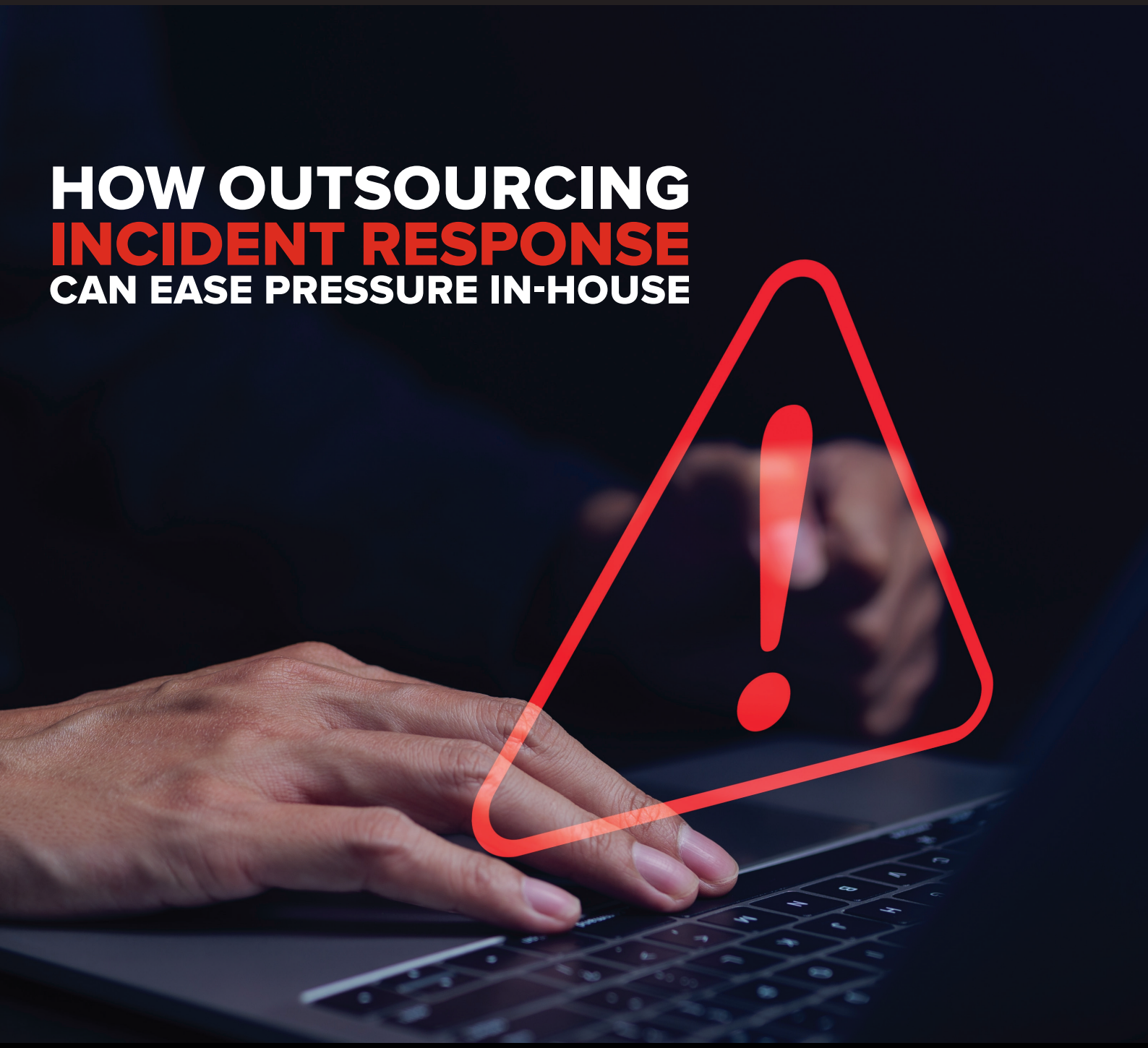
MSP CHANNEL INSIGHTS
CONNECTING THE CHANNEL PARTNER ECOSYSTEM

HOW OUTSOURCING INCIDENT RESPONSE CAN EASE PRESSURE IN-HOUSE



ISSUE I 2024
AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION
MSP-CHANNEL.COM

INSIDE

HOW THE CHANNEL CAN HARNESS THE POWER OF AI

AI is capable of identifying and automating some actions, it's imperative that humans are the ones making critical decisions

EVERYTHING WILL BE CONNECTED

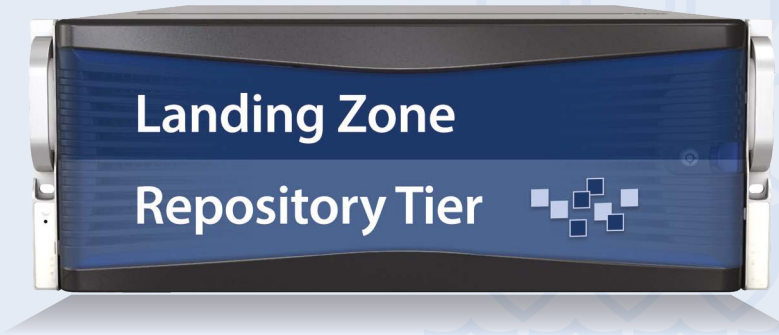
5G networks are expected to grow and develop for years to come, strategists are already offering up visions far beyond 5G

HARNESSING IT TO POWER AI AND GPT

IT leaders cannot open a web browser without learning how AI and GPT can save businesses time, resources, and money

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 >

VIEWPOINT

By Phil Alsop, Editor

The Channel opportunity – knocking on an open door?

A GLANCE through this issue's news pages should provide some heart-warming optimism for the Channel, as these headlines demonstrate:

- Less than one in five businesses have increased productivity with AI tools
- 1-in-2 businesses lose employees when DX projects fail
- AI skills and talent gaps widen
- AI and cloud transformation dominate IT Investment priorities for 2024
- Data reveals workers are craving fewer, yet more impactful collaboration tools
- 56% of organisations are prioritising Cyber Security in the year ahead
- Less than one in ten European businesses succeeding with digital transformation initiatives

Businesses of all shapes and sizes are facing a series of significant challenges and, it would seem, are not doing terribly well when it comes to addressing them. Even allowing for the 'lies, damn lies and statistics' truism, the picture painted by our news stories suggests that a majority of companies have yet to come to grips with AI, digital transformation, cloud, collaboration and cyber security.

Put it another way, if you run a Channel business and knock on the door of virtually any organisation and tell them that you are able to solve their cybersecurity/cloud/AI/digital transformation challenge, then there is every chance you will be welcomed with open arms and be given every opportunity to explain just how you can help. Ok, so end user budgets might be tight and the spectre of previous project failures might cloud the warmth of the welcome you receive. Nevertheless, many, many organisations are caught in the technology transition phase. They know that they must address some crucial, complex business challenges and understand that technology investments will be required along the way, but not that many are confident as to how they go about both the addressing and the investment parts.

Cue Channel organisations to step up to that much touted 'trusted advisor' status. And, let's be honest, many Channel organisations themselves will be struggling to come to grips with some of the same business challenges within their own organisations, let alone those of their customers, not least when it comes to the brave new world of AI.

The good news is that, as you embark on your own technology improvement journeys, you will learn many valuable lessons and gain much valuable knowledge, which will impress your customers as you help them. The less good news is that, at least when it comes to AI, right now it's something of a Wild West Frontier. I'm not sure that many, if any, organisations truly understand just how, where and when AI will be making the biggest impact. In which case, be honest with your customers and collaborate to explore AI's potential. Above all else, don't ignore it just because you don't understand it. There will be some big AI winners over time.

MSP CHANNEL INSIGHTS

Angel BUSINESS COMMUNICATIONS

Editor
Philip Alsop
+44 (0)7786 084559
philip.alsop@angelbc.com
Sales Manager
Peter Davies
+44 (0)2476 718970
peter.davies@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
Stephen Whitehurst: Chairman

