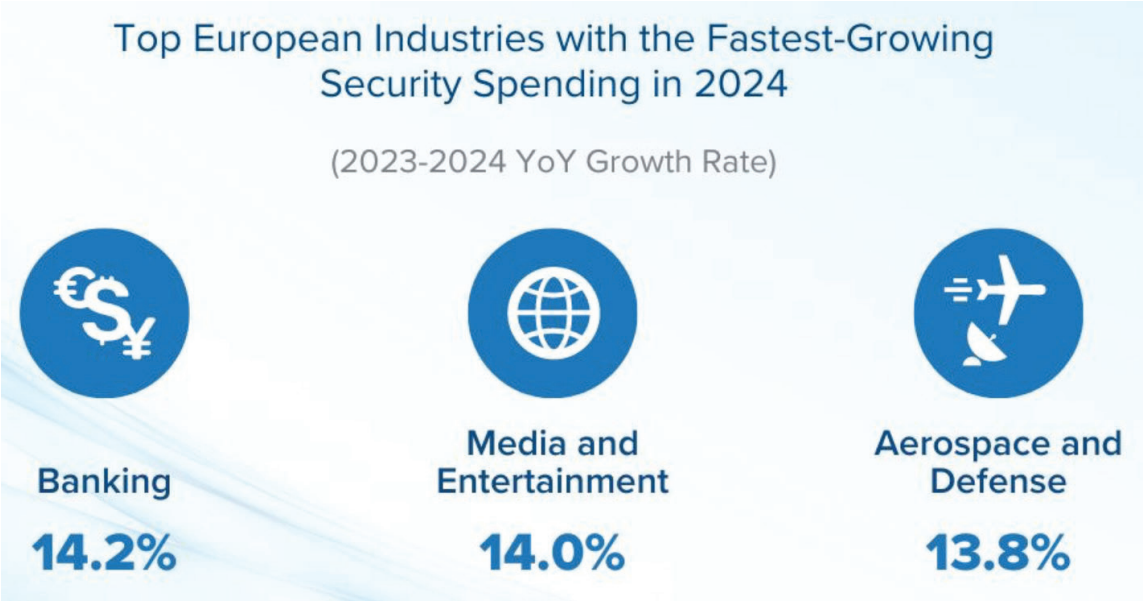


Figure 2

potential of AI and generative AI requires time. Although it is clear what benefits AI and GenAI solutions potential bring to companies' internal organization and processes, effectively realizing these benefits requires long-term planning. This requires companies to have a flexible and adaptable business plan to integrate AI and GenAI in a broader forward-looking and responsible strategy.".

Banking, retail, and software and information services are the top 3 industries in terms of spending, representing nearly a third of the European AI market. In the financial sector, notable uses of AI solutions span the cybersecurity risk areas, including augmented fraud analysis and investigation and threat intelligence and prevention systems, while customer support use cases include program advisors and recommendation systems. Moreover, financial institutions are increasingly integrating GenAI into their banking services; for example, for fraud detection or to generate accurate predictions and scenarios.

Evolving customer expectations and needs, fierce competition, and the quest for enhanced online customer experience are all factors driving retailers to experiment with emerging technologies. The retail industry in particular is taking advantage of the opportunities created by AI. With uses such as augmented customer service agents or expert shopping advisors and product recommendations, customer experience and satisfaction are always at the center of retail objectives, where AI can become a transformative force. Moreover, GenAI is gaining traction as many retailers expect to explore large language models (LLMs) and foundation models (FMs) applications in marketing, sales and customer engagement.

Finally, the software and information services industry, which represents software vendors and information and data services companies, is characterized by spending on AI by providing AI infrastructure. These companies grant users access to this infrastructure, providing resources needed for computing and for storage for AI systems development or the provision of AI services to end customers. AI spending in this industry will be driven by hardware components, which represents the largest tech component of the overall AI market. Nevertheless, software's market share will increase in the long term, growing fastest than any other technology component, as software providers will allow end users also to leverage their platform as a service (PaaS) and software as a service (SaaS) solutions. In addition, technology leaders can use GenAI to accelerate software development.

Double digit growth for European security spending

According to the Worldwide Security Spending Guide published by International Data Corporation (IDC), European security spending will grow by 12.3% in 2024, marking another year of strong momentum with double-digit growth. Spending in the region is expected to increase at a steady pace throughout the whole 2022-2027 forecast period, reaching $84 billion in 2027. Security thus proves to be a key IT investment area for European organizations, which will have to continue facing the constant threat of cyberattacks, securing hybrid work environments, and ensuring compliance with both national and international regulations (e.g., NIS2 and DORA).

The significant security spending growth trend will characterize the whole European region in 2024, with Central and Eastern European (CEE) countries having the highest growth rates (for example, 15.4% in the Czech Republic and 13.4% in Hungary) driven by the constant rise of the software market. In fact, security software and services are expected to be the key growth areas across all European countries, including the top spenders — U.K., Germany, and

France — which together account for more than 50% of the European market.

"European organizations face unprecedented cyberthreat levels, driven by a huge and voracious cybercrime economy, the proliferation of every attack tool and service imaginable on the dark web, and a turbulent geopolitical landscape," says Mark Child, associate research director, IDC European Security. "The European Union is striving to drive a regionwide improvement in cyber resilience through a host of legislative measures that will, notably, also bring much greater involvement of executive management in cybersecurity strategy.

Nevertheless, addressing the threat requires substantial and holistic engagement from all organizations. Cybersecurity investment strategies need to coalesce around improved cyber risk quantification, a balance of preventive and proactive measures, consideration of all user groups and business processes, and the availability of requisite skills and resources both in-house and sourced from third parties."

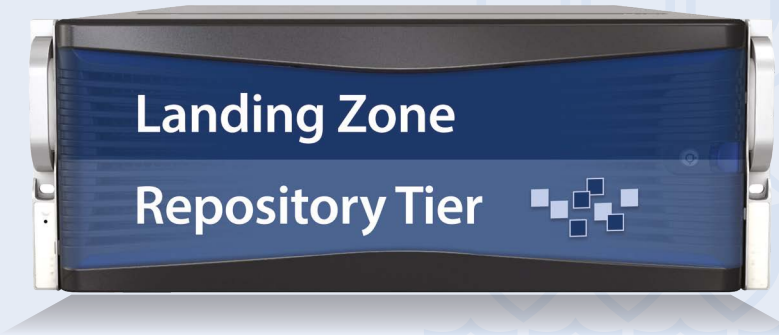
Banking, central government, local government, telecommunications, and retail will spend the most on security this year. These five industries combined will represent almost 38% of the total European security market. The fastest growing industries in 2024 will be banking (14.2% year-on-year growth), media and entertainment (14.0%), and aerospace and defense (13.8%).

"The increasingly sophisticated tools available to cybercriminals — now including generative AI — are transforming security from a technical requirement to a key strategic factor for companies across all industries to stay competitive on the market. This is even more true for verticals like banking, media, defense, telecommunications, and government, where cyberattacks can have dire consequences on both business operations and on the organization's reputation," says Stefano Perini, research manager, IDC European Data and Analytics. Small and medium-sized businesses, which are traditionally less prepared than larger companies in terms of cybersecurity, will also be particularly exposed to the rising tide of cyberattacks. In response to this, they will increasingly focus on managed services, as well as on training their employees to deal with the new security risks."

Banks will continue to face a growing number of cyberthreats like ransomware, extortionware, and exfiltration, and will increasingly invest to secure existing business processes and protect new digital transformation initiatives. Media and entertainment firms will have to secure themselves from a growing number of malicious attacks that can be more damaging than for other industries, owing to their high public visibility. Because of the ongoing geopolitical tensions in the region, the aerospace and defense industry will increasingly focus on securing both IT and OT assets and protecting them from data breaches.

EXAGRID®

The future is here.
Tiered Backup Storage



- Fastest backups
- Fastest restores
- Scalability for fixed-length backup window
- Comprehensive security with ransomware recovery
- Low cost up front and over time

WINNER
SDC AWARDS 2023

- **Storage Company** of the Year
- **Backup/Archive Innovation** of the Year

Thank you so much to all who voted, and congratulations to our fellow SDC Awards 2023 winners!

Visit our website to learn more about ExaGrid's award-winning Tiered Backup Storage.

LEARN MORE >

Why your enterprise needs AIOps more than ever

Today's enterprise IT estates are incredibly complex. Rapid adoption of hybrid cloud architectures and diverse technologies, infrastructure, and applications is essential to digital transformation, but this spread of tools and services simultaneously poses a significant challenge for organisations striving to manage their IT operations and deliver top-notch business services and customer experiences.

BY RICHARD CHART, CHIEF SCIENTIST AND CO-FOUNDER, SCIENCELOGIC

AS IT OPERATIONS (ITOps) teams grapple with an intricate web of interconnected services, there's mounting pressure to monitor, maintain, and optimise systems to meet service level agreements. But IT's capacity to discover digital assets, extract data, sift through alert storms, and gain intelligent insights has now surpassed human processing abilities.

And, with more digitisation, there's even more data to deal with. Tool sprawl has created silos of analysis hindering teams from gaining full observability over IT estates, and obstructing their view of operations, making it challenging to take swift action and resolve issues before the business is impacted.

In the unending pursuit of operational efficiency, artificial intelligence (AI) for operations (AIOps) no longer feels like an option – it's the way forward.

How AI enables modern IT operations

AIOps is not a new concept. But, until now, ITOps teams have struggled to extract meaningful, actionable insights from their AI implementations. Much of this difficulty stems from the complex and siloed nature of modern IT estates, compounded by the lack of human-friendly interfaces, but technology leaders also often find it hard to make AI work for their specific business needs or scale its deployment across the enterprise.

But innovative approaches have emerged that take AIOps to the next level.

To accelerate the adoption of AIOps, these novel methods combine AI insights with a user interface designed for simplicity and comprehension. Once fully developed, AI functions as a co-pilot, analysing vast amounts of data across various cloud platforms and distributed systems, highlighting critical findings

about system health in a consolidated and digestible manner.

In doing so, AI enables IT teams to view their digital environment as a cohesive system, eliminating blind spots in infrastructure visibility and automating troubleshooting and solutions in real-time. When performance issues arise, AI-based anomaly detection tools quickly determine the root cause. These are coupled with generative AI components capturing and leveraging organisational knowledge to recommend automated remediation actions. These actions are designed to be easily comprehensible by IT teams and can reduce the signal-to-noise ratio and expedite mean time to repair (MTTR).

Moreover, modern AIOps can discern performance patterns and anomalies autonomously, even rare events that have not occurred before, without requiring explicit user guidance, streamlining workflows and ensuring optimal service uptime.
How can enterprises realise modern AIOps?
Setting aside the advantages of AIOps, integrating AI and automation into IT operations management (ITOM) necessitates change in both tools and processes.This shift starts with ensuring teams understand why things are changing. Whether it's to reduce downtime, speed up analysis, consolidate monitoring tools, or simplify IT and business processes, everyone from ITOps to DevOps must be on the same page and work toward the same goals.

The primary obstacle for any enterprise is complexity. The legacy state of ITOps, characterised by disparate monitoring tools and dashboards, can lead to mistakes and inefficiencies. Implementing a unified framework for automated device discovery, data synchronisation, analysis, and event reporting can streamline matters and unite data and personnel so that coordinated action can be taken to achieve desired business outcomes.

In order to attain this reality, ITOps teams first need to understand their infrastructure, no matter how complex it is. This means mapping each element of their hybrid IT environment, identifying interdependencies, and understanding how each part of the estate connects to business service offerings. The reality of modern IT environments is that nothing is static. Applications move based on load patterns or scheduled activities, traffic paths change to avoid failure points, new components are integrated - all creating a rich tapestry of dynamic relationships.

ITOps team must rely on tools at-home in this dynamic, hybrid cloud world to ensure that the model of the entire tech stack is complete and current, achieving full observability over the entire IT environment. With data now collected and consolidated, AI can dig through it, analyse it, and deliver useful insights into how the system behaves and performs. It can also suggest actions to fix any problems. At the same time, ITOps teams can set up automated workflows to do specific tasks, like rebooting servers or applying patches, based on what the AI recommends.

Moving to a business-first architecture

In terms of business outcomes, modern AIOps is transformative. It enables IT pros – even Level 1 and 2 engineers – to predict issues before they occur, identify root causes, and address problems before they impact the user experience. With the aid of AI and automation, they are empowered to tackle tasks that previously required Level 3 expertise and interventions. Which in turn, frees valuable IT resources to focus on growth initiatives and furthering technology innovation.

Human-friendly AIOps also eliminates the need for a broad range of monitoring tools by aggregating IT information across clouds and devices, and deriving insights that every team can use to inform responses and resolve issues. Of course, full task automations don't need to happen at once. As enterprises advance along their AIOps journey, human oversight and control is vital to reducing risk and ensuring optimal outcomes.

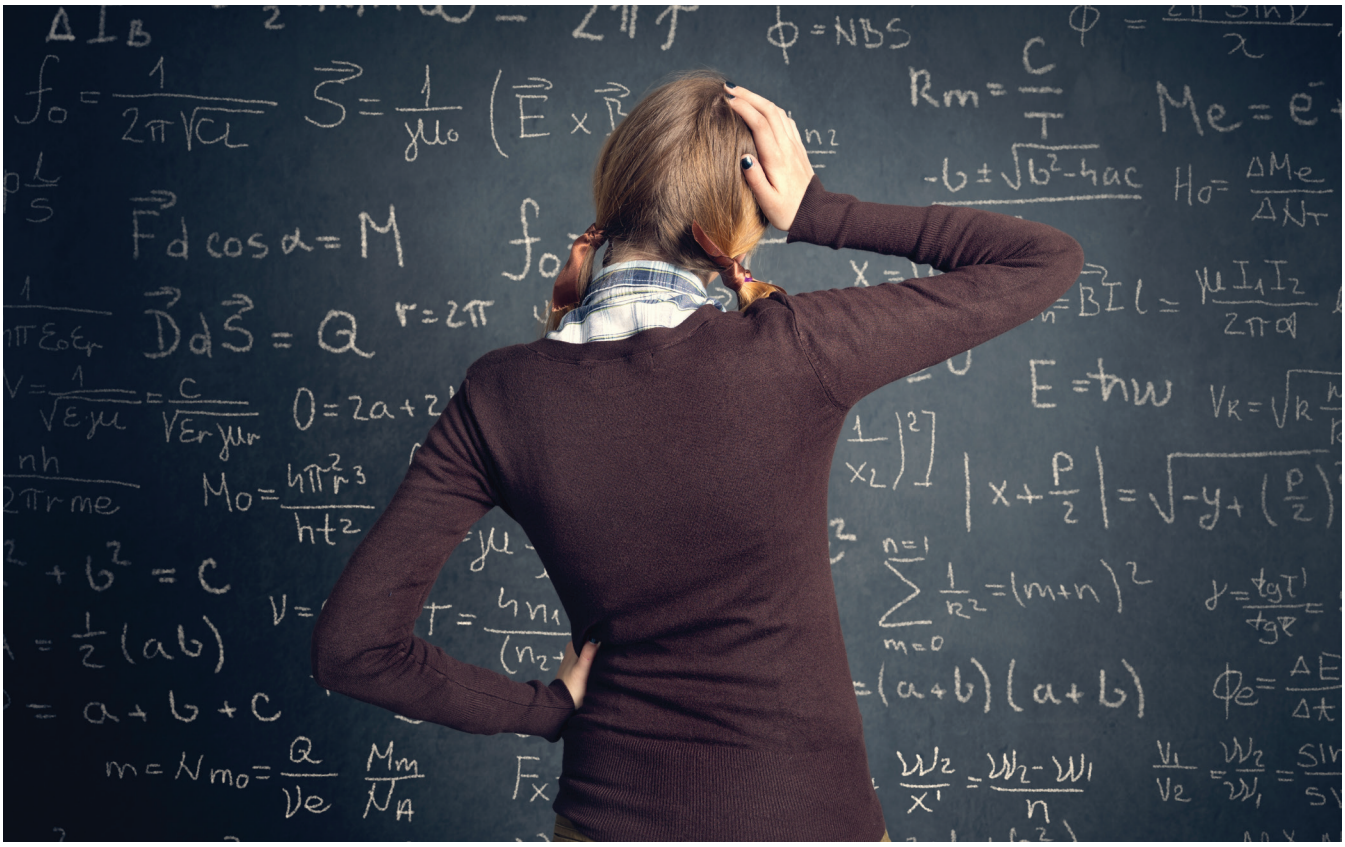
The primary obstacle for any enterprise is complexity. The legacy state of ITOps, characterised by disparate monitoring tools and dashboards, can lead to mistakes and inefficiencies

Some organisations may choose to automate only specific systems or processes. As human operators gain confidence in AI's ability to match their intentions, they can move towards a state where AI works alongside them, a trusted copilot directing their actions without the need for constant oversight. In fact, according to Gartner, 84% of organisations view AIOps as a pathway to a fully automated network.

This journey culminates with a state of "autonomic IT," a fully realised state of AIOps, where technology estates and IT capabilities don't simply run themselves, but are self-empowered. Autonomic IT operations combines data, AI, and automation across every area of observability, analytics, and remediation to monitor, optimise, and even heal technology investments while they run. And with tech running itself, IT teams can achieve and deliver even greater value to the business.

It's time to unlock IT and business potential with AIOps

Imagine seamless integration of tools, complete visibility into hybrid-cloud setups, and minimal disruptions that are resolved before affecting customers – this is the essence of what AIOps offers. And in today's complex modern enterprise, it's a necessity.



Mitigating the threat of quantum computing

If the science of quantum computing feels a lot like black magic to you, you are not alone. The technology – which seems to almost mystically just "know" the answer – allows us to solve problems previously thought impossible, like quickly factoring multiples of large primes. And it is capabilities like this that have IT security people very worried, since a large portion of modern cryptography is based on exactly the principle of leveraging hard-to-compute math problems.

BY DAVID CORLETTE, VP PRODUCT MANAGEMENT, VIPRE SECURITY GROUP

SO, HERE'S the nightmare scenario: we have built our security infrastructure on the use of hard math problems used to encrypt our private and sensitive data; someone builds a quantum computer that can quickly decrypt that data and can learn all our secrets. Panic in the streets! Will all secure websites have to stop operating? Will we have to start actually walking into physical banks again?

Well, no. Quantum computing isn't exactly news, and there are already several efforts underway to create cryptographic algorithms that are "quantum safe"—meaning they can't be cracked by quantum computing. In fact, we are pretty close to having some of them approved by National Institute of Standards and Technology (NIST) and the European Union Agency for Cybersecurity (ENISA), and efforts have already started to code them into the common cryptographic libraries. But this process will take some time, and of course even once that is done it can take a very long time, for all the real-world implementations to actually start using (much less requiring) these updated libraries. Heck, even a full year after the critical Log4j vulnerability was disclosed, many major packages still haven't updated the version they use.

Hence, a lot of the risk comes down to how long it will take for quantum technology to advance to the point where it can actually solve these hard math problems, a capability that will require lots of logical qubits – it often takes hundreds or thousands of physical qubits to produce a single reliable logical qubit).So far quantum computers are only up to double digits. And although some people think that a secret government lab somewhere might have something better hidden away, and there have been some claims of large numbers being factored

(usually depending on a lot of tricks), most people think we are at least a couple years away from general-purpose cracking of our current crypto algorithms.

So, are we totally safe then? Well... not quite. Although it is very likely that common systems like web servers and browsers will roll out quantum safe crypto in time, there will be a lot of systems that drag their feet. Transport Layer Security (TLS) 1.3 was published in 2018, and it took three full years for it to get rolled out to more than 50% of websites. On top of that, even if we can secure new connections, our old encrypted data might be lying around waiting for someone to decrypt it (like, say, in that enormous US government facility in Salt Lake City).

So, what can you do to mitigate the potential threats posed by quantum computing, and its anticipated ability to break current crypto? Here are some thoughts:

- Make sure you update to the latest versions of the software you run in your organisation, particularly anything that can accept a network connection or stores anything encrypted. This is good security practice anyway, but it is particularly important for anything that uses encryption.
- If your software vendors seem to be lagging in adding support for quantum safe crypto, ask them to get cracking.
- Just having up-to-date software isn't enough. Make sure you review the configuration of that software and disable the use of older or less secure protocols. This may require some testing of the clients that use your services, and may require updating those client systems as well, to support modern encryption. Continue this process as quantum safe crypto is rolled out.
- Where possible, increase the length of any keys used for encryption. A 2048-bit key will be a lot stronger than a 1024-bit key, and quantum computers will have to develop even further to factor those longer keys.
- If you don't need to store private or sensitive data, don't store it. If you do need to store it and it has already been stored with an older protocol or a shorter key, consider exporting, re-encrypting, and re-storing that data, then deleting the old data that has weaker encryption.

Naturally, everything listed above is already industry standard practice, but these items have particular significance in the face of quantum computing and will become much more relevant as we approach the decryption event horizon. How aggressively you pursue these will depend on your risk profile, but every organisation should at least be keeping their software up to date. There's no need for panic, but some due diligence would be a good idea.

Remaining robust and resilient against cyber threats

The past few months have been challenging for information security as organisations continued looking for ways to stay ahead of hackers. Overall, phishing attacks increased in frequency and complexity, in part likely driven by a major trend: artificial intelligence (AI) phishing attacks. Phishing remains the most prevalent attack method amongst bad actors, mainly due to its relatively low cost and high success rate. The significant implementation of AI in the coming years only furthers this problem.

BY NIALL MCCONACHIE, REGIONAL DIRECTOR (UK & IRELAND) AT YUBICO

ACROSS THE BOARD, businesses, governments and consumers have been targeted via phishing attacks, with cyber criminals often seeking credentials and identity information, to subvert legacy multi-factor authentication (MFA).

According to Yubico's recent survey, 91 percent of employees still rely solely on a username and password to secure their accounts, which could be a contributing factor as to why phishing attacks are so prevalent. To stay as secure as possible, there must be a shift away from passwords and other weak forms of authentication, and a move towards modern, phishing-resistant MFA, such as hardware security keys. As cybersecurity threats continue, it is essential for businesses and consumers to implement strategies alongside phishing-resistant MFA to prevent these attacks.

Prioritise implementing Zero Trust strategies

Although businesses spend a lot of time and energy attempting to prevent breaches, cybercrime is somewhat inevitable. When attacks take place, the next line of defence should be to minimise the impact of the breach. When implemented holistically, Zero Trust Architectures (ZTA) create additional trust boundaries that limit the attacker's ability to move laterally.