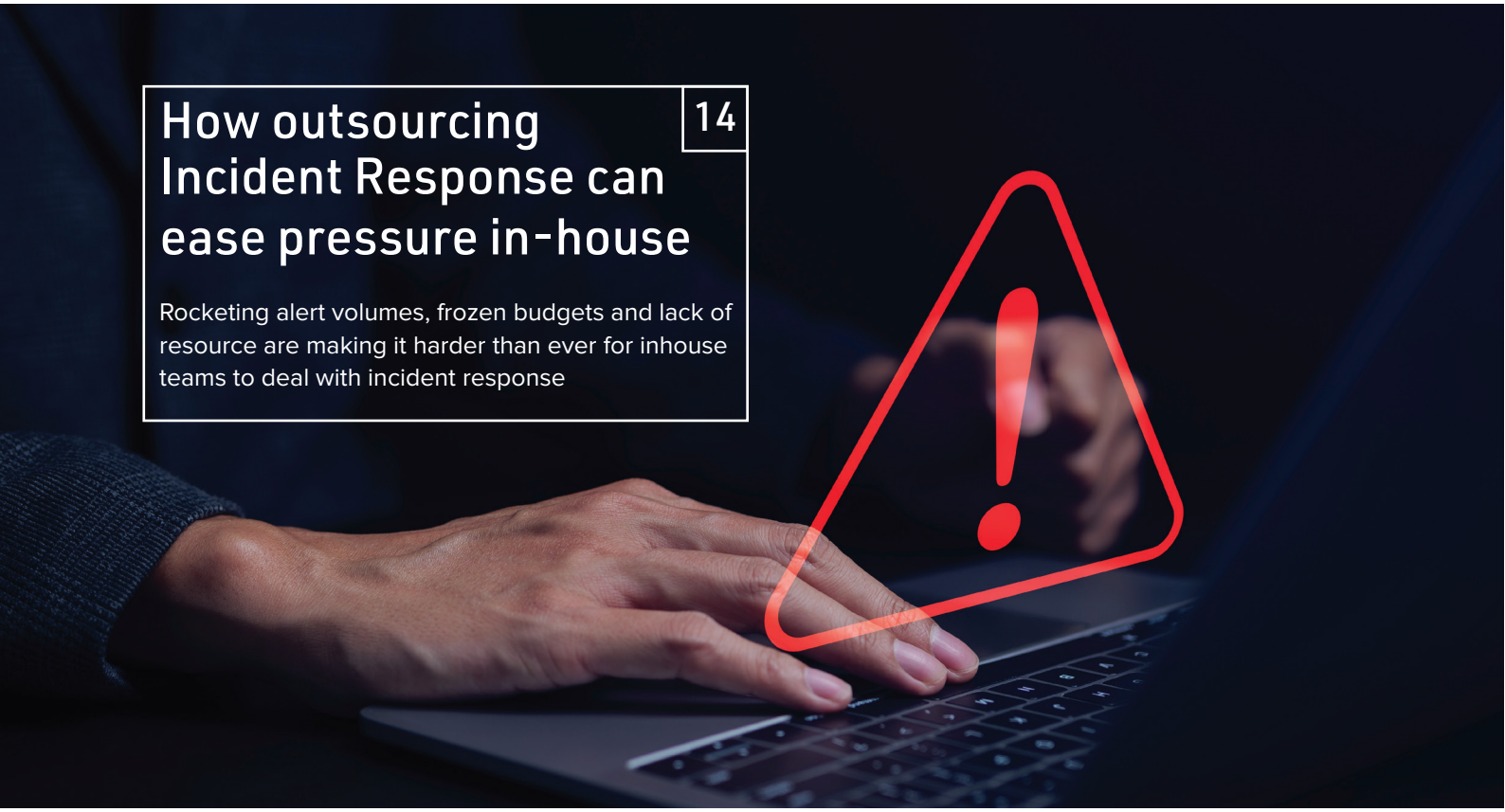
Published by:
Angel Business Communications
6 Bow Court
Burnsall Road
Coventry CV5 6SP

T: +44 (0)2476 718970
E: info@angelbc.com

MSP-Channel Insights is published four 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)

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



How outsourcing Incident Response can ease pressure in-house 14

Rocketing alert volumes, frozen budgets and lack of resource are making it harder than ever for inhouse teams to deal with incident response

16

NEWS

MSP CHANNEL INSIGHTS

Angel BUSINESS COMMUNICATIONS

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

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

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

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

Directors
Sukhi Bhadal: CEO
Scott Adams: CTO

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

MSP-Channel Insights is published six 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.

ISSN 2396-9016 (Online)

Less than one in five businesses have increased productivity with AI tools

New research from Pluralsight reveals that despite accelerating AI adoption, the majority of businesses don't understand the AI skills their employees have, and lack an upskilling strategy to develop them further.

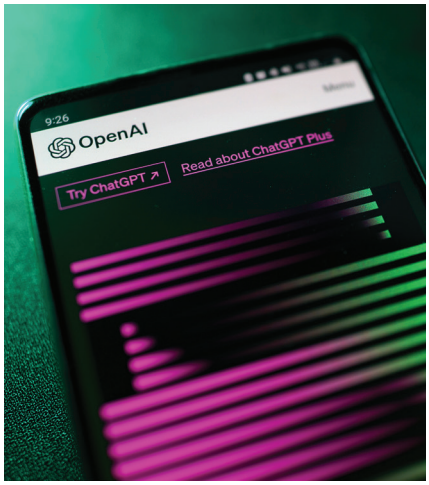
THERE IS a stark disconnect between business investment in AI and how prepared employees are to use the new technology for efficiency and productivity gains. Fewer than 20% of businesses have seen a productivity boost from using AI tools, and over 90% of technologists feel there is not enough investment in training to use the technology. New research from Pluralsight shows this problem is compounding fears around AI and job security amongst employees who feel their role is at risk of being replaced and that their skills will quickly become obsolete.

The report titled "Pluralsight AI Skills Report: The Gap Between AI Investment and Worker Readiness" surveyed 250 decision-makers & 250 technology practitioners in the UK on current strategies and attitudes towards AI adoption, AI skills and the future of technology work in the era of AI.

AI as a competitive driver of business success

Three important findings from the report:

- Businesses across industries are looking to make use of AI. Ninety one percent of organisations say they are planning to increase investment in AI technologies in the next 12 months, and 93% have accelerated AI initiatives in the last 12 months.
- The primary motivations are to enhance the customer experience and/or support, improve the employee experience, and increase automation and efficiency.
- Embracing AI is not just a nice to have anymore; it is becoming a necessity in the modern business landscape across multiple industries. 94% of decision makers agree that those not investing in AI in the near future will fall behind the competition.



Understanding AI skillsets within organisations

Businesses face a significant disconnect between wanting to invest in AI, but not believing that it will actually be effective. The research shows 40% of business leaders and technologists believe AI will add more frustration to people's jobs.

At the same time, 20% of business leaders do not understand their teams' proficiency in AI, and there is uncertainty from technologists too. Just over half (53%) of employees think their role is at risk of being replaced by AI, and 79% think their skills will quickly become obsolete as AI advances.

Indeed, 91% of business leaders themselves say they are likely to replace or outsource talent in order to successfully deploy AI initiatives. Technologists are well aware of how to fend off this potential risk; 97% acknowledge that staying up-to-date on AI skills is the best way to ensure they have a job in the competitive market.

Commenting on the research Pluralsight's CEO, Aaron Skonnard, said, "If businesses are to succeed with AI deployments, there is no doubt that they need the right talent in place to work with the technology. But this must not come at the expense of their current workforce – who, through upskilling, can help organisations fill skills gaps from within. Organisations must focus on training their existing talent to propel them through the next wave of AI innovation."

Matching AI investment with employee training to drive productivity

In order to bridge the gap between AI investment and skill sets, developing talent is crucial. But a lack of investment into skills is felt by employees, with 81% of technologists agreeing that their company often invests in new technology without consideration for teaching employees how to use it. While 94% of businesses agree that AI initiatives will fail without staff who can effectively use and work with these tools, 88% of technologists agree that their company is investing in training for new AI-technologies less than they should be.

This means employees are left to play catch up with new AI investment, and businesses are suffering, with only 16% seeing increased productivity or efficiency as a result of adopting AI tools.

"Unsurprisingly, fears that AI technologies have the potential to put people out of work are top of mind for technologists," according to Skonnard. "Instead of focusing on how jobs will be replaced by AI, business leaders and technologists should instead focus on how they can use AI to augment their existing skills. When it comes to AI, it shouldn't be about how organisations can get by with less, but how organisations can do more with their existing staff."

1-in-2 businesses lose employees when DX projects fail

Nearly 9 in 10 senior business leaders (88%) said that just 50% or less of their digital transformation (DX) projects completed in the past year achieved the expected goals or outcomes, which has impacted the employee experience.

EVANDA has launched a sponsored IDC InfoBrief, Leveraging the Human Advantage for Business Transformation. Exploring how organisations are tackling the evolution to the digital business era, the InfoBrief uncovers the roadblocks, tactics and outcomes of digital transformation (DX) efforts in the last year, as well as strategic drivers and approaches to integrating major technologies shaping the landscape, such as artificial intelligence (AI) and automation.

The research, which surveyed business leaders and decision-makers across the globe, revealed that the overwhelming majority (88%) said that only 50% or less of their DX projects in the past year met the expected goals or outcomes. And when businesses miss the mark on DX projects, it's not just their infrastructure or competitive position that suffers.

While 62% reported failure resulting in them being less technically mature than competitors and having a longer time to market, key challenges damaging the employee experience emerged as consequences too. Many are facing frustrated staff (56%), as well as a rise in staff attrition (50%) and a less stimulating work environment (44%).

The causes of lacklustre results from digital transformations reinforce the notion that strategies too often neglect to prioritise a people-first approach in the planning, design and implementation of digital initiatives. For example, 39% of respondents indicated that a lack of employee buy-in was a key reason for failing to meet expected outcomes, implying a need for cultural considerations to encourage user engagement. This was followed by conflicting opinions from leadership (36%) and a lack of collaboration internally (33%), demonstrating a struggle to successfully navigate organisational dynamics or engage stakeholders throughout projects. When reflecting on failed DX projects, over half recognised that investments would have been better channelled into people-centric projects such as upskilling staff (55%) and improving IT and line of business communication (50%).

Amid the rapid advancement of AI and the generative AI boom over the last few years, the survey also uncovered strong levels of current implementation and adoption plans in the pipeline, with almost half (49%) of the respondents having already deployed AI in their organisation or running a proof of concept. Many organisations recognised the impact of retaining a human influence on their use of AI, with 51% declaring it as very or extremely important.

Similarly, automation strategies were aimed at empowering a stronger employee experience and freeing people to work more strategically. 58% said their automation strategy is highly or very highly focused on removing mundane tasks, and 54% agree that employee engagement and satisfaction are integral. The data on DX shortcomings, however, highlights a gap between many businesses' intentions for digital projects and the ability to bring these to fruition.

Despite this, for those who do get DX projects right, there are promising employee and customer outcomes beyond the business benefits. As well as achieving outcomes such as process optimisation (62%), cost reduction (57%) and revenue increases (53%), respondents also reported improved customer experiences (45%) and an uptick in employee productivity, satisfaction and retention (42%) when initiatives were effectively managed. Endava CEO John Cotterell commented: "The success of digital solutions is inherently reliant on understanding how people will respond to new technologies. This research reinforces the fact that nurturing amazing products and services demands a human-centric approach throughout every stage of digital evolution. In practice, this is all about people, understanding user needs and expectations, working through cultural barriers to adoption and collaborating with employees to build engagement from the outset.