The adoption of ZTAs has also driven attackers towards post-authentication attacks, forcing them to try and subvert preventative measures such as device registration. It is common for enterprises to require specialised registered devices for administrative access to the environment. Registration of one of these devices should be a rare event – so much so that it is appropriate to

notify a broad set of operations personnel to the event to ensure it is authorised.

This type of approach provides defenders with an opportunity to detect attacks early. In fact, quite a few high-profile attacks in the last few years have been detected this way. Well-crafted alerts around rare and sensitive events that are then reviewed by personnel should be prioritised throughout 2024 and beyond.

Preparing for advanced AI-driven attacks

While there are known benefits of generative AI, bad actors can use this technology to their advantage. For example, generative AI can assist with phishing attacks by writing customised emails on a massive scale or placing scam phone calls to thousands of people at once. By automating the time, skill, and labour-intensive parts of running phishing campaigns, generative AI can increase the number of attacks and lower the bar for less savvy cyber criminals to conduct phishing attacks.

Phishing attacks usually focus on convincing the victim to provide personal information, but attacks can be mitigated by validating the request using an alternative communication path. Although some forms of communication, such as a phone or video call, are generally thought to be trustworthy, it is important to understand that cyber criminals can use AI to mimic voices. Additionally, if an individual receives an email from a family member asking for money to help them get out of a situation, the end receiver should call them using a recognised phone number to confirm the situation.

Increasing misinformation around global events and election campaigns

AI and deep fakes will have a major impact around the world, especially when it comes to spreading misinformation to influence global events and elections. 2024 is a major election year in many countries across the globe, including the UK. With this in mind, there will likely be a steady rise in attacks in an attempt to erode the public's confidence in election systems and to undermine democracy. The challenge will be mitigating the threat of deep fakes to limit their impact.

Common methods of consuming information and communication will need to adopt some of the ideas that have been incorporated into Zero Trust models. Video content sites may need a method for viewers to confirm the identity of individuals appearing in videos to combat concerns of deep fakes – and the same should be true for email content.

Individuals and organisations should always double check their sources and be sceptical of content that is too good to be true or feels off. To have any meaningful impact on disinformation, governments around the world need to continue prioritising cybersecurity and partnering on cybersecurity posture. As passkeys become ubiquitous and the adoption of electronic identities becomes more common, there will be basic building blocks required to increase the trust in content and communication systems, using well-understood and battle-hardened approaches.

dapting to the expected rise of post-authentication threats

The last few years have seen an increase in the adoption of MFA, meaning attackers have needed to adapt and broaden their tactics around these new defences. Additionally, there has been a return to social engineering attacks that entice victims into downloading and installing software, as well as a resurgence of fake, but convincing, web pop-ups that lead victims to believe their device is infected. This eventually turns into a common call centre-based technical support scam.

Although not new, there has been an increased focus on stealing browser tokens that allow an attacker to impersonate the victim. These tokens or identifiers are set after successful authentication and are used to uniquely identify the authenticated user as part of their web session. In some cases, these tokens are traded and sold and can sometimes support larger ransomware or extortion campaigns. The prevalence of token-based theft is leading to more research into token binding, a technical solution that ties the token to a specific device. This allows defenders to detect when the tokens are stolen and then used on a different device or in a different geographic location.

Looking ahead

In light of increasing cybersecurity threats in 2024, companies should prioritise advanced cybersecurity methods and educate the workforce on the need for better cybersecurity practices. By doing so, they are better positioned for success when mitigating emerging cyber threats.

Organisations must consider implementing phishing-resistant solutions such as strong MFA that offers security and convenience. For example, FIDO2 security keys are proven to be the most effective phishing-resistant option for business-wide cybersecurity. By removing the reliance on passwords, MFA can be used for both personal and professional data security.

Companies also need to be more proactive in changing attitudes surrounding cybersecurity, as employees at all levels can be the biggest strength or weakness in cybersecurity. Regular cyber training paired with robust passwordless security will equip employees to be effective cyber defenders. There are many opportunities to become more cyber secure and stay ahead of evolving information security threats. In 2024 and beyond, attackers will certainly continue evolving and adapting to keep up with changing cybersecurity postures, so it is vital that businesses and consumers around the world do the same.

How the insider has become the no.1 threat

The insider threat is now twice as likely as phishing to be the cause of a breach. That's according to a recent survey by Apricorn of over 200 IT security decision makers which found insider threats were the biggest threat with 40% citing these (22% unintentional and 20% intentional) as the main cause of a data breach within their organisation. For comparison, almost a quarter (24%) of breaches were found to result from ransomware attacks, a fifth phishing emails (21%) and lost/stolen devices (18%).

BY JON FIELDING, MANAGING DIRECTOR, EMEA AT APRICORN

THE RESULTS may seem surprising given that phishing attacks usually dominate the headlines until we look at the cause of this surge. Non-malicious insider threats can, to a large extent, be attributed to an increase in the remote workforce. The same survey revealed that 48% of mobile workers knowingly put corporate data at risk of a breach in 2023, revealing that hybrid or remote working is playing a role. But the increase in malicious attacks is also due, in part, to the economic pressures people are now under, allowing organised criminal gangs to brazenly recruit insiders.

Complicit recruits

It's a combination of events that the ISC2 has also picked up upon in its Cyber Workforce Study 2023 which found that 52% had experienced an increase in the insider threat over the past year, with 71% attributing this to economic uncertainty. Moreover, of those who had contact with a malicious insider,

39% said they or someone they knew had been approached to become one, revealing just how widespread the practice is and that insiders may well be recruiting other insiders.

In fact, the problem of malicious leakage has doubled compared to last year, with a fifth of organisations reporting they had suffered a breach attributable to malicious employee during 2023, according to the Apricorn survey. There is a certain resignation to this with almost half (48%) admitting that their company's mobile or remote workers have knowingly exposed data to a breach over the past year, a rise from 29% in 2022, while 46% stated that their remote workers "don't care" about security, up from 17% the previous year.

For the organisation, this means the insider threat has not only become more pronounced but harder to counter. It requires effective management on two fronts in terms of managing the remote/mobile workforce and dissuading employees from swapping cash for credentials/data. For these reasons, businesses need to reinforce the security culture through staff awareness training and step up their policy enforcement, in addition to applying technical controls to ensure data is protected at all times.

That's not what is happening today. The Apricorn survey found only 14% of businesses control access to systems and data when allowing employees to use their own equipment remotely, a huge drop from 41% in 2022. Nearly a quarter require employees to seek approval to use their own devices, but they do not then apply any controls once that approval has been granted. Even more concerning is that the number of organisations that don't require approval or apply any controls has doubled over the past year (17% compared to 8% in 2022). This indicates a hands-off approach that assumes a level of implicit trust, directly contributing to the problem of the insider threat.

Bringing insiders back

So, what needs to happen for organisations to exercise control and to help mitigate the risk? Firstly, we need to see a more proactive approach, starting with staff awareness programs that must be relevant and meaningful. The processes they advocate should not impede workflow because overly prescriptive controls can create obstacles that frustrate users and encourage them to seek workarounds. A balance needs to be reached to make the controls workable.

Secondly, while employee devices are here to stay, it's imperative that the organisation exercise some control over their use. There are now numerous ways to remotely manage the end user device and endpoint connectivity. Zero Trust initiatives, for example, are rapidly making the VPN obsolete in providing a secure means of access. The principle behind zero trust is never trust and always verify so that every access request is treated as potentially malicious until it is authenticated. It's an approach which is much more suitable for distributed networks than the trust traditionally assumed within the perimeterised network. Zero Trust also exercises the concept of least privilege, where the individual user is only given access to the data required to do their job, thereby limiting the potential for a malicious user to infiltrate the network.

For the organisation, this means the insider threat has not only become more pronounced but harder to counter. It requires effective management on two fronts in terms of managing the remote/mobile workforce and dissuading employees from swapping cash for credentials/data

Encryption should also be more widely used to protect data at rest, in transit and in use, helping to prevent the interception or loss of data. However, the number of businesses encrypting physical devices has declined markedly over the past two years. Only 12% encrypt data on laptops today compared with 68% in 2022 and only 17% desktop computers, down from 65%. Similarly, only 13% encrypt mobile devices versus 55% in 2022, 17% USB sticks, down from 54%, and 4% portable hard drives, down from 57%. It's a rapid decline that suggests the focus has shifted to other data protection methods, leaving these devices unnecessarily exposed.

Prioritise recovery

Finally, in the event that data is compromised or stolen, the business will need to ensure it can rapidly recover, which makes an effective backup strategy a must. Ideally there should be provision for physical local backups to be made as well as sending data to a centralised cloud-based repository. The 3-2-1 rule is well known in providing a belt and braces approach in this regard. It advocates that at least three copies of data should be held on at least two different media with at least one held offsite, preferably offline and encrypted. Taking these steps can help ensure end users and their devices are effectively managed, reducing the opportunity for employees to compromise data whether that be intentionally or unintentionally.

Going forward, the likelihood is that both instances will increase. Cutbacks are seeing staff workloads grow, increasing the potential for error. The cost of living crisis is beginning to bite deeper, making those same staff more susceptible to criminal recruitment. And, at the same time, organisations have taken their eye of the ball, failing to maintain best practice procedures such as the use of backup and encryption to protect data. It's therefore vital that we get 'back to basics' to stem the flow of data being liberated by insiders.

Exploring the relationship between identity and data security

Identity-based security has gone beyond being a fad and is now a necessity to ensure business cyber security.

BY STUART HODKINSON, VP EMEA AT PLAINID

IN 2006, British Mathematician, Clive Humby, boldly claimed that "data is the new oil", referring to how important information is to businesses of all sizes. Now, in 2023, Humby's prediction has primarily been made true, with companies spending incredible amounts of money to collect, store, and analyse this data. Data is now essential to do business, with it being used to fuel business decisions, from better understanding the consumer, to enacting digital transformation at a larger scale.

Whilst there are undoubtedly benefits to this explosion of information, this data can cause major problems if it falls into the wrong hands. Sensitive company information can be leaked to competitors, or personal information about customers and staff can be breached, resulting in failed compliance obligations. These threats, and more, become increasingly likely if not protected by a robust data management strategy.

However, many companies are stuck in the past. Most will rely on static solutions that are difficult to maintain, and unable to meet the demands of fast-paced businesses. Whilst perimeter-based solutions do provide some protection, they are not able to keep up, often requiring coding to make changes. This means that only those with IT backgrounds can make amendments, providing limited visibility of an organisation's security landscape to the everyday user, and in turn, becomes much harder for these users to understand their risk responsibilities.

Today, the biggest challenge is how to respond to a bad actor accessing your network and having unrestricted visibility of company data. The simplest remedy is to limit this movement until security teams can secure the network. However, the old adage of "prevention works better than a cure", rings true. Cyber security is a defence-based mission, and arming IT teams with smart security solutions can be the key difference between a full-blown security incident, and a security alert.

Yet, a one-size-fits-all solution will not cut it. An up-to-date security solution will be "identity aware" and adhere to the principles of "dynamic authorisation" (in this context, 'authorisation' refers to the management, control and enforcement of the connections of identities to data, functions, and apps they can access. By adopting these approaches, this becomes the first step to having truly 'smart' security.

Identity as a prerequisite to smart security

A key cornerstone to smart security is a zero trust approach to authorisation. At the heart of a zero trust architecture is the ability to decide whether to grant, deny, or revoke access to a resource, based on the conditions an access request is made in. For example, if an already authorised user based in a UK office is trying to access Asia-specific files at midnight local time, this suspicious activity could

be flagged to security teams, or the request denied automatically.

This approach then acknowledges that sometimes, authorised users can have their credentials exposed, and bad actors can exploit their preauthorised access to exploit sensitive data. Therefore, by requiring even preauthorised users to routinely reauthorise their identities, data becomes even more secure.

Equally, the zero trust ideology works well within in the modern work environment where more companies are using data hubs, like cloud storage, to allow their employees to work more freely from anywhere. With data moving more fluidly among users in and out of an organisation, it's increasingly difficult to rely solely on traditional perimeter security methods. This rise in complexity is why smart, identity-first security will be a business necessity going forward.

Therefore, one of the most significant benefits of zero trust is its ability to automate permissions policies that virtually eliminate human error and lower risk exposure. It also gives security teams dynamic decision-making capabilities that allow them to rely on risk signals to make real-time decisions on what users can access.

The link between authorisations and data

When adopting a zero trust approach, it's important to keep in mind the link between the identity world and the security of your data. There is a growing trend to provide advanced data access controls that are identity-aware, dynamic, fine-grained and governed by policies. Data owners should think of identity-first security as part of their data access control strategy and to research their options. This is crucial for securing the organisation's most important asset: its data.

Authorisation vs Authentication

Yet, identity-first security cannot end there. Continuous authentication must happen at every stage down to the final file that the user accesses. This can be likened to security at an airport. When you first arrive at the terminal, there are no barriers to get into the terminal - everyone is welcome. However, to proceed into security, the passenger must present a boarding pass. Then, through security, they need that boarding pass again, as well as their ID, to get to the gate. Finally, a valid ID is needed to board the plane, a

nd everyone must sit in an assigned seat. Throughout this whole process, every additional step requires strong control and reconfirmation of identity. Even then, there is still only certain areas of the airport which an individual can access unrestricted - having access to the terminal doesn't mean they can board any plane, and accessing a plane doesn't mean they can sit anywhere they'd like.

This same idea should also be implemented in the digital world, combining authentication and authorisation, and enforcing granular controls as a user gets near data.

Utilising Authorisation

To summarise, authorisation is the ability to, and actively manage, the identity's connection to sensitive data as a part of identity-first, zero trust security. This approach will only work when implemented through an advanced authorisation solution that can address all paths to data applications, APIs, microservices and the data hub itself.

If this is not properly addressed, data breaches will continue to get more aggressive, and increasingly expensive to resolve, especially as businesses continue to consolidate their data into large data hubs. Therefore, an easy solve would be to invest in solutions that require identity access controls throughout the entire technology stack. This will then reduce the impact of breaches by restricting movement within the network until its presence is authenticated, and if needed, removed.

Identity-based security has gone beyond being a fad and is now a necessity to ensure business cyber security. There is continued investment in the identity space as the importance of reconfirming identities has become common knowledge to IT and Business leaders alike. Ensure your security is not left behind.

When adopting a zero trust approach, it's important to keep in mind the link between the identity world and the security of your data. There is a growing trend to provide advanced data access controls that are identity-aware, dynamic, fine-grained and governed by policies

The end is near for the password

The origins of the computer password aren't entirely clear, with many believing it emerged from the Massachusetts Institute of Technology in the early 1960s. Since its inception, whenever that may be, as an authentication tool, the password hasn't really changed. While it proved effective in an internet-less world, today it's seen as a legacy authentication process that needs to be tossed aside for passwordless alternatives.

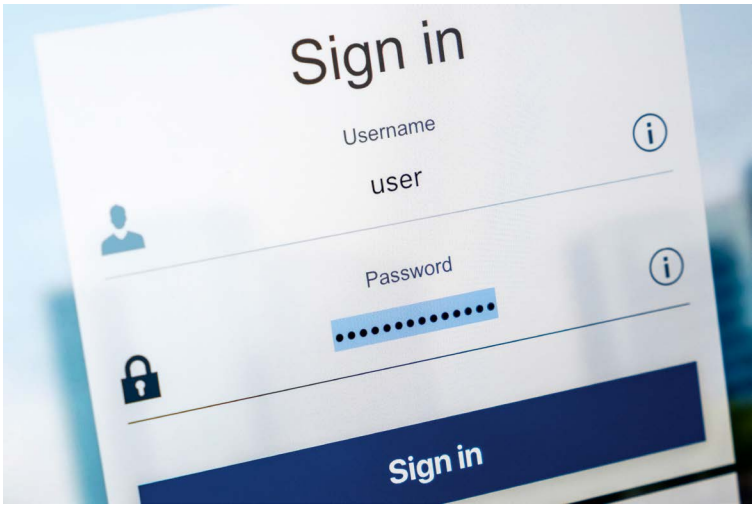
BY ALEX LAURIE, SVP EMEA, PING IDENTITY

THE PASSWORD is an outdated tool which proves ineffective against today's threat landscape, luckily, big tech companies, such as Amazon and Google, have woken up to this and are looking to better secure their futures. Our latest research indicates the move couldn't have come at a better time, finding that consumers are becoming increasingly impatient when encountering poor digital experiences, especially when accessing their accounts. It leads to the notion that the end of passwords may well and truly be here.

Big tech domino effect

Earlier this year, in quick succession, Google and Amazon announced they would begin offering passwordless authentication methods in the form of passkeys. Considering that access management companies offer these solutions, and have done so for several years, why are Google and Amazon's announcements so important?

As two of the globe's most dominant technology enterprises with billions of users between them, these organisations can spark the necessary global change to passwordless. Instead of the billions of Amazon and Google users gaining access to the company's platform through passwords, they are now asked to consider shifting to passkey alternatives when signing in.



We're at the start of the long awaited passwordless era – as more organisations follow suit and continue to set up passkeys, users will begin feeling the impact of a more efficient login process and will exist in a more secure environment.

What makes passwordless alternatives that much better?

Passwords are a constant threat, leaving organisations open to an array of attack vectors – with phishing the most common. If you think back to some of the most infamous recent attacks, such as the Colonial Pipeline Hack, threat actors often gain access to a system using compromised passwords. With 24 billion pairs of stolen credentials up for sale on the dark web, it's easy to see why account takeover is an easy angle for cybercriminals to attack. On top of this, passwords are an inconvenience.

Think back to the number of times you've ended up locked out of a certain platform and had to embark on the painstaking process of resetting your password, and how many people keep track of their passwords on their phone, or in a notebook next to their computer?

With consumers wanting greater convenience and enhanced security, passwordless authentication tools provide the only solution that appeases both appetites sufficiently. Offering significantly increased security due to the lack of a crackable code, more efficient access thanks to biometrics, and reduced

Passwords are a constant threat, leaving organisations open to an array of attack vectors – with phishing the most common

costs as there's no need to allocate budget for password management or storage solutions, passwordless is the logical path for the tech industry to travel. And, thankfully, with big tech acting as the first domino, more will begin to adopt passwordless authentication methods.

While the transition will take time from both a B2B and B2C perspective, our research indicates that consumers will welcome passwordless authentication. 59% of the UK said if passwordless authentication was offered, they'd be happy to switch website/app/service.

Adding to the UK's digital ID debate

As the UK begins its passwordless migration, it will also add urgency to one of the country's most significant debates – the adoption of digital identities. While under the nose of politicians for many years now, the barrier to digital ID adoption has traditionally revolved around a lack of consumer trust. However, our research has found that 55% of UK citizens support a single-use government-issued ID. Yet despite these findings, the UK trails the rest of the world in terms of adoption. Like passwordless authentication, the UK public needs to be shown digital IDs are a tool to improve security and efficiency, and that they won't, in any way, impinge on their rights. Preventing the resale of their data is now a top priority for consumers when considering app features, with 70% of our global survey agreeing with this sentiment.

Thus, ensuring and articulating the fact that consumer data will remain secure will ease barriers to digital ID adoption.

Passwordless: the ultimate consumer experience

As we move into a future where tools like digital identities and passwordless authentication build a frictionless consumer existence, both the public and private sector will play important roles in empowering everyone to make the transition with ease. Thanks to Google and Amazon's actions, and the impressive tools the Access Management industry has built, 2024 will be a crucial year in the pursuit of ultra-secure and efficient digital experiences.

Don’t be the weakest link in surging phishing attacks

Cyberattacks hit the UK hard over the past year. Reported cases of fraud more than doubled to £2.3 billion in 2023 – a figure fuelled by online scams, phishing attacks, and system breaches – according to BDO UK.

BY SAIRAM T A, ENTERPRISE ANALYST, MANAGE ENGINE

PHISHING remains the most common initial attack vector, which shouldn’t be surprising; after all, phishing attacks are one of the least expensive attacks to launch, yet they generate huge payouts. And opportunities for phishing fraud have greatly increased due to wider access to AI technology, which makes cyber risks harder to control.

Barclays Bank warned in 2023 that 70% of scams now happen on social media, online marketplaces, and dating apps. And Martin Lewis, Currys, and BBC have all recently been impersonated in online phishing scams. Law enforcement has indicated that there’s been an increase in smishing (SMS phishing), impacting shipping companies and many other industries. Missed delivery texts are a common scam tactic; phishers often pretend to be from UPS, Evri, and the Post Office. And HMRC has warned about bogus tax refund offers being sent over text and email, reporting 207,800 referrals of suspicious contact over the past year, particularly in response to the Self Assessment tax deadline in January.

Why phishing thrives today

Phishing is the most common initial attack vector today because it helps bad actors access a network and search for sensitive data in order to conduct an attack at a later stage. It’s popular, at least in part, because it’s cheap to conduct. An entire phishing campaign, including a phishing kit and hosting, can cost as low as £40. Also, phishing is easily scalable because every employee is a potential target. In an organisation with thousands of employees, one oversight by an individual can bring the entire organisation down. Remember, an organisation’s security is only as strong as its weakest link.

Novel phishing attack types have emerged
Phishing attacks using novel tactics are rising, such as malicious QR codes embedded in phishing emails. What’s more, generative AI threatens to make phishing attacks more dangerous. For example, the infamous CL0P Ransomware Gang is known to have used Truebot. Such threat actors are leveraging phishing campaigns with malicious redirect hyperlinks to deliver new Truebot malware

variants. Recently, we've also seen the rise of QBot Trojan attacks—with new variants discovered in January. This type of attack comes in the form of an email with context-aware information. These emails will contain an attachment or a link from a supposedly trusted source, prompting you to download or open a file, or enter your credentials.

A single click triggers a malware download, and subsequently, your system or network will be hacked. If the file contains obfuscated data acting as window dressing, it can go unnoticed by your organisation's security team. This attack is also conducted on reply-chain emails, which often lends to the credibility of the email.

Unfortunately, the novel forms of attacks keep coming. Domain impersonation and business email compromise attacks have seen a spike. A small tweak to a familiar-looking domain of your organisation—along with the display name of a current employee—can trick you into thinking that a malicious request is legitimate.

Phishers also keep improvising. The unsubscribe malware scam is a new phishing tactic that you should be wary of. After you click the unsubscribe button of a fraudulent email, the bad actor learns that the email address is active, making you a target of further phishing emails. The unsubscribe link might also lead to a website that downloads malware onto your system. It's worth noting that the best way to deal with unsolicited emails is to mark them as spam, delete them, or block the sender—don't directly interact with the email's contents.