It's encouraging that more and more businesses are recognising the importance of human response to new technologies, as well as the potential impact of not prioritising people within technical development. As they shape their digital strategies for the year ahead and beyond, developing inclusive digital solutions and constantly being mindful of people will go a long way towards bridging the gap between innovative products and market success."

AI skills and talent gaps widen

Skillsoft's IT Skills and Salary Report highlights the importance of skill building as businesses strive to keep pace with rapid technological change driven by AI.

SKILLSOFT has released its 2023 IT Skills and Salary Report. Based on insights from more than 5,700 global IT professionals, including leaders and staff members, the report examines the state of the IT industry, underscoring the pressing need for workforce upskilling and reskilling given the rapid advancement of AI and machine learning (ML) technologies.

Key findings include:

- AI and ML are the biggest areas of focus for IT leaders, though 43% rate their teams' AI and ML skill sets as low.
- One-in-three IT leaders are struggling most with finding qualified AI and ML talent.
- The top driver of skills gaps is the rate of technology change outpacing training programs.
- Last year, 45% of IT professionals said management did not see a tangible benefit from training. Just 15% now say the same, as skill building becomes a business imperative.
- 97% of IT leaders say certified staff adds value to their organisation.
- IT professionals' top reason for skill building is to prepare their organisation for new technology, especially as generative AI (GenAI) becomes more advanced.

"With AI accelerating disruption at an unprecedented pace, the need for workforce training has never been more obvious and consequential," said Orla Daly, Chief Information Officer, Skillsoft. "Organisations are at a critical point where they need to be deliberate and proactive about building skills and capabilities – especially related to AI – or risk falling behind in the coming year. Interactive training experiences where professionals learn by doing will unlock rich possibilities, creating business value while increasing team member engagement and morale."

Increasing scope and efficacy of training.

Skill development is a critical piece of the puzzle for building a competitive organisation, though more work is needed to optimise training among technology teams. Only 37% of IT professionals report receiving training "most of the time" when their employers invest in new technology. Additionally, compared to last year, 40% more IT leaders say their organisation is not investing enough in professional development and 80% more say their current training programs are not effective at developing the skills they need.

This presents a missed opportunity for strengthening business outcomes and talent retention. IT professionals who receive training report improved work quality (62%), a greater sense of engagement (47%), and faster job performance (45%). Meanwhile, 82% of IT professionals say training is extremely or very important to their career and a lack of development was the top factor that drove respondents to change employers in the last year.

Taking a "whole-person" approach to development.

"Hard" or technical skills have traditionally been prioritised in the IT industry, while "soft" or power skills can fall by the wayside despite being essential for adapting and augmenting transformative technologies, especially GenAI. IT professionals rank team communication (40%), interpersonal communication (21%), and emotional intelligence (13%) as the three most important skills for IT leaders to have.

However, just 6% of IT leaders said leadership skills will be a key area of investment moving forward, and only 7% said the same about power skills. With 72% of IT leaders ranking their existing teams' leadership skills as medium to low, there is a significant gap between training needs and priorities in this critical area.

This presents a major opportunity for businesses to build well-rounded IT professionals by providing leadership training as a differentiator to drive greater innovation, growth, and efficiencies.

Building next-generation skilling programs

Skills gaps, talent shortages, and technology transformation are challenges impacting IT departments. However, they are all obstacles that can be remediated with a well-orchestrated training program that blends multiple modalities and content types.

According to IT professionals, the most important features of a training program include quality of content (55%), opportunities for hands-on practice (50%), and multiple learning methods (38%). Online, on-demand training is the most popular learning modality among IT professionals this year (59%), followed by online live training (46%) and impromptu training at work (31%).

Additionally, IT professionals leverage a variety of learning resources ranging from employer training subscriptions (35%) and certification prep guides (25%) to online communities (24%).

AI and cloud transformation dominate IT Investment priorities for 2024

Businesses continue to grapple with IT recruitment and training challenges as they seek to keep up with accelerating technology advancements.

NEW RESEARCH by Rackspace Technology, in association with VMware, finds that despite ongoing economic uncertainty, businesses are committed to prioritizing their IT investments in 2024, particularly in transformative technologies such as artificial intelligence (AI) and cloud transformation.

According to the 2024 IT Outlook Report, which surveyed 1,420 global IT professionals, 63% of organizations plan to re-calibrate their investments in 2024. Moreover, artificial intelligence dominates as the top priority, with 65% of respondents identifying pervasive artificial intelligence as the technology that will have the most significant positive impact on their organization over the next 12 months.

The survey also underscores the continued adoption of the cloud. When asked about the makeup of their organization's IT infrastructure and how it will evolve over the next 12 months, edge computing, private cloud, and public cloud increased as a percentage of workloads, while data centers, colocation facilities, and mainframes declined.

"These results highlight a decisive shift in artificial intelligence from the technical curiosity and pilot programs in 2023 to accelerating business outcomes through the industrialization of Responsible AI solutions in 2024," said Srini Koushik, President of Technology and Sustainability at Rackspace Technology. "In the cloud arena, the increased focus on the edge and private cloud indicate that organizations are simultaneously migrating more of their critical workloads while adopting a more sophisticated workload-aware approach to their overall cloud infrastructure."

AI Evolution

As generative AI continues to mature and grow in importance, 33% of organizations say they have either completed prototypes and are taking projects into production or already have projects underway and plan to expand them, while another 66% of respondents are either currently ideating on the use of generative AI or plan to do so. Just 1% of respondents have no plans to use generative AI. Moreover, 67% of those surveyed say they will have generative AI either integrated into some processes or fully integrated into all processes in 12 months.

While many organizations are using AI primarily for "table stakes" tasks such as sentiment analysis and code development, the use cases where respondents see the greatest expected benefit include security (54%), new product development (50%), increased productivity (45%) and enhanced speed and efficiency in existing work processes (42%). At the same time, organizations report challenges in implementing AI programs. 42% of survey participants acknowledge demonstrating the value of AI as a hurdle, while insufficient technological infrastructure support for AI was noted by 38%, followed by a shortage of skilled IT talent, at 32%. Organizations also continue to grapple with data governance policies and strategies in response to AI. Less than half (46%) of organizations have policies or strategies in place to address privacy concerns, and only 42% say they have addressed data bias.

"While some organizations have already implemented AI-powered solutions, many are still in the early stages, grappling with the considerations and challenges associated with AI

adoption," added Koushik. "They are not just contemplating but actively addressing the issues associated with the widespread integration of AI into their business processes and operations, marking a crucial phase in their transformative journey."

Private Cloud, Edge Ascending

The survey highlights an ongoing evolution in companies' cloud strategies as workloads migrate away from within the organization's walls. When asked to compare their current infrastructure with their projected infrastructure composition over the next three years, private cloud rose by 4%, while public cloud saw a smaller increase, with concurrent decreases observed in workloads running on other servers, including mainframes and on-premises data centers. Edge computing is also becoming a priority, with 30% of organizations saying it will be part of their IT infrastructure makeup in 12 months, compared to 26% today. 75% of respondents say they are employing a hybrid cloud strategy today. Survey participants identified resource shortages and security/compliance risks as their primary challenges in transitioning to the cloud, at 34%. This was followed by concerns such as cost overruns (33%), resistance to change (28%), inappropriate cloud provider selection (24%), and a lack of stakeholder buy-in (23%).

Data reveals workers are craving fewer, yet more impactful collaboration tools

Almost half (45%) of workers want more guidance from their organisation on how to collaborate effectively with teammates.

ASANA has released new data from its Work Innovation Lab, with insights from Dr. Bob Sutton, Stanford Professor and bestselling author and Dr. Paul Leonardi, Department Chair and Professor at UC Santa Barbara. The findings, based on 3,004 knowledge workers across the US & UK, reveal the potential for more effective utilisation of collaboration technologies in the workplace.

Broken tech stacks are draining workers' time

Almost a third (32%) of workers say that their organisation has collaboration technologies that aren't being used effectively, in part because of insufficient training and change management around the technologies. Almost half (45%) of employees say that their organisation should provide more guidance on how to collaborate effectively, underscoring the importance of more structured workflows, clear communication channels, and visibility into team activities to aid in more intuitive and intentional collaboration.

The majority (68%) of employees interact with different functions daily, highlighting the need for tools that facilitate smooth interdepartmental collaboration. However, almost a third (32%) of workers say that their organisation has collaboration technologies that aren't being used effectively, with 38% of workers claiming their organisation uses four or more different communication and conferencing tools.

This fragmented tech stack is having a substantive impact on workers' time. On average, every day, employees spend:
· Nearly an hour and a half (84 minutes) each workday looking for information they need to get their work done.
· 57 minutes per workday switching between collaboration tools.
· 30 minutes per workday just deciding what collaboration technologies they should use for a specific task.
That's the equivalent of spending over a day and a half each week inefficiently navigating too many disconnected tools to get work done.

This time drain caused by ineffective collaboration isn't going unnoticed by workers. Almost one-third (32%) of workers are not opposed to changing jobs for a company that provides more useful collaboration technologies for them at work.

What is a clear solution? We find that the most productive workers use a "sweet spot" of 12 different digital collaboration tools, including one (but not more than one) work management tool. These tools are intended to provide a central source of truth, and the fragmentation is felt more acutely when information is spread across multiple work management tools.

Businesses must bolster tech audits
One reason organisations may be operating with less than optimal collaboration processes is that they've hyper-invested in collaboration tools in silos and haven't taken time to stop and evaluate their usefulness. 34% of knowledge workers aren't sure how often their organisation evaluates whether the collaboration technologies used across the business are useful or not.

Of the 66% of knowledge workers who do have a sense of how often their organisation evaluates the usefulness of collaboration technologies, over half (55%) say it's done twice a year or less, or never at all. This suggests that there's a need for more frequent business-wide evaluations.