How to prepare for tomorrow

While there are numerous ways to safeguard your digital enterprise, here are my top-four tips.

1. Train employees to recognise phishing attempts. Have a red team in your organisation to identify vulnerabilities, play the role of an attacker, and periodically simulate attacks. Awareness training can inculcate good habits, such as taking a step back and inspecting anything unusual received over email, SMS, or a phone call. If you receive an email from a legitimate source asking you to do something urgently, it is always best to reach out to the sender separately to confirm the message.

2. Deploy phishing-resistant MFA. Unauthorised access can be prevented by using phishing-resistant MFA. These apps require an additional layer of authentication, such as a passkey that can only be accessed with your face ID or fingerprint.

3. Use UEBA and SOAR for proactive detection and response. A SIEM tool equipped with user and entity behaviour analytics (UEBA) profiling will help you spot anomalies. The user behaviour variables are customisable; they can be based on time, event patterns, and the number of events triggered. ML-driven security orchestration, automation, and response (SOAR) capabilities will automatically execute workflow profiles and assign tickets to security admins to quickly remediate a phishing attack.

Phishers also keep improvising. The unsubscribe malware scam is a new phishing tactic that you should be wary of. After you click the unsubscribe button of a fraudulent email, the bad actor learns that the email address is active, making you a target of further phishing emails

4. Monitor privileged users. Privileged users are the most vulnerable to spear phishing because of their access to sensitive information. Ensure you follow the principle of least privilege, train privileged users to exercise caution, and have visibility into privileged user account activities.

Today, phishing thrives on social engineering, so it's vital to stay vigilant, especially if you have privileged access to your network. Trust your gut instinct if you do find anything out of the ordinary, then take a step back and analyse the situation. Don't be the weakest link in this rapidly changing realm of cyberthreats. It is high time that organisations become more cyber-aware and take cybercriminals head on.

AI – coming to the rescue

AI tools like Microsoft Copilot for Security can take the strain off cybersecurity professionals and bridge the skills gap

BY JOSHUA PAULUS, HEAD OF SECURITY AND IDENTITY AT INTELLIWORX

AS ARTIFICIAL INTELLIGENCE (AI) continues to gain notoriety, new tools are emerging that could have profound impact on a wide range of sectors and professions.

One such profession is cybersecurity - a vital function for all businesses in today's landscape, and yet one which is facing significant challenges in attracting and retaining the right talent.

In a study of more than 1,000 cybersecurity professionals across the US and Europe, it was found two thirds (66%) had "significant stress at work" - with nearly as many saying that stress impacted their work performance.

But with Generative AI, there's an opportunity to both optimise the human element of cybersecurity while improving the quality of life (and work) for those on the frontline. In this coming year, Gen AI will begin to take on tedious, administrative tasks on behalf of security teams. In addition, it will enable junior cybersecurity professionals to take on more challenging, higher-level tasks - taking the pressure off of those at the top.

By embedding this type of Gen AI into existing workflows, it will not only free up security analysts' time in their current roles, but enable them to take on more challenging work - alleviating some of the pressure that has been created by current security workforce and skills challenges.

Take for example Microsoft Copilot for Security, which dramatically reduces the manual burden on security professionals, allowing them to respond to cyberthreats quickly, process signals at machine speed and assess their organisations' risk exposure in minutes.

Alleviating the admin strain on cybersecurity pros

One of the big advantages of Gen AI tools like Microsoft Copilot for Security is that they can be used to do cumbersome, manual tasks that take time away from cybersecurity professionals doing what they do best - stopping the bad guys from getting in.

Tools like Microsoft Copilot for Security can be used for example to translate technical content into a more readable, user-friendly format. Such tools can enable security teams to analyse data from a vast range of different sources or modules, enabling them to conduct traditionally time-intensive, tedious data analysis with speed and precision.

Gen AI can also be used to create summaries of incidents and threat assessments in simplified language that is more understandable and actionable for novice users, thereby significantly alleviating the admin strain on security professionals.

Reducing human error and stress

Gen AI tools will also be able to reduce human error in spotting threats and the stress that comes with it for security professionals.

For example, AI is able to detect phishing emails that humans might miss, noticing even the smallest grammatical errors that a human may reasonably find difficult to spot. This helps the good guys sift through data, detect phishing attempts, and provide real-time security suggestions.

Threat detection and response also becomes more efficient for security professionals with tools like Microsoft Copilot for Security, surfacing the key information they need to make decisions quickly.

Perhaps one of the greatest benefits of Gen AI is the shift from reactive to proactive cybersecurity. By alerting teams to potential threats based on learned patterns, Gen AI allows for pre-emptive actions before a breach occurs, preventing the stress that occurs when threat actors get in.

Mind the skills gap

AI also has the potential to help shrink the UK's cybersecurity skills gap. This skills gap has plagued both the global and UK cybersecurity industry for years - with no obvious way to bridge it.

For organisations AI tools can automate some processes and help eliminate the need for some roles where they may be struggling to recruit the right talent, or empower junior members of staff to complete more complicated tasks.

Attack disruption – socking it to the SOC?

Why businesses must move from outdated SOCs to attack disruption in combatting modern threat actors.

BY DOMINIC CARROLL, E2E-ASSURE'S DIRECTOR OF PORTFOLIO

IN THE EVER-EVOLVING landscape of cyber security, security operations centres (SOCs) are integral for proactively detecting and responding to threat actors. Using a combination of people, technology, and processes to monitor, detect and prevent cyber attacks, we've found SOC-as-a-service to be one of the most popular cyber security operations to outsource, and used by almost a third of CISOs and cyber security decision makers (29%).

However, we've also uncovered that a third (36%) of UK businesses feel their provider is underperforming. It's a recurring theme I have encountered more frequently when in conversation with my fellow cyber professionals. Many SOC-as-a-service and Managed Security Service Providers appear to be relying on re-selling pre-configured product offerings that will inevitably lack sufficient tuning and therefore pull a frustratingly high percentage of false positives.

Indeed, we found that providers not fulfilling their tuning obligations and escalating too many false positives was a frustration felt by almost a third (29%) of the 500 CISOs and cyber security decision makers surveyed.

What is most concerning is when we delve deeper into the impact of services operating in this way, it becomes evident that these monitoring methods are no longer sufficient to accurately protect UK businesses. Modern threat actors are moving much quicker from initial access to data encryption, resulting in an increased need for improved detection and response techniques.

Most SOCs have a simplified IT infrastructure setup which depicts a user's endpoint device, providing access to data that is valuable to a threat actor. The user endpoint device has a detection and response agent installed, but crucially, this is only deployed in what we call audit mode.

Events and alerts may be generated and sent to a central Security Incident and Event Management (SIEM) platform for logging. But if the alert is not tuned to the correct priority or is using an outdated ruleset, this won't be enough to raise a critical incident in many cases.

The constant influx of false positives wastes precious analyst time, which could be spent proactively mitigating risk through proactive threat hunting activities and quickly investigating true malicious alerts

As a result, escalations of malicious activity may be too slow and lead to an even slower approval time from the appropriate authoritative individual to take containment action.

False alerts cause burnout

The traditional SOC models reliance on 'out of the box' set ups, that are not efficiently tuned to the environment they're monitoring, can lead to overwhelmed and burnt out analyst teams.

The constant influx of false positives wastes precious analyst time, which could be spent proactively mitigating risk through proactive threat hunting activities and quickly investigating true malicious alerts.

With over 70% of CISOs telling us that they would pass responsibility over to an outsourced provider to gain quicker decisions, the question is how can this be best achieved if current technology methods are failing?

Solving the problem with attack disruption

The most important implementation any cyber security team should be deploying right now is what we refer to at e2e-assure as Attack Disruption. This involves applying automation into the security operation to isolate first and investigate immediately. By this I mean, where appropriate, rulesets and automation are implemented to detect anomalous account activity, rogue processes, or malware.

Rather than wait for an analyst to manually act further down the chain, the account is temporarily disabled, or the endpoint is temporarily isolated from the network.

SOC analysts are then immediately alerted to a high priority incident which is triaged as being a true or false positive. If it does happen to be a false positive, the account is re-enabled, or the device is released from isolation. If it's a true positive, the next steps in the response process are then activated.

We have recently seen Microsoft reveal their own automatic attack disruption implemented within Microsoft Defender for Endpoint, with their focus on 'human operated attacks'.

The implementation of an Attack Disruption technique makes your environment increasingly more difficult to bypass as threat actors must invest in a whole new operating model to have any hope of going undetected. This consequently makes you a much less desirable target.

Why the OWASP API Security Top 10 needed to change

Application Programming Interfaces (APIs) are integral to our digital ecosystem, acting as the glue that connects applications and services on our mobile phones, cars, and internet-enabled devices. They act as the gateway to these processes and systems, and it's this access that makes them so attractive to cybercriminals. But how APIs function also makes them fairly unique when it comes to security.

BY ANDY MILLS, VP EMEA, CEQUENCE SECURITY

UNLIKE APPLICATIONS a human typically accesses, APIs are made for machine-to-machine communication and respond to API calls to exchange data. It's this call pattern that attackers look to exploit, and unless the API is monitored using behaviour analytics the chances are the attack will go undetected. This is because most solutions, such as Web Application Firewalls (WAFs), look for signature-based attacks or monitor for spikes in network traffic typically associated with automated attacks rather than focusing on the API per se.

API security is among the most unique types of security, leading to the creation of the OWASP API Security Project and the subsequent release of the OWASP API Security Top 10 in 2019. It's since become the go-to resource for those tasked with developing and maintaining API, from developers to security teams, as it outlines the most prevalent tactics, techniques, and procedures (TTPs) used by attackers. Earlier this year, the list was revised and updated because, as the Group acknowledges, a lot has changed in API security, with the sector having matured considerably over the past five years.

Attack patterns

Attackers have become much more adept at targeting APIs and are quick to pivot from one technique to another or combine attack types. We first noticed this last year when Trinity attacks emerged, which saw Broken User Authentication combined with Excessive Data Exposure and Improper Assets Management. Although a relatively small number (100 million) of attacks were registered to adopt this technique, it indicated a new level of sophistication.

This evolution in attacks, as well as some API protocols gaining more traction than others and changes in defence, has driven the need for the Top 10 to be updated. Utilising public data and the results from bug bounty programs, as well as input from API specialists including vendors such as us, the new version contains several significant changes.

A seemingly new category, for example, Broken Object Property Level Authorisation (API1) (BOLA), combines two of the previous categories: Excessive Data Exposure and Mass Assignment. This change emphasises the importance of proper authorisation so that APIs are designed so that only authorised users can access or modify specific properties.

Another new addition is The Unrestricted Resource Consumption (API4). This highlights the importance of managing the resources required to satisfy API

requests, an issue that is particularly relevant in cloud computing, where resources are billed per usage. Unrestricted resource consumption can lead to increased operational costs, with attackers effectively bankrupting victims, and can even result in Denial of Service (DoS) if not properly managed.

Abusing APIs

Business Logic Abuse has long been a prime attack method that sees the functionality of the API turned and used against it either excessively or in an automated manner. The Unrestricted Access to Sensitive Business Flows (API6) category directly addresses this issue and encourages the implementation of appropriate rate limiting and abuse prevention mechanisms to stop attack automation from being utilised against it.

Previously, API6 was classed as Mass Assignment, but both are talking about taking advantage of objects and their properties within the application flow. Examples given on the OWASP API Security Project page are for a ride-share app in both cases, which sees the exploitation of backend systems. But something subtle about the renaming makes the 2023 version seem like something that needs to be fixed rather than being nebulous and confusing. The name change effectively establishes a call to action and is a good call by the Project leaders.

Another change is Improper Inventory Management (API9), highlighting the importance of maintaining a proper inventory of hosts and deployed API versions. As microservices architectures and API-first approaches become more prevalent, keeping track of all deployed APIs becomes a significant challenge. In most cases, organisations significantly underestimate the number of APIs they have deployed, leading to shadow APIs slipping beneath the security radar. So, this category helpfully emphasises the need for keeping track of APIs, their governance and lifecycle management.

Finally, the new Unsafe Consumption of APIs (API10) category highlights the risks associated with trusting data received from third-party APIs. Developers often inherently rely on third-party APIs, as they do internal APIs, leading to weaker security controls and exposing the business to supply chain attacks. This category encourages developers to treat third-party API data with the same level of scrutiny as user input.

What's been omitted

However, it's also telling which categories have been replaced. The OWASP API Security Project authors state that Injection, which was previously API8, has now been removed not because it isn't a threat but because it is not unique to APIs. The new list aims to encapsulate security risks specific to APIs and build awareness around API security issues. Injection attacks or vulnerable and outdated components are still an issue, but such risks are

generic and don't behave differently in an API context.

Similarly, Excessive Data Exposure, API3, has been taken off the list. It's been replaced with Broken Object Property Level Authorisation (API3) because this is the natural next step resulting from sensitive data exposure. But again, it isn't a direct replacement because many items in the list involve sensitive data exposure; it's simply a move away from too generic a term.

If we look at a typical attack pattern, the progress can effectively be mapped to the Top 10. Many breaches start with an API that the victim organisation is unaware of, which would be API9 in the new list. The API is then found to return some user data which would be API1 and the attacker then goes on to attack automation, using a bot to try to exploit this as fast as possible which comes under API6 and completes the attack chain.–

The new Top 10 is not a radical departure from the original version, but it moves the conversation on. It makes the TTPs much more API-specific and suggests an urgency that may have been previously lacking. There's more emphasis on the importance of proper authorisation at both the object and function levels, managing resource consumption, protecting sensitive business flows, and maintaining a proper inventory. It also introduces the concept of unsafe consumption of third-party APIs, highlighting the risks of trusting data from external sources.

As dependency on APIs increases and sustained attacks escalate, the list will prove invaluable to all those involved in API development, management, and security. Does it create arbitrary distinctions between TTPs, and is a top 10 the best format to present this information in? That's debatable. But it certainly raises the profile of these attacks and makes API security more accessible to the mainstream, and that has to be a good thing.

If observability is the solution, why are so many enterprises reluctant to embrace change?

IT environments today are so complex that humans cannot manage them alone. Just ask anyone who's been on the sharp end of a digital services outage. Depending on the scale and longevity of the outage, such incidents can lead to a loss of revenue, customers, productivity, and reputations. And that's just for starters.

BY ROB JOHNSON, SOLARWINDS, VP SOLUTIONS ENGINEERING

ACCORDING TO SolarWinds 2023 IT Trends Report, the typical enterprise suffers, on average, nine outages every month – each lasting around twelve hours – costing organisations $13.7M (£11M) a year. Although the data for the report came from 300 IT and C-level managers from North American global enterprises, the figures will resonate with enterprises in the UK and Europe.

As the report clarifies, "Modern enterprises revolve around being reliable, effective, and frictionless – especially in providing end-to-end digital service."

To ensure that these systems continue functioning without interruption, the IT teams charged with keeping them up and running must embrace observability.

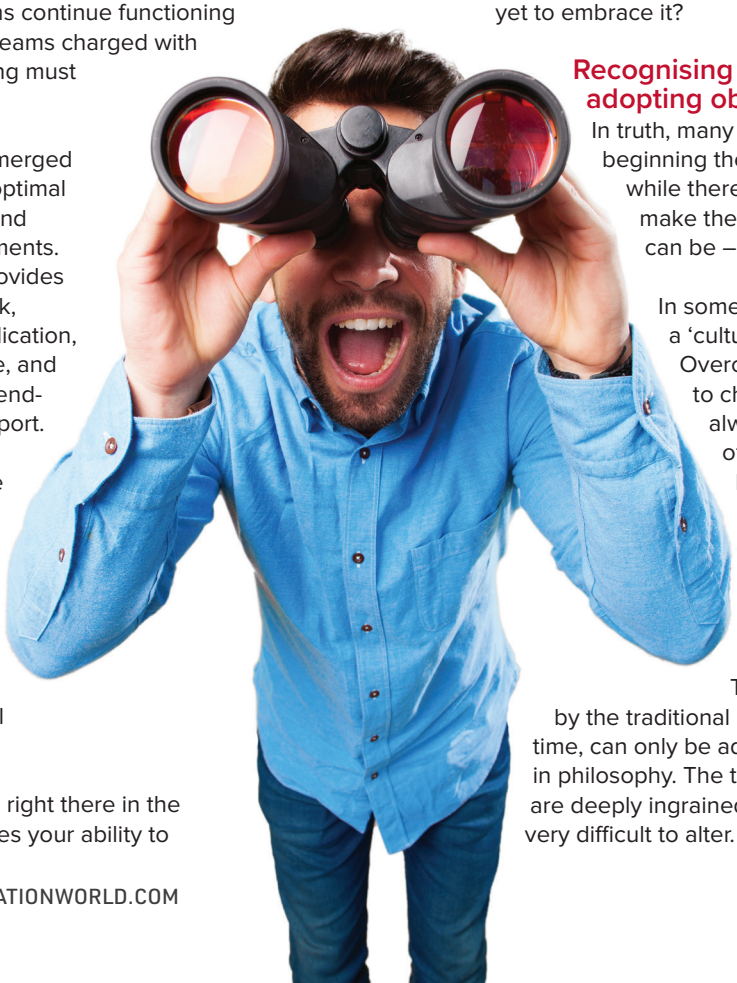
"Observability tools have emerged as a solution for achieving optimal performance, compliance, and resilience in digital environments. In essence, observability provides visibility across your network, infrastructure, systems, application, database, digital experience, and log monitoring — all in one end-to-end solution," said the report.

"The observability discipline also goes a step beyond monitoring, using cross-domain data correlation, machine learning, and AIOps to provide actionable business insights needed to identify and remediate issues in real time.

"In other words, the value is right there in the name: observability enhances your ability to observe your digital ecosystem with increased transparency, improved detection, and more intelligent insights," it said.

Indeed, the report found that almost all (96%) of those who had adopted observability tools had seen improved customer service. Seven in ten (71%) said they could innovate faster, while the same number said they could reduce the average time taken to solve issues.

With such a strong case favouring observability, it begs one question: why have so many enterprises yet to embrace it?



Recognising the barriers to adopting observability

In truth, many enterprises are still beginning their observability journey. And while there are plenty with the drive to make the necessary changes, there can be – at times – strong headwinds.

In some cases, IT professionals face a 'cultural resistance' to change. Overcoming the 'Why do we need to change? This is how we have always done it' mindset can often be compounded by a lack of support from leaders to advocate such a shift.

IT leaders with an outdated best-of-breed approach are also causing headaches.

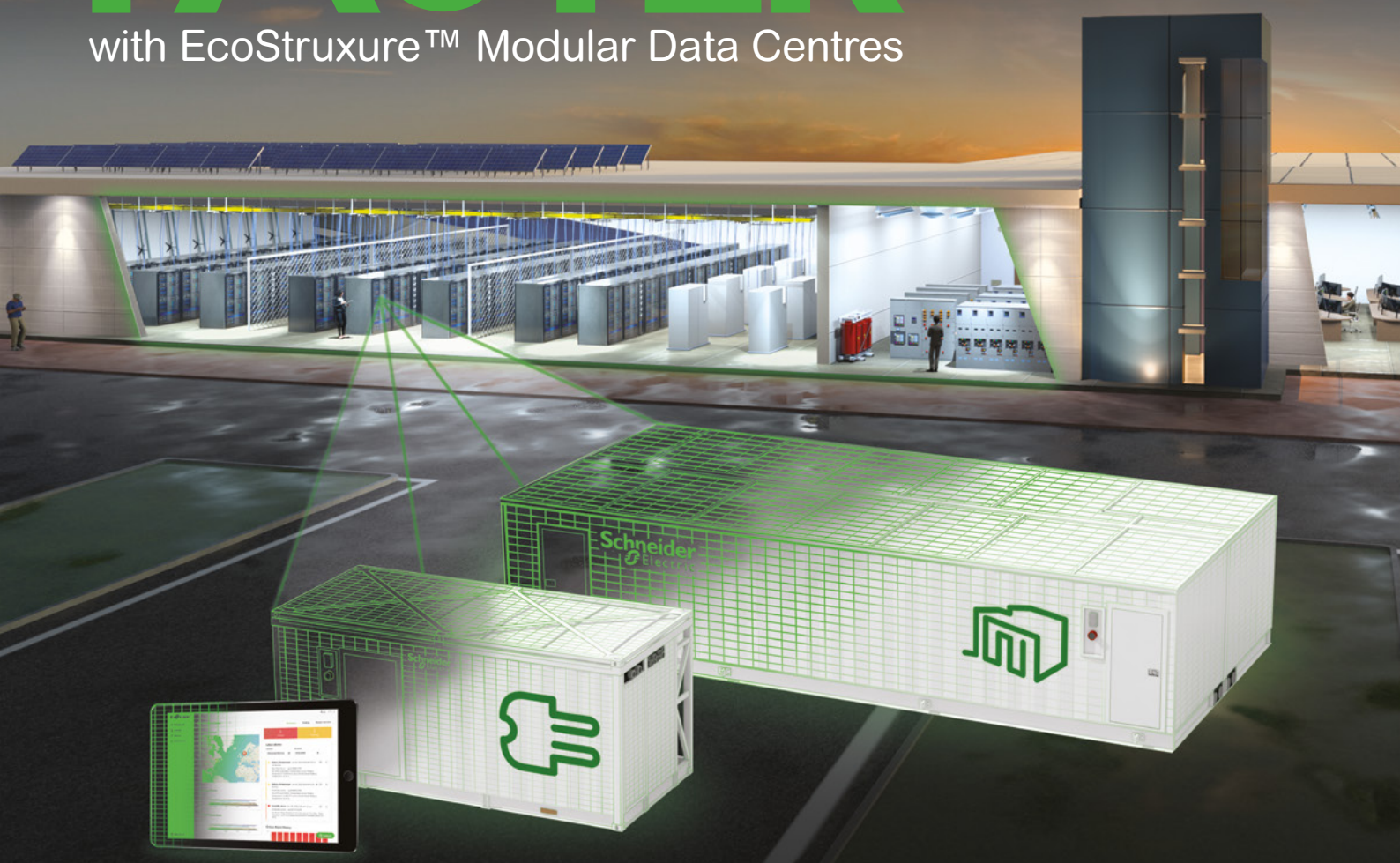
The inefficiencies triggered by the traditional approach, both in cost and time, can only be addressed with a change in philosophy. The trouble is, philosophies are deeply ingrained in a person and can be very difficult to alter. To optimise operations,

EcoStruxure™
Innovation At Every Level

Deploy your data centre

FASTER

with EcoStruxure™ Modular Data Centres



EcoStruxure Modular Data Centres are a smart alternative solution to overcome the traditional challenges of data centre builds.