Workers ask for standardisation in tech tools

Standardising tech tools across teams could also help to reverse ineffective collaboration. Despite the multitude of different roles, skills, and viewpoints in organisations, the majority (74%) of workers would prefer that everyone in their organisation use the same set of core collaboration technologies. They are frustrated by the friction that comes with a siloed approach. Interestingly, we found that workers care much more about standardisation than about customizability in judging the usefulness of a collaboration tool.

AI provides part of the solution

AI can help automate routine tasks, intelligently organise data, and provide actionable insights, thereby potentially reducing the need for redundant tools.

Over a third (36%) of workers say that AI will help reduce the number of collaboration technologies needed to complete their work—work management tools that are built atop strong data foundations that connect work across the organisation will become more critical than ever.

Employees using too many tools are most enthusiastic about AI (59% versus 47%) and its ability to help reduce the number of tools they need to complete their work (50% versus 36%).

However, only 28% of workers say their organisation is well-prepared to deploy collaboration technologies with AI capabilities, indicating that even though AI can positively impact how we collaborate with others, it's difficult to get right and there's a desire for AI capabilities that are integrated into existing tools.

Softcat study reveals key business tech priorities for 2024

56% of organisations are prioritising Cyber Security in the year ahead.

A NEW REPORT by leading providers of IT infrastructure, Softcat, offers a look into the technologies that businesses are prioritising over the next 12 months. The findings are based on the views of more than 4,000 customers from 2,900 organisations in the UK and Ireland, across 27 industries in both the public and private sectors.

The report, which is produced annually, reveals organisations are, for the second year running, prioritising Cyber Security above all technology areas, with 56% of respondents saying that it is their focus over the next 12 months. Kieron Newsham, Softcat Chief Technologist for Cyber Security, said: "It's clear from the report's findings that organisations are yet again recognising the importance of cyber security amid the relentless pace of technological advancement and evolving threats. "To truly mitigate risk, organisations must be resilient. They can do this by being wary of how new technologies can increase threats while embracing and utilising them to recover and normalise operations after cyber incidents."

After Cyber Security, organisations are prioritising Digital Workspace, with 'Devices and End User Computing' the second most cited technology investment area for over a third of organisations over the next year (39% of respondents).

Organisations that recognise the importance of optimising their digital workspace to maximise efficiency in an age of flexible work environments and an ever-changing digital landscape, e.g. generative Artificial Intelligence (AI), will reap benefits such as enhanced productivity, security and sustainability. Data is the third most important technology area, with 28% of customers

citing it as a priority area over the next 12 months, followed by Networking and Connectivity (25%) and Datacentre and Private Cloud (18%).

The report also highlights the importance of AI, its potential to reshape business and technology and how organisations should balance the scales of opportunity and challenges to harness the newfound intelligence responsibly. Meanwhile, this year, organisations were also able to share what they expected to be their biggest challenges over the next 12 months.

People-related challenges were a concern for 48% of respondents, followed by Commercial Risk (40%), Processes (31%), Technology Experience (30%) and Procurement (26%).

For those working in the IT landscape, key themes mentioned for each challenge include inflation, technology advancements and skill gaps, which will likely see organisations and their employees increase resilience and continuously adapt to remain ahead of the competition.

Additionally, as organisations embrace the fifth industrial revolution, respondents were able to rank their key environmental, social and governance (ESG) focus areas for the year ahead.

People and Culture is top the priority for 70% of respondents over the next year, closely followed by Sustainability (68%) and Diversity and Inclusion (55%). This year marks the third year running that sustainability is high on the agenda for many businesses, with more than three times more respondents citing it as a priority, up from 19% in 2022. Richard Wyn Griffith, Chief Commercial Officer, commented on the findings: "As we continue to navigate the ever-changing landscape of technology, it is essential that we remain vigilant and adaptable. The past year has seen global unrest, but it has also presented us with countless technological opportunities for growth and innovation.

By taking a measured and strategic approach, we can effectively manage the risks associated with emerging technology, while also seizing the opportunities that it presents. It is critical that we remain proactive in our efforts to safeguard against cyber threats, integrate AI into our operations, and build digital resilience.

"Only by embracing change and remaining steadfast in our commitment to progress can we hope to thrive in this new age of digital transformation. I look forward to continuing to work with our customers towards a brighter future!"

More than half admit to ignoring cybersecurity alerts due to information overload at work

More than half of today's office workers are ignoring important cybersecurity warnings due to being overwhelmed and fatigued from digital communication.

NEW RESEARCH from CybSafe has shed light on an alarming trend in today's workplaces. Digital overload and multiple new communication channels are not only reducing productivity but are leading to a decline in engagement with cybersecurity training. As a result, people are increasingly ignoring cybersecurity notifications and are more likely to display risky cybersecurity behaviours like clicking on phishing emails or ignoring notifications to turn on Multi-Factor Authentication (MFA).

More than half (54%) of today's office workers are ignoring important cybersecurity alerts and warnings due to information overload from digital communication. 47% admitted to feeling the information overload is having an impact on their ability to identify threats such as suspicious emails.

With 72% confirming they feel at least occasionally overwhelmed with the amount of information and communications they get at work, it's little wonder cybersecurity engagement is being impacted as a result. Today's workers are frequently interrupted by the buzz of notifications, reminders, and messages on various platforms.
The new research is released as ICO data indicates a 41% year-on-year increase in data security incidents reported to the body between Q2 2022 and Q2 2023. Cyber incidents (a type of breach with a clear online or technological element which involves a third party with malicious intent.) saw a significant 157% increase over the same period, with ransomware and malware events seeing particularly prominent increases of 241 and 550%, respectively.

As cyber threats evolve and increase in complexity, the implications of these trends are concerning. Risks range from individual data compromises to significant business data theft.
Worryingly, the survey of 1000 office workers uncovered important cybersecurity warnings are going unnoticed. The digital deluge is affecting employees' ability to spot cyber dangers. 41% feel information overload is impacting their ability to retain and apply knowledge gained from cybersecurity training sessions - a fact being displayed by people's self-reported security behaviours.
Daily habits show a slip in safe actions and higher engagement in risky behaviour.

36% admit to occasionally cutting corners on cybersecurity practices
7% admitted they often skip steps like using safe networks or setting strong passwords, all in the name of saving time.

Less than 1 in 4 employees - 23% - report being engaged with their cybersecurity training. And 41% say there's just too much information to remember and use. This shows that companies need to stop and consider better ways to help employees change their behaviour and engage with cybersecurity. If the end goal of an organisation's cybersecurity programme is culture change, access to training in itself is not evidence the training is being consumed or internalised within the workforce. There is more work to be done on how and where leaders are communicating cybersecurity best practices to their workforce.

The survey lays bare the obstacles hindering cybersecurity training.
The top barriers:
- Time constraints (42%)
- Interest and motivation (30%)
- Complexity of training materials (15%)
- No direct relevance to daily roles (10%)

The research also found 77% of people expect their digital experiences to be as frictionless and personalised as consumer experiences. This suggests leaders need to do more if they want to see stellar cybersecurity engagement within their workforce.

Oz Alashe MBE, CEO of CybSafe, reacted to the research, stating, "As time goes on, organisations understand the question 'do our people have access to cybersecurity information?' is the wrong one. Instead, many are now asking, 'How do we give cybersecurity support in a way that will engage workers and lead to genuine behavioural change?'

"We must empathise with the workforce of today. Employees are caught in an erratic stream of emails with varying levels of importance and instant messages on multiple platforms, not to mention social media-it isn't surprising cybersecurity information is getting lost along the way. Importantly, however, this inconsistency isn't merely inconvenient or irritating— it's actively undermining the goal of informed cybersecurity behaviour. This is the issue we now need to tackle as security professionals."

"As a result, CISOs need to consider not only the material their people are consuming but on what platform it is being delivered to them and in what way."

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

How outsourcing Incident Response can ease pressure in-house

Rocketing alert volumes, frozen budgets and lack of resource are making it harder than ever for inhouse teams to deal with incident response. Our survey of 205 IT security decision makers in August revealed that 90% of them saw an increase in security alerts over the past 12 months. The majority (76%) reported an increase of between 1-50% of alerts while just over a quarter (26%) reported a 26-50% increase in alerts.

BY PATRICK WRAGG, HEAD OF INCIDENT RESPONSE AT INTEGRITY360

IT'S NOT JUST ALERT FATIGUE that is causing issues, however, because responding to incidents can be highly stressful. All eyes are now on how effectively the team responds and mitigates the threat resulting in a high-pressure environment. The most stressful aspect of responding to a cybersecurity incident was the speed required to effectively diagnose and mediate incidents cited by 40%, followed by the sense of responsibility (31%). Interestingly, 24% said the fear of being wrong was an issue which ranked above any difficulty in diagnosing the incident (22%). C-level executives feared being wrong more than information security analysts, perhaps because the fallout from a poor response to a cyber incident could be worse or even catastrophic for their career.

Other stressful elements among information security analysts were ineffective communication, suggesting that reporting processes aren't as smooth as they could be, and the relentless need to focus on the incident until it was resolved, both of which were named by 26%, respectively. In contrast, the CIO clearly feels caught in the middle, with 30% reporting they experienced pushback on recommended response from teams and 28% feeling under pressure from above via the C-suite.

Challenges facing IR

Having proper processes and sufficient resource in place is key for effective response but the survey suggests that there have been cutbacks here. Almost a third said the top challenge was having insufficient budget, with the complexity of the incident and a lack of board level understanding coming in joint second. The disconnect with the board was felt most keenly among information security analysts (33%) whereas CIOs were markedly less concerned (13%) suggesting those doing the firefighting do not feel sufficiently heard.
In terms of resource, the skills shortage is beginning to be felt, with 23% saying there was a lack of skills or experience among those tasked with response, while a fifth of respondents and a third of CIOs thought they lacked the tools to be able to respond effectively (this was the second biggest challenge after budget for them).

Unfortunately, it looks as those some organisations aren't keeping their incident response capabilities up to date. Among information security analysts, over a quarter were concerned about untested incident response plans and processes while a fifth complained of a lack of defined IR playbooks, indicating that while many have incident response plans in place these are not always regularly put through their paces which would lead to the process being continually improved.

Collectively, this all paints a picture of incident response being under strain which means the organisation becomes less effective in its response, increasing the potential for a breach. It's for these reasons that organisations need to think carefully about how well equipped they are to handle incident response before, not after, a major incident occurs. But this also presents specialist security providers, namely those offering cyber defence and incident response services, with an opportunity to provide some much needed assistance.

Outsourcing IR

Outsourcing incident response can provide numerous advantages, acting as a scalable resource that then frees up in-house personnel to focus on improving the security posture. The customer benefits from access to specialists 24x7, providing the organisation with more resource and expertise to help manage the situation. This can include malware experts who are able to utilise multiple investigation and forensics tools, experience and methodologies to respond to the incident and assist with decisions. Consequently, investigations can be carried out faster, Mean Time to Respond (MTTR) reduced and dwell time (i.e. the time during which the attacker is on the network) can be minimised.

Assured cyber incident response providers, such as those assessed by the NCSC, can help with every stage of the incident lifecycle from triage, through to containment and remediation. This begins with exploring the scope of the incident and establishing a communication matrix for escalation. As undefined or unclear lines of communication and responsibilities can be an issue, this helps ensure that everyone understands their responsibilities and provides a clear line of sight for senior management. Second comes detection and analysis. Assessment tools will need to be deployed and used to determine the potential impact and log analysis conducted in order to carry out root cause analysis. The incident can then be contained and eradicated, minimising downtime and paving the way for the organisations to return to business as usual.

The final stage sees the incident response team produce a technical report detailing the incident and each stage of the investigation which can then be pored over by the board and senior management to create improvements.

Considerations for the channel

An effective incident response provider should invest in advanced toolsets to keep their offerings competitive and have a diverse range of specialists on the team in order to provide their customers with sector-specific advice. They should be able to notice attack patterns and swiftly respond to zero-day vulnerabilities, for example. Doing so requires them to have an accurate understanding of the customer environment, so they need to be onboarded in advance, briefed and a retainer contract put in place so that in the event of an incident the resource is immediately to hand.

However, increasingly, incident response is now being seen as a part of a more proactive offering – Managed Detection and Response (MDR). This uses machine learning and AI to detect and analyse threats in real-time and automated response which means it can significantly drive down MTTR. Security analysts threat hunt to identify and address threats before they can impact operations and a range of services is employed, from endpoint and network monitoring to threat intelligence and, of course, incident response. It's this combination of automated technologies and human expertise that marks MDR out and it is particularly suitable for those businesses that are highly targeted by criminals.

Going forward it's clear that incident response performed in-house will reach its limit in certain sectors, providing channel players with the opportunity to offer their services to boost resources.

Having an outsourced incident response resource on tap is undoubtedly valuable in conferring human and technological resource to carry out investigations and digital forensics. It provides a scalable offering that confers peace of mind. But for many of those that take a critical look at their detection and response capabilities, factor in ongoing investment, a growing skills shortage and an increase in threat levels, it may well make more sense to look at MDR.

The power of differentiation

It's time IT resellers leveraged brand-building strategies

BY NATHAN SELBY, HEAD OF CLIENT SERVICES AT ACTIVE PROFILE

WITHIN THE LAST FEW YEARS, the IT reselling landscape - and the entire world - witnessed a seismic shift, largely driven by a supercharged surge in pandemic-driven remote working. In response to the COVID-19 crisis, resellers moved at pace to support businesses in their overnight move to smart working. And it came as no shock to see that many of these businesses were ill-prepared for such huge and irrecoverable changes.

A major result of this? Sales of solutions such as Microsoft 365 and Google Workspace sky-rocketed at a rate we'd never seen before.

A shifting focus

Jump ahead to 2023, and there's been another crucial shift of focus. Now, the widespread utilisation of vendor solutions for the day-to-day running of many businesses has pushed the development of in-house products and services firmly into the spotlight. Resellers are investing more than ever when it comes to crafting new solutions for customers - either building on top of existing vendor products or creating their very own intellectual property.

But with so much careful planning and key resources being ploughed into these smart solutions, are resellers neglecting to nail their brand awareness strategies when it comes to taking these products and services to market? And without an established and unique brand voice, how do resellers hope to cut through their noisy, oversaturated marketplaces?

The answer is brand-building

It's no surprise to hear that the IT reseller landscape has always been a fiercely competitive one. In a pre-COVID world, businesses often stuck to the same old trusty IT partner. One that was probably local, with office visits from human experts to troubleshoot techy problems in person. This emphasis on geographical convenience was often a clincher when it came to building business rapports with IT partners. However, the past three years has seen many of those constraining relationships melt away, as borderless trading and remote working became the norm, and businesses begin to explore which vendor actually suits their requirements best, not simply their location.

A massive consequence of this, however, is that end-user businesses have been swamped with samey messages from countless IT resellers – very few with any real differentiation or distinctiveness. It's this sense of brand uniqueness that will allow certain resellers to stand out from the crowd and shine brighter in a marketplace saturated with dull, generic messaging and branding.

So, with this in mind, it's time for businesses in this space to leverage bold brand awareness like never before.

A strategic approach, not a superficial one

One of the biggest pitfalls when it comes to brand-building is strategic thinking (or rather, the lack of it...) Many resellers looking to enhance their brand can become fixated on simply churning out superficial top-of-funnel awareness ads. This is not content strategy, it's simply content.

For outputs to become the building blocks of brand awareness that resonates – a more laser focused approach is needed. Before resellers produce anything, they must first start with a plan. Asking: what is the business goal? Is it to scale? Is it to take a new solution to market? Is it to appeal to a new audience? Only when resellers have considered their why can they think about the how. This is how a strategic mindset is developed – and ultimately, will prove to be the key to establishing a brand voice capable of cutting through the noise to generate those all-important leads.

Content with intent: A game-changer for resellers

In a market flooded with 40,920 IT resellers across the UK alone, the importance of creating content with a purpose cannot be overstated. The age of simply creating dull, generic blogs is over. Resellers must instead embrace a bespoke approach that resonates with their target audience, offering valuable insights and solutions that address their pain points and business challenges. Calls to action must be strong, and angles must be genuinely intriguing and insightful.

The power of a full-funnel approach

A holistic marketing strategy that encompasses each stage of the buyer's journey is also pivotal for resellers aiming to establish an engaging brand presence that stands out from the crowd. By integrating a full-funnel approach that caters to awareness, consideration, and decision-making - resellers can effectively engage with potential customers at every touchpoint, fostering a deeper connection and driving those all-important conversions at the end point.

The age of data capture and marketing experiments

Today, data is the driving force behind successful marketing and brand building. It's all about collecting the right info. For resellers, this means understanding what their customers want and need. By capturing data smartly, they can build trust and tailor their approach to each client, in more accurate ways than ever before. Trying out new marketing ideas, such as growth experiments, is a particularly powerful way to get key insights they can really work with. These experiments allow resellers to test which marketing and brand awareness approaches work and which ones fail, so they can keep on improving and tweaking their brand messaging and presence, for it to land perfectly with the right audience, at the right time. By tapping into the world of data and marketing experiments, resellers have a golden opportunity to really get to know their customers and make savvier choices that will ultimately lead to growth and success.

A holistic marketing strategy that encompasses each stage of the buyer's journey is also pivotal for resellers aiming to establish an engaging brand presence that stands out from the crowd

In a nutshell...

So, as the tech vendor space continues to evolve, and more players enter the arena – it's becoming increasingly clear that adopting a bold and strategic approach to brand awareness is undoubtedly one of the main cornerstones of enduring success in the IT reselling sphere.

With the right elements of brand messaging nailed down, IT resellers can quickly begin to carve a unique identity for themselves, fostering stronger connections with their target audience and even establishing themselves as industry leaders.

According to research by Active Profile, one in two resellers are now already focusing on brand building activities in 2023. So, if you haven't already – it's time to start building.

Everything will be connected

Even though 5G networks are expected to grow and develop for years to come, technology strategists are already offering up visions that look far beyond 5G. If their 6G scenarios become reality, we can expect a wonderland of communications in the 2030s.

BY ALEXANDER PABST, VICE PRESIDENT MARKET SEGMENT WIRELESS COMMUNICATIONS AT ROHDE & SCHWARZ

THE LTE STANDARD (4G) meets the needs of most mobile network users. Download speeds of up to several hundred megabits per second make it easy to stream high-resolution video content or download large files within seconds. 5G is available in much of the world but mostly piggybacking on LTE (NSA). Pure 5G standalone (SA) rollout will happen over the next years, yet research into the next generation of mobile communications has already started; 6G is expected to be rolled out by 2030.

But are any needs left unsatisfied by the technically advanced 5G system, which is subject to ongoing development and extension? A pair of authors posed this very question back in September 2018 [1]. What started as a discussion among experts has since gained serious momentum. Political and industrial interest in 6G has triggered a global technological race with billions flowing into research and development.

What needs can 6G meet?

"6G will satisfy the expectations that 5G has created," was how Dr. Ivan Ndip from the Fraunhofer Institute for Reliability and Microintegration (IZM) pithily described the situation in an interview in spring 2021. Although 5G has yet to reach its full potential, applications are emerging that require 6G for large-scale implementation. Autonomous driving is one example.

At autonomy level 5, which is still a long way off, vehicles will not be as autonomous as the name suggests. After all, vehicles share roads, traffic lights and other infrastructure with countless other road users. For everything to run smoothly, autonomous vehicles must be connected in three ways: with each other, with roadside facilities and with a traffic control centre. Since many situations are safety-critical, such as emergency braking, high transmission speeds and reliable signal transfer are vital.

SDC AWARDS 2024

SAVE THE DATE 28.11 2024

Leonardo Royal City London

NOMINATIONS OPEN: **26.02**
NOMINATIONS CLOSE: **30.08**
SHORTLIST ANNOUNCEMENT: **27.09**
VOTING OPEN: **30.09**
VOTING CLOSE: **01.11**
CEREMONY: **28.11**

To find out more about nomination or sponsorship, contact us on:

+44 (0)2476 718970

email: awards@sdcawards.com

https://sdcawards.com/home

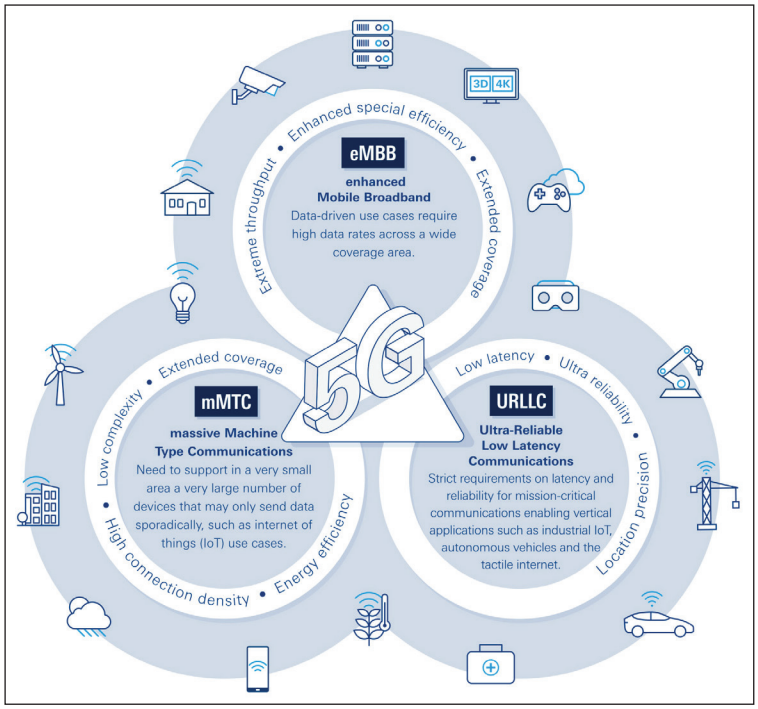


KPI	5G	6G
Peak data rate	20 Gbit/s	1 Tbit/s
Average available data rate	100 Mbit/s	1 Gbit/s
Signal latency	1 ms	0.1 ms
Maximum channel bandwidth	100 MHz	1 GHz
Reliability (error-free data blocks)	99.999 %	99.99999 %
Maximum user density	106/km²	107/km²
Maximum user speed	500 km/h	1000 km/h
Positioning accuracy	20 cm to several meters in 2D	1 cm in 3D

➤ Table 1: Comparison of 5G performance data and KPIs discussed for 6G.

Vehicles require extremely high data rates to exchange sensor data and download detailed traffic plans. 5G is clearly a big step forward, but with a maximum data rate of 20 gigabits per second and signal latency of a millisecond, it is probably not good enough for true autonomous driving. Completely autonomous vehicles will only be possible with 6G, which is to reduce signal latency by a factor of ten and increase data throughput by a factor of fifty (Table 1).

Autonomous driving is a key cutting-edge application that is pushing 6G research. Other important applications are extended reality (XR) and industrial automation. These sectors hinge on the ultra-low latency promised by 6G for instantaneous decision-making and seamless user experiences.



➤ Figure 1: 5G aims to cover three application groups. Enhanced mobile broadband (eMBB) allows classic mobile applications but with much better performance than LTE. Massive machine type communications (mMTC) support energy efficient low-performance applications such as sensor networks. Ultra-reliable, low latency communications (URLLC) focus on real-time applications that require ensured signal transit times and availability.

Focus shifts to machines

In 6G, functions and services for efficient machine-to-machine communications (M2M) will play a vital role.

URLLC and mMTC (see Fig. 1) are two of three key 5G focal points in this area. In addition to autonomous driving, 5G applications include Industry 4.0, smart cities and smart homes. Rather than a single type of M2M communication, many different types are needed. Just look at a connected factory where end-to-end signal transit times in the lower millisecond range need to be combined with minimum latency variation and highest reliability. Smart cities or smart homes have completely different requirements. A smart home needs utility meters, sensors and control elements for everyday items such as waste bins or appliances to remotely provide information or automate processes.

These applications only require sporadic radio communications with small amounts of data. The radio network for a smart city must connect hundreds or even thousands of identical end-point devices, many of them battery powered.

Such applications were inconceivable when mobile communications were first developed but now define the 5G concept. The main focus has shifted from people to devices or machines and the internet of things (IoT).

The 6G vision

Technical development is closely aligned with the demands of different industries. The visions for 6G vary widely and merge to form a fascinating landscape. Bringing this landscape to life will require evolution of existing technologies but also capabilities that are mostly not yet available, but which are within reach on the medium term. The interaction between all these technologies will create the sixth mobile communications generation,

but the term fails to describe the true potential of 6G.

Digital twins on the holodeck

Facebook founder Mark Zuckerberg announced the metaverse in autumn 2021 and also changed the company name to Meta. With that he gave once gimmicky VR headsets new market relevance. They are the main tool for implementing Zuckerberg's vision of extended reality. The company has the means, since VR headset manufacturer Oculus is part of the Meta empire.

Reimagining the original idea behind the VR headset is ambitious and visionary. Specialists use the glasses, for example, to project a 3D model of a part to be mounted into the real image – together with information on how to handle the part.

The person wearing the glasses can even interact manually with the holographic projection as if it were real. This includes touching and manipulating the projection. Making such a system available in the millions and affordable for everyone is Zuckerberg's vision and one of the guiding scenarios for 6G.

Extended reality – the combination of real and virtual worlds – encompasses a number of other substantial visions if taken to its logical conclusion. Ultimately, the long-term goal is total immersion into a new world that is experienced as if it were real. This includes elements such as three-dimensional optical resolution capable of fully stimulating human eyesight, an appropriate acoustic environment, instantaneous reaction by all synthetic objects (tactile internet) and finally, a credible representation of all of these things. Some of these objects have to match up with twins in the real world.

The digital twin is an interactive, virtual representation of a real object or machine that can be manipulated from the metaworld. The ability to operate machines from practically anywhere has potentially far-reaching consequences for the work environment and society at large. One potential impact is the revival of rural areas, since people will no longer need to move to urban areas for work.

When thinking about scenarios like this, you simply cannot ignore 6G. VR headsets do not have the processing power required for the immersive artificial world of the metaverse. And if we want the headset to be compact and look like regular glasses, we need external computing power. If this processing power comes from the cloud, 6G is absolutely necessary.

Transferring extremely large quantities of data to the glasses with video resolutions of at least 8K in stereo requires transport capacities of several hundred gigabits per second along with signal transit times of a tenth of a millisecond to enable natural reactions in real time. 5G does not have the capacity for this. Networks will also need to allocate computing power intelligently for the various 6G services, and this is where artificial intelligence comes in. In fact, AI will be ubiquitous in 6G networks.

Although the internet of things is slowly taking shape and industrial and transportation applications have received a boost from 5G, universal connectivity is only possible with 6G

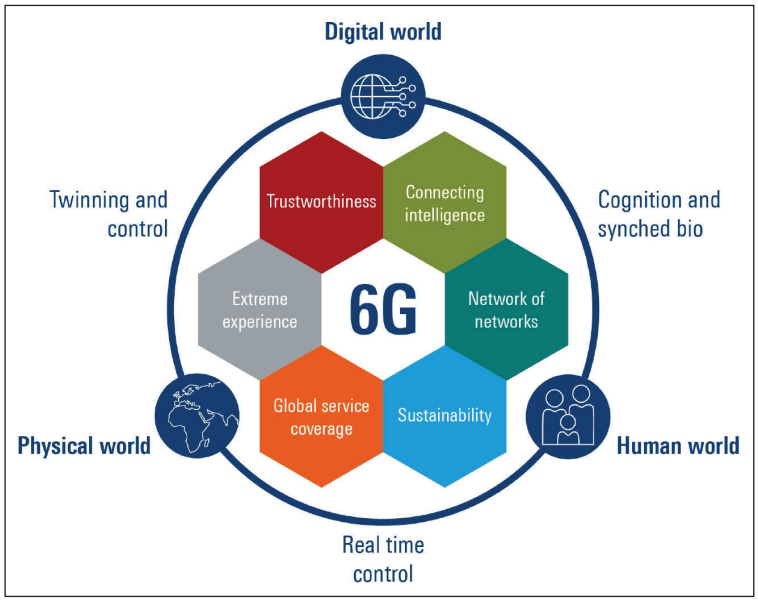
The real internet of things

Although the internet of things is slowly taking shape and industrial and transportation applications have received a boost from 5G, universal connectivity is only possible with 6G. Based on its technical configuration as well as its capacity, 6G should be capable of integrating any number of objects in homes, industries, road transport or infrastructure. This opens up networking opportunities that were never possible before.

Embedded radio sensors can help monitor the condition of bridges and highways, making it easy to see when maintenance is needed. The RFID tags commonly used in retail sales and logistics can only be read from a short distance. Equipped with special sensors and a larger range, however, they could be used to monitor food quality.

The IoT boost will also change how connected radio sensors are powered, which presents a

➤ Figure 2: Augmented reality glasses are already merging real and virtual worlds, but the vision with 6G is to include all senses for total immersion.



➤ Figure 3: 6G is set to meld the physical world (environment, machines), the digital world (data, virtual environments) and the human world in a symbiotic way, as shown here in the vison presented by the European Hex-X initiative.

huge challenge for their large-scale deployment. The sheer quantity of these sensors as well as the degree of miniaturization makes it unfeasible to exchange the power cells. Since many applications are conceived for long-term deployment over many years, the sensors must be able to provide their own power. Zero energy devices and energy harvesting are two buzzwords here. T

oday's RFID sensors work with electromagnetic energy harvested directly from a nearby reader or scanner. But 6G sensors will have to make do without this convenience and obtain power from suitable local sources such as heat, light or motion. As with many other 6G topics, research in this area is still in its infancy.

A network of radio networks

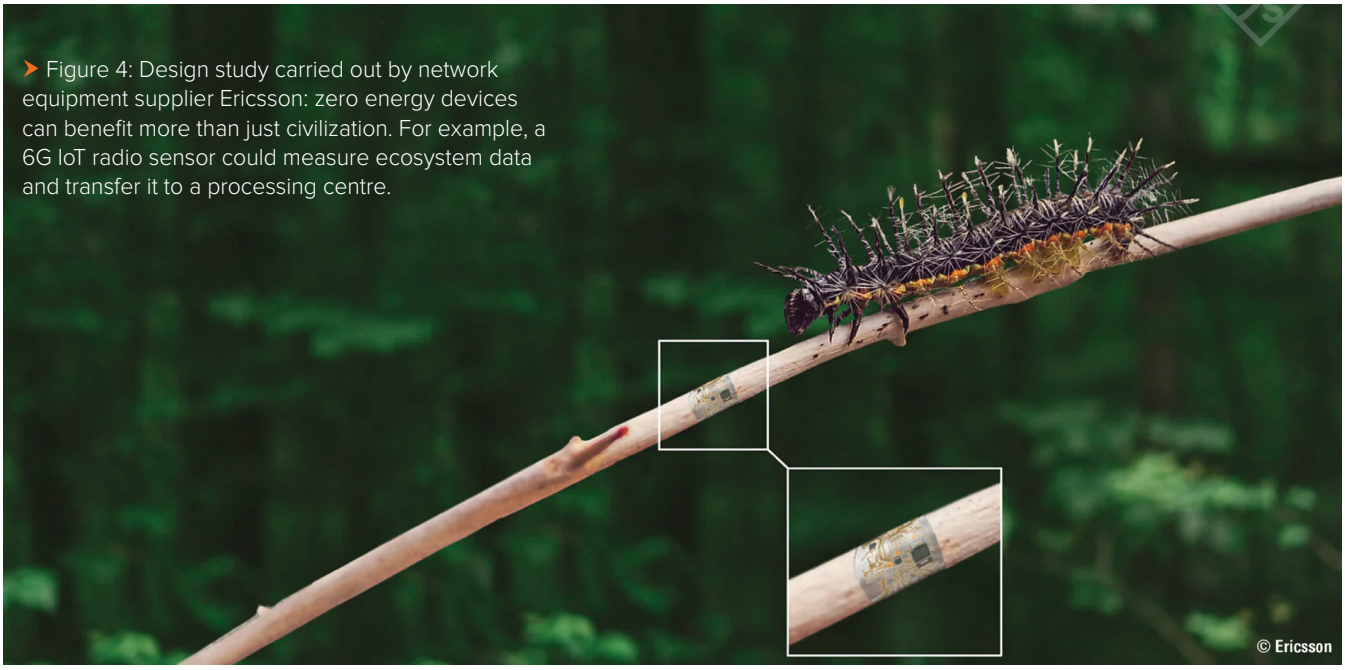
6G will be not only an inexhaustible basis for the internet of things, but also a new kind of internet. With 6G, fixed, mobile terrestrial and non-terrestrial networks will integrate seamlessly into a constantly changing heterogeneous network landscape (organic network). Commercial, private and public subnetworks of all sizes will coexist, ranging from the macrocells that exist today and provide coverage over an entire square kilometre – to attocells and zeptocells with coverage for a single room or vehicle. Openness, virtualization and disaggregation are required to tailor network functionality to the customer application and to spark innovation of new services The disaggregated network's function blocks must provide multivendor support in compliance with the standard. Rohde & Schwarz is an active member of the O-RAN alliance, which is already laying the foundations for this.

The race is underway

Initial discussions of 6G only began a few years ago, but since then a lot has happened in industry, research institutes and the political world.

Research initiatives have been set up around the world, financial support has been granted and alliances have been forged. Politicians understand that competitiveness – and the economic prosperity of their countries – may rest on equal participation in the 6G system while avoiding dependency.

In the spring of 2021, Japan and the USA agreed to invest 4.5 billion dollars in 6G research. South Korea has an ambitious plan to invest some 195 million dollars over the next four years and will be ready for preliminary field tests by 2026.



➤ Figure 4: Design study carried out by network equipment supplier Ericsson: zero energy devices can benefit more than just civilization. For example, a 6G IoT radio sensor could measure ecosystem data and transfer it to a processing centre.

6G RESEARCH AREAS

There is a need for further research and development in the following areas:

FREQUENCIES: 5G is using the millimetre wave range (> 20 GHz) for individual communications for the first time. FR2 (7.125-24 GHz) is the most promising frequency for mass 6G rollout. But 6G will also use higher frequencies: up to 100 GHz and higher for sensing and 90-170 GHz for backhaul. Even the terahertz range (300 GHz to 3 THz) is being explored.

ANTENNAS: at such high frequencies which correspond to short wavelengths, the antennas have dimensions in the millimetre range. Base stations will combine up to 60,000 of these antennas into arrays to supply simultaneous coverage for hundreds of mobile devices via individual directional beams. Reconfigurable intelligent surfaces (RIS) are being developed today. They could be deployed on building walls, for example, to improve the performance of wireless communications in terms of coverage and efficiency.

ARTIFICIAL INTELLIGENCE (AI): AI will be a major hallmark of 6G. It bears the potential to dynamically adjust the network to cope with varying environment and customer demand. AI will be used in technical components as well as in network planning and monitoring. The ultimate goal is to achieve a zero-touch (self-optimizing) network in terms of cost, energy, spectral and operational efficiency.

VIRTUALIZATION: all of the main network components should be defined and addressable via standardized abstract functions. This ensures that products from different manufacturers can be combined while leaving room for specific technical configurations.

SELF-POWERED SENSORS: quantity wise, myriads of miniature sensors will form the largest share of the internet of things. They will need to operate maintenance-free for prolonged periods of time while obtaining power through energy harvesting.

INTEGRATED RADIO, SENSOR AND COMPUTER NETWORK: 6G will be much more than just a radio network. Integrated location and sensing functions will allow the position of network users to be pinpointed down to the centimeter while checking his vital functions. The network's processing power will also be massively distributed and harnessed either close to the network user or in remote data centres depending on requirements (edge, fog and cloud computing).

DATA INTEGRITY: 6G networks will form the backbone of business and industry – even more than 5G. Countless business processes and services will be based on these networks. Data security is therefore critical. Users must be correctly authenticated with absolute reliability. Every connection will require encryption. Block chain technology is being considered as a way to avoid dependence on central instances in order to ensure data integrity.

ENERGY EFFICIENCY: energy demands inevitably also rise when data communications grow exponentially. The energy consumed per bit transmitted needs to fall in order to keep energy efficiency in check.

Europe has launched its flagship 6G project, Hexa-X, with organizations from nine different countries. Rohde & Schwarz is actively working with relevant research organizations worldwide. Separately, the German Federal Ministry of Education and Research is providing 700 million euros in funding until 2025.

In the short term, 250 million euros will go to four national research hubs where Rohde & Schwarz is involved as a partner or project coordinator.

And then there is China. Of course, China has no intention of giving up its strong 5G position simply because the next generation of technology has arrived. China's Ministry of Science and Technology is working with other ministries and government agencies to coordinate national resources and get 6G ready for deployment as quickly as possible.

Rohde & Schwarz has been a close partner to industry as well as a leading supplier of T&M equipment since the very beginning of the digital mobile communications era. The company's products and expertise are already in use today in various 6G research and development projects, and the company is committed to also provide the measuring equipment needed for 6G large scale rollout.

FURTHER READING / REFERENCE

[1] David, K., Berndt, H.: 6G vision and requirements: Is there any need for beyond 5G? IEEE Vehicular Technology Magazine, Vol. 13, Issue 3, Sept. 2018.

How the Channel can harness the power of AI

It's important to remember that, for now at least, while AI is capable of quickly identifying and automating some actions that need to be taken it's imperative that humans are the ones making critical decisions on where and when to act.

BY GUY MARCH, SENIOR DIRECTOR OF EMEA CHANNELS, TENABLE

YOU DON'T HAVE to spend much time researching Artificial Intelligence (AI) before tripping over messaging around how various products have been revolutionised with the technology. There is excitement for the opportunities it could deliver in healthcare treatments and medical advancements. The possibilities for our transport networks and the vehicles that use them. The thought of visiting the Metaverse. The list really does go on. However, there is also concern about the dangers it presents. Not least within cyber criminality as bad people use it to do bad things.

So what is the AI reality?

The Power of AI

Historically Artificial Intelligence (AI) was used primarily to analyse data. Machine learning, an application of AI, uses mathematical models of data to help a computer learn without direct instruction. Deep Learning, part of a broader family of machine learning methods, structures algorithms in layers to create an "artificial neural network" that can learn and make intelligent decisions on its own. Today, with Generative AI — a subset of AI, it is possible to learn about artefacts from data but take this further to generate innovative new creations that are similar to, but don't repeat, the original.

Harnessing the power and speed of Generative AI, such as Google Virtex AI, OpenAI GPT-4, LangChain and many others, it is possible to return new intelligent information in minutes. This can be used to accelerate research and development cycles in fields ranging from medicine to product development and of course cybersecurity. Generative AI is going to change the way humans interact with software, computing devices and the cloud.

Speaking specifically from a cyber perspective, the biggest impact it will have is enabling security professionals to better interact with security data. Most vendors are investing significant resources into leveraging AI to solve foundational security problems. Harnessing the power of AI potentially enables security teams to work faster, search faster, analyse faster and ultimately make decisions faster. That said, Generative AI depends on a breadth and quality of data to provide clear and accurate insights. If you have unique data then you're going to have unique intelligence guiding decisions. It's truly "garbage in, garbage out" — or "gold in, gold out" — depending on the source. MSSPs are perfectly positioned to help their customers by feeding reliable intelligence into their data sets, drawing from a mix of multiple point solutions to aggregate this information and deliver strategic actions that will reduce cyber risks.

Making sense of it all can be daunting. Customers are looking to their channel partners to decipher the polished marketing to really understand what exactly is being offered. They want strong counsel to understand what the solution is capable of, what they need it for, and what is unnecessary expense.

AI turned rogue

While created as a tool for good, AI can just as easily be weaponized by malicious cyber attackers to accelerate their money making schemes or even create misinformation. There are a number of examples and methods by which generative AI can be leveraged maliciously. Generative AI, simply put, is a method by which a model builds relationships between words and when interacted with can predict what a response should be based on these relationships. It learns about artefacts from data and generates innovative new creations that are similar to, but don't repeat, the original.

We're already seeing bad people test the bounds of what's possible, with AI used to create deep fake videos. Attackers are also harnessing the power of Generative AI to accelerate their capacity to "create" malicious emails, malware, and more. Now, instead of creating these malicious communications or software themselves, which is time consuming, they are using the speed and intelligence of Generative AI to write the malicious code and communications on their behalf. This means they can operate their illicit activity to launch attacks quickly.

When you look at code, from a generative AI perspective, it's just words. Looking at how that code has been exploited in the past and using that to find new zero day vulnerabilities in other code sets becomes much easier. We have seen one example where a security researcher was able to get a bot running in the snapchat application to write in basic code that is similar to how ransomware locks a system down. We have also seen examples of phishing attacks becoming much more sophisticated and being able to easily evade the algorithms of anti-spam software.

Whilst AI can be used to automate more targeted and convincing attacks, the flaws these attacks target haven't changed. That means the foundation to defending against any style of attack, be it AI or human powered, remains unchanged. What has changed is the rate at which the cat and mouse game is played. Attackers are going to be much more efficient in many aspects.

The good news is that generative AI can also be a supercharger for cyber defenders.

AI harnessed by the good guys

Security teams have long struggled to address the challenge of prevention in the face of evolving attack techniques. With attackers constantly finding new ways to breach organisations, security teams struggle to keep up.

Attackers see many ways in and multiple paths through technology environments to do damage to organisations. Even with broad visibility of the attack surface, it is difficult for security teams to conduct analysis, interpret the findings and identify what steps to take to reduce risk as quickly as possible.

As a result, security teams are constantly in react mode, delivering maximum effort but often a step behind the attackers.

A commissioned study of 100 U.K. based cybersecurity and IT leaders, conducted in 2023 by Forrester Consulting on behalf of Tenable, found that the average organisation was able to prevent 52% of the cyberattacks they encountered in the last two years. However, having only this much coverage left them vulnerable to 48% of the attacks faced, with security teams forced to focus time and efforts reactively mitigating rather than preventing attacks. Looking at what's holding the teams back from switching focus, it was evident that time is not on their side. Six in 10 respondents (60%) say the cybersecurity team is too busy fighting critical incidents to take a preventive approach to reducing their organisation's exposure. A different approach is needed.

AI has the potential to do just that. It can be used by cybersecurity professionals to search for patterns, how they explain what they're finding in the simplest language possible, and how they decide what actions to take to reduce cyber risk.

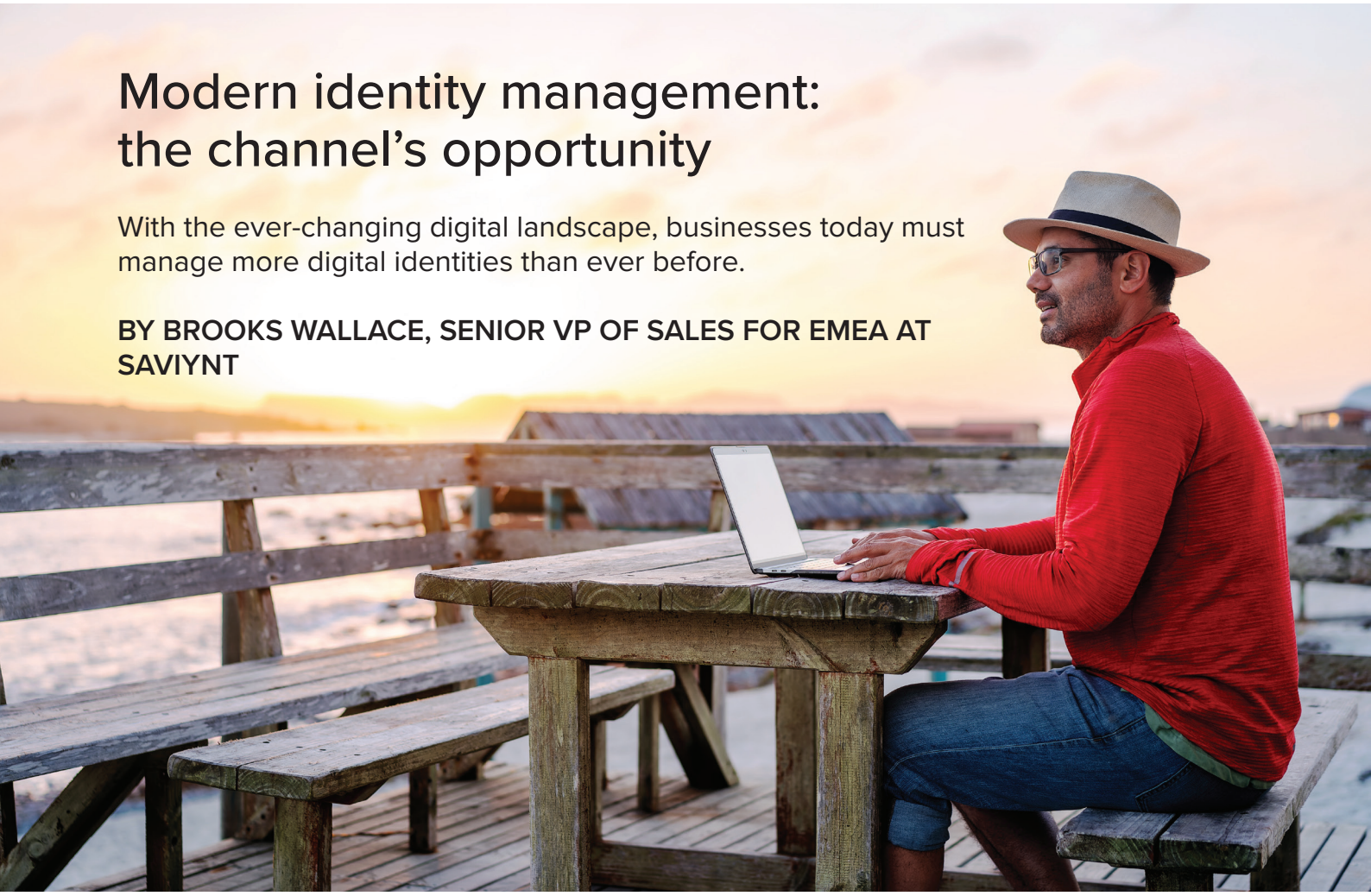
AI can and is being harnessed by defenders to power preventive security solutions that cut through complexity to provide the concise guidance defenders need to stay ahead of attackers and prevent successful attacks. Harnessing the power of AI enables security teams to work faster, search faster, analyse faster and ultimately make decisions faster.

For MSSPs, generative AI is the same as any other new technology that enters the arena. There is a learning curve but, as defenders, we must take time to understand our data infrastructure to determine where the greatest risks lie and then take steps to reduce that risk. It's important to remember that, for now at least, while AI is capable of quickly identifying and automating some actions that need to be taken it's imperative that humans are the ones making critical decisions on where and when to act.

Modern identity management: the channel's opportunity

With the ever-changing digital landscape, businesses today must manage more digital identities than ever before.

BY BROOKS WALLACE, SENIOR VP OF SALES FOR EMEA AT SAVIYNT



FOR EXAMPLE, employees often have multiple digital identity profiles across tens if not hundreds of different applications, while third parties – such as consultants, supply chain partners and clients – may also need access to a company's infrastructure. The growing use of IoT devices means that machine identities are also part of this environment so require proper management and protection. Furthermore, the increased reliance on cloud-based services and the prevalence of hybrid working have only added to the surge in the number of identities.

Managing this proliferation of digital profiles can be complex, yet it is essential to set and enforce policies around who and what can access infrastructure. Otherwise, companies could find themselves exposed to both security and compliance risks. Many businesses are aware of this challenge and recognise that they need to modernise their identity strategies. However, they also acknowledge they need help from trusted advisors in order to select, deploy and then manage the right platform for their organisations.

While the channel has a proven track record of supporting cyber deployments and providing expert guidance for selecting and implementing the best technologies for their customers, identity management solutions have not always received the same priority as more headline-grabbing solutions, such as Enterprise Detection and Response (EDR) or Incident Detection and Response (IDR). For channel organisations, identity management represents