Such as allocation of space, deployment in industrial environments, or the ability to scale capacity quickly - frees up other real estate or buildings to better support the organization's core function.

- Faster Deployment - Simplify the planning, construction, and implementation
- Flexibility to scale at a more granular level, resulting in less oversizing
- Prefabricated, pre-assembled and pre-tested in the factory prior to shipment.
- Delivered as functional building blocks of power, cooling, IT or all-in-one data centre
- Securely manage system from anywhere

Ready to get started with EcoStruxure Modular Data Centres?

se.com/datacentre

Life Is On | Schneider Electric

The message is clear. Observability can play a key role in bringing these successes to enterprises. How? By accelerating insights, improving data integrity, resilience, and automation, and reducing human error – all while supporting data privacy regulations

businesses must champion IT leaders with a platform philosophy.

Inadequate communication – to explain why such change isn't just necessary but essential – can be another hurdle.

Even if the argument is accepted and leaders' philosophies change, the obstacles don't end there. Users may revert to old processes and systems without proper training and ongoing support. And if there's any misalignment with the business – or if the current infrastructure is incompatible with the new observability solution – then there is bound to be pushback.

Even then, implementing a new solution requires time and money. And if teams are stretched – or budgets are thin – it isn't easy to justify and find resources, especially since there is now an overwhelming choice of observability tools available. Anyone who has spent any time looking into this will know that there is a plethora of choices available, a situation at times so confusing it can lead to decision paralysis.

And it goes without saying that as soon as you start discussing the automation of tasks, talk inevitably turns to concerns about whether such a decision is a precursor to job losses.

What's clear is that enterprises are holding back for plenty of reasons. More than seven in ten (72%) reported that the accelerating pace of technological change – including apps and networks – was problematic, with 58% citing the growing complexity of modern applications.

A similar number (58%) said that observability blind spots in today's modern networks — including cloud, tunnels, and databases — also made life difficult. At the same time, just over half (52%) said that insufficient observability budgets were an 'extremely challenging' obstacle.

The results of observability are plain to see

That said, these obstacles can be overcome. Those enterprises that have already embarked on observability solutions report greater automation, a reduction in tool sprawl, and the 20/20 vision of comprehensive single-pane-of-glass visibility. In fact, according to the survey, enterprises that adopted observability saw an outstanding 233% improvement in the auto-escalation of IT service management (ITSM) or help desk tickets. They also recorded an off-the-chart 213% increase in performance for the auto-remediation of simple alerts.

In fact, they saw improvement across the board in a way that not only fosters transparency and collaboration but also encourages a system of ongoing review.

The message is clear. Observability can play a key role in bringing these successes to enterprises. How? By accelerating insights, improving data integrity and resilience, implementing automation, and reducing human error – all while supporting data privacy regulations.

Or, to put it succinctly, making the transition to observability makes business sense. And it makes enterprises function better.

MANAGED SERVICES SUMMIT LONDON

11 SEPTEMBER 2024

155 BISHOPSGATE LONDON

CELEBRATING its 14th year, the Managed Services Summit – London continues its tradition of being the premier managed services event for the UK IT channel.

As delegates have come to expect the event this year will again feature presentations by leading independent industry speakers, a range of sessions exploring technical, sales and business issues by leading specialists in the sector, and extensive networking time to meet with potential business partners.

The Managed Services Summit UK is an executive-level event, so you know you'll be among the best in the sector, and those featured will explore the latest trends and developments, evolving customer requirements and how to create value through managed services – both for your own organisation and your customers.

THEMES, TOPICS & TRENDS

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

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

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

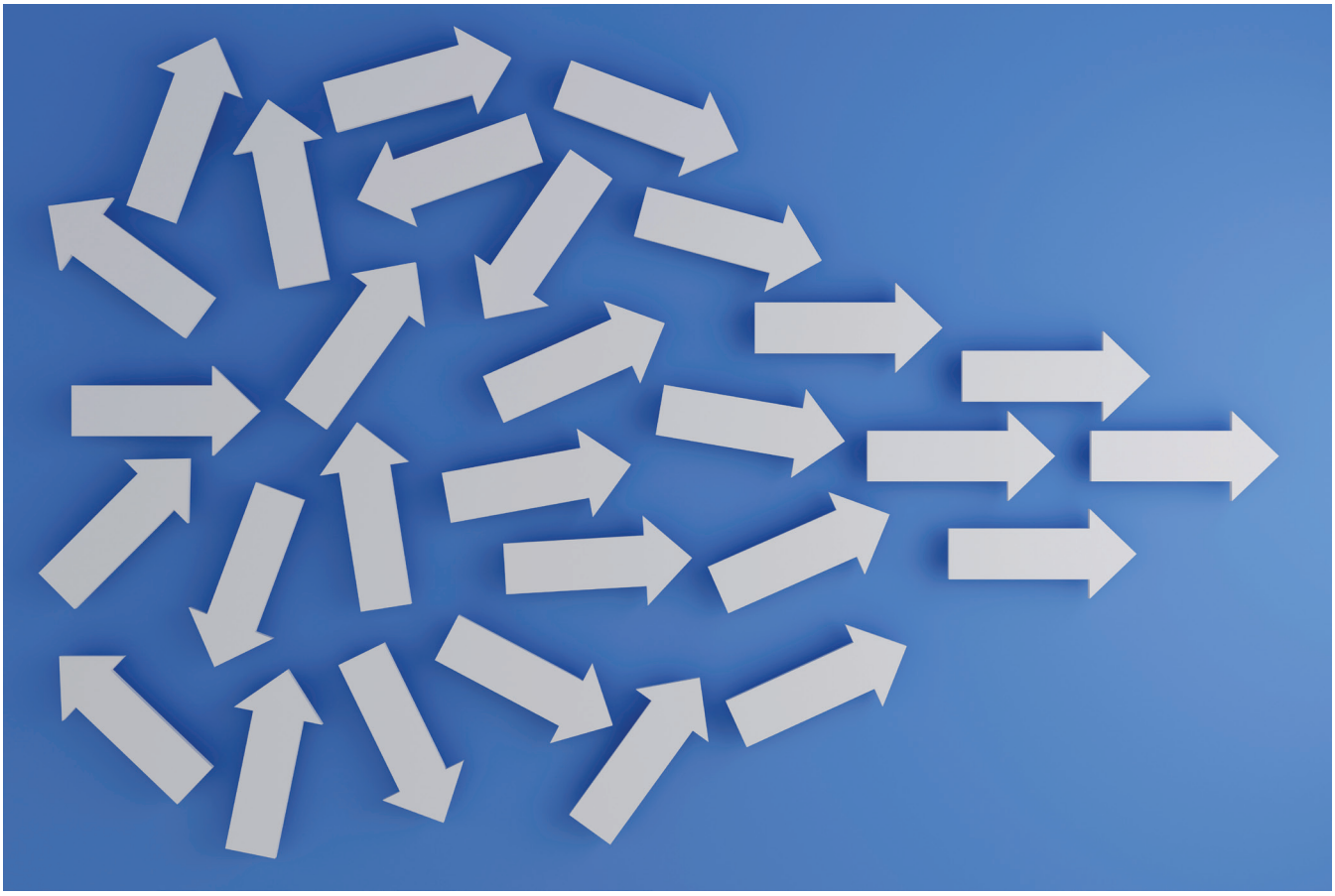
Sukhi Bhadal
sukhi.bhadal@angelbc.com
+44 (0)2476 718970

Peter Davies
peter.davies@angelbc.com
+44 (0) 1923 690211

Mark Hinds
mark.hinds@angelbc.com
+44 (0)2476 718971

https://london.managedservicessummit.com

Angel BUSINESS COMMUNICATIONS · IT EUROPA · ANGEL EVENTS



Business leaders demand total IT-business alignment as experience becomes a key strategic priority

Digital experience has become a pressing concern for C-level executives in every industry. With applications and digital services now the front door for most organizations, business leaders know that they need to be delivering exceptional and seamless digital experiences in order to gain market share and drive growth.

BY JOE BYRNE, CTO ADVISOR, CISCO OBSERVABILITY

CRUCIALLY, what business leaders really want to understand is not just how applications are performing, but how they are driving business value. They're looking to understand how new innovations are engaging customers and driving revenue. And at the same time, C-level executives know that any drop off in digital experience can have profound consequences, in terms of loss of customers, sales and reputation, and so they want to detect threats to application availability, performance and security. They can then direct resources to address potential issues before digital experience suffers.

In order to generate this level of insight into how application performance is impacting business outcomes, organizations need total alignment between IT and the business - something which has traditionally been a challenge for most organizations. And of course, as anybody that works in IT will know, the current shift to modern application architectures is making IT-business alignment infinitely more difficult.

With the pressure mounting to deliver innovative, seamless and secure digital experiences, and

to demonstrate how application performance is creating business value, IT teams urgently need new tools and approaches to meet the demands of senior leaders.

C-level executives want to understand the business impact of digital experience

The research reveals that digital experience has become a significantly more critical issue for 75% of C-level executives over the last three years.

Business leaders want to understand the experience that customers and employees are receiving when engaging with their organization through digital channels. They're looking for insight into application performance to identify where applications are delivering strong business results so that they fully exploit these opportunities. At the same time, they want to identify potential issues and vulnerabilities which pose a significant threat to digital experience, in order to mitigate risk and avoid a revenue-impacting incident.

Within retail, for example, C-level executives want to be able to analyze the performance of every stage of the user journey, from sign up and log-in, through to search and check-out. They want to scrutinize the speed and efficiency of every phase of the workflow, in order to optimize performance and identify opportunities and risks.

Business leaders recognize that digital experience is now critical to commercial success. And this is why they are now heaping pressure onto their IT teams to deliver enhanced digital experiences which drive tangible business results. C-level executives know that IT needs to be completely aligned to wider business strategy and objectives in order for their organizations to compete and succeed in the market. Indeed, all of the CIOs I've spoken to recently have told me that forging closer alignment and connection between IT and the business is now an urgent priority. In particular, they're searching for new ways to measure and report to senior leaders on the business impact of digital experience.

Complexity is making it harder to achieve IT-business alignment

IT teams now find themselves operating under the spotlight, with senior leaders pushing them to deliver ever more intuitive, personalized and seamless digital experiences - and to show how applications and digital services are creating value.

The problem is, however, that the vast majority don't have the tools and insights they need to effectively manage application availability, performance and security, nor to contextualize application data with business metrics. This means they're struggling to maintain seamless digital experiences, and they're unable to show C-level executives how applications are impacting the business. The shift to modern application architectures, built on cloud-native technologies, has resulted in soaring levels of complexity in the IT department. Technologists are struggling to manage an increasingly sprawling and volatile IT estate, with most still relying on multiple, siloed monitoring tools across their applications and underlying infrastructure. They have no clear line of sight for applications running across hybrid environments and therefore it's becoming almost impossible to detect issues, understand root causes and apply fixes before digital experience is affected.

Despite their best efforts, technologists simply can't do their jobs. And as a result, the likelihood of applications and digital services suffering disruption and downtime is growing significantly.

This lack of unified visibility across applications and underlying infrastructure also means that IT teams have no way of tracking the business impact of applications. They're unable to demonstrate how digital experience (whether good or bad) is affecting business outcomes – which is exactly what C-level executives are demanding to know.

Full-stack observability is essential for IT-business alignment and to deliver exceptional digital experiences

The answer to this growing challenge in the IT department is full-stack observability. It provides technologists with real-time insights into availability, performance and security up and down the IT stack, from customer-facing applications right through to core infrastructure, across both cloud-native and on premises environments. This allows IT teams to quickly identify issues, understand root causes and apply fixes, before customers are affected.

Full-stack observability also enables technologists to correlate IT performance data with real-time business metrics. This means they can easily pinpoint and prioritize the issues which have the potential to do serious damage to experience. Significantly, given the need for complete IT-business alignment, by linking application data to business KPIs, full-stack observability enables organizations to track, measure and report on the impact that applications and digital services are having on the business.

With full-stack observability, IT teams can provide business leaders with a comprehensive set of metrics and insights related to experience - from number of unique sessions, average revenue per session and average revenue per transaction, through to 'revenue at risk' from potential outages, and overall user experience (based on defined workflows).

Ultimately, full-stack observability helps to establish a common language between IT and business stakeholders and creates the foundation for IT to operate in total alignment with wider business strategy. For business leaders looking to accelerate growth through their digital channels, full-stack observability is now mission-critical.

Rapid insights and enhanced AI are more important than ever

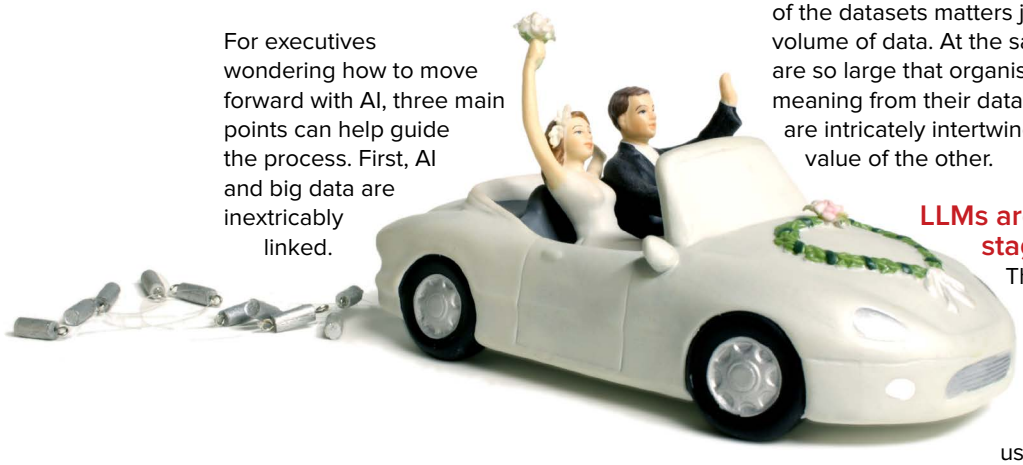
The marriage of service and operations data has become known as ServiceOps, and it's commonly used to drive collaboration across the organisation – automating routine tasks and gaining advanced warning of disruptions.

BY RAM CHAKRAVARTI, CHIEF TECHNOLOGY OFFICER, BMC SOFTWARE

WHEN I'VE TALKED with business leaders in recent months, the conversation inevitably turns to ChatGPT and the rise of generative AI. Nearly universally, executives recognise that the technology represents a huge paradigm shift in business as a tool that could radically change their enterprise. Invariably, I also hear them say they and the people who work for them already have full workloads. They're not entirely sure how to proceed, and they don't have time to learn all of the intricacies of the new AI models, develop a plan that would dramatically transform their business and their internal workflows, and then implement it.

There is a path forward to realising the value of AI in the enterprise – and it doesn't involve a wholesale transformation of the business in one sweeping change, as some chest-thumping futurists would tell you. However, it does leverage existing assets that many businesses have long tried to gain more value from.

For executives wondering how to move forward with AI, three main points can help guide the process. First, AI and big data are inextricably linked.



Second, it's still early days for large language models (LLMs), and they are best deployed in domain-specific models. Third, the absolute key to extracting value from AI is the ability to operationalise it.

AI and data are intertwined

A few short years ago, we used to hear about data lakes – that single repository of firm-wide data built to accelerate insights. Today, companies talk about data oceans. In this age of cloud computing, IoT devices and social media, the trend toward increasing data volumes points ever upward.

Yet depending on the industry, somewhere between 40% and 90% of data goes unused. Companies have so much data, they don't know what to do with it.

For AI to have value, it must be trained on high-quality datasets. For many use cases, the quality of the datasets matters just as much as the volume of data. At the same time, data volumes are so large that organisations can't unravel meaning from their data without AI. AI and data are intricately intertwined, one unlocking the value of the other.

LLMs are still in a nascent stage

There's tremendous hype over LLMs because they allow users to interact with systems using the same language we would use to talk to a friend or

colleague. The potential for the democratisation of once-complex tasks is immense. At first glance, LLMs seem to have almost unlimited potential.

Most organisations should look to apply AI to specific use cases using domain-specific models that can provide immediate value. Further, they should team up with strategic partners (software vendors and systems integrators) from concept through implementation and value realisation. Finally, they should ensure that the solution addresses all of the elements of risk – security, accuracy, quality, privacy, biases and ethics – to be viable for operationalisation.

Company-wide transformation isn't going to happen overnight. However, organisations can look for well-defined projects that can generate success and provide their teams with the experience they need for future iterations.

Operationalising innovation

What does a successful marriage of data and domain-specific AI look like in action? Let's consider IT operations and service management to illustrate the concept. On the IT operations side, organisations have a large volume of data – metrics, logs, events, traces, network, storage, application performance data and cloud monitoring data – extracted from various environments. This data can be linked to the service context of the business such as tickets, downtime and maintenance requests.

This marriage of service and operations data has become known as ServiceOps, and it's commonly used to drive collaboration across the organisation – automating routine tasks and gaining advanced warning of disruptions.

By training and fine-tuning an LLM on ServiceOps, domain-specific data organisations can identify patterns and generate previously unobtainable information such as resolution insights, business risk prediction and more.

Generative AI has the potential to democratise complex tasks by allowing users to interact with them using natural language. They also automate cybersecurity defences in response to attacks that are themselves deployed at speeds faster than humans could possibly react.

Despite generative AI being in a nascent stage, organisations can reap the benefits by operationalising high-value use cases with a pragmatic approach – one that encompasses domain-specific LLMs complemented by instituting the requisite guardrails such as prompt engineering orchestration, security and regulatory compliance built into the solution.

Reshaping the healthcare industry with Generative AI

It's challenging to envision a domain with greater promise for AI applications than healthcare. AI, particularly through neural networks, is driving progress in healthcare across various fronts, from diagnosing diseases to developing novel drugs and treatment approaches.

BY MANISH SHAH, CHIEF TRANSFORMATION OFFICER, SERVICENOW

RECENT YEARS have showcased the synergy of computer science and machine learning, leading to the creation of neural networks that emulate the human brain. These networks exhibit rapid data classification and clustering, reducing analysis time from hours to mere minutes compared to human-performed tasks.

Enter Generative AI (Gen AI), a game-changer that allows healthcare companies to harness these advanced capabilities at scale. Gen AI promises a more seamless, integrated experience for both patients and healthcare providers, ushering in a significant enhancement in care delivery.

An inconsistent patient journey

Navigating patients through the healthcare system can be riddled with variations and inconsistent experiences. A patient journey—doctor visits, medication, diagnostic results, specialty physician, hospital visits—generates a large digital footprint, often in siloed systems that are not easy to decipher quickly to make informed care decisions.

Healthcare has got good at providing detection and diagnostics. During hospital encounters patients are hooked up to individual functioning devices that generate digital signals but often do not talk to each other or to their Electronic Health Record systems. When a specific threshold is crossed, each device sets off a signal or alert at the nurse's station. The nurse must walk into the patient's room to figure out why the alert went off. Around 99% of these alerts are false positives that require significant human intervention, such as the leads coming off or the patient moving in bed.

Enhancing patient care through AI

The excitement around Gen AI is its ability to deliver more precise, targeted intelligence using large language models that take in large volumes of data and then simulate all the possibilities based on algorithms and history.

With Gen AI, we can go well beyond sharing individual data points. We can assimilate and integrate disparate signals into an intelligent layer that merges the data into a holistic picture across

devices and inputs. AI can take individual patient neural sensory networks and bring all the data into one intelligent layer, making it easier for caregivers to respond to the alerts and signals that matter the most. Gen AI helps identify the right resource to oversee patient care and take action at the right time.

Upholding ethical governance in data models

In the last decade, we've seen other game-changing technologies based on AI: digital cameras that use laser ambient light movement to inspect and monitor patients in their rooms. No human being can process all the signals being read by cameras better than an AI.

But the real promise of AI technology lies in providing the intelligence to deliver a safer, higher quality of patient care. Technology is advancing in real time, delivering visual information that is like what a human sees when they walk into a patient's room. Technology can create a more productive, effective workforce that knows precisely which situations require human intervention and can communicate what is needed in a timely manner.

Gen AI is modeling the human brain but processing significantly greater volumes of data. However, while the human brain naturally understands some fundamental basic concepts like morals and empathy, AI does not.

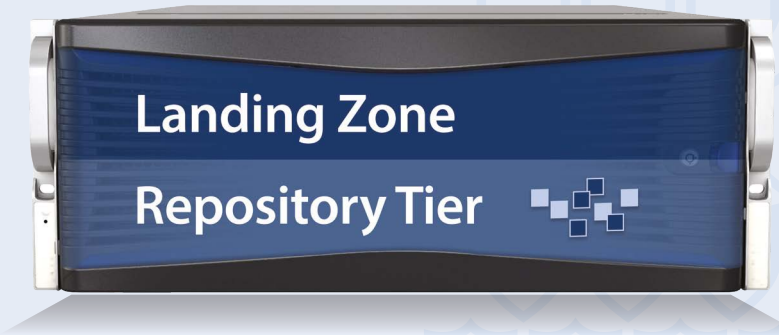
As an organisation, it is important to think about building the basic core elements of ethics, governance, and morals guard rails into AI models. Modeling best practices must align with basic principles for your organisation, such as delivering the best patient care. In the future, a regulatory body may dictate what those principles are, but as healthcare professionals we need to make sure they are part of AI policies from day one.

The future of patient care

The critical moment has arrived to implement Gen AI for an enhanced, seamlessly integrated experience for both patients and providers. It has the potential to shape more intelligent neural networks, facilitating proactive diagnosis and treatment. However, along with tremendous opportunities, there comes significant responsibility. It involves embedding your organisation's ethical and moral principles into the AI models as guardrails. If companies take the necessary steps to uphold these principles, then the resulting advancements in patient care will be worth it, revolutionising how healthcare is delivered in the future.

EXAGRID®

The future is here.
Tiered Backup Storage



- Fastest backups
- Fastest restores
- Scalability for fixed-length backup window
- Comprehensive security with ransomware recovery
- Low cost up front and over time

WINNER
SDC AWARDS 2023

- **Storage Company** of the Year
- **Backup/Archive Innovation** of the Year

Thank you so much to all who voted, and congratulations to our fellow SDC Awards 2023 winners!

Visit our website to learn more about ExaGrid's award-winning Tiered Backup Storage.

LEARN MORE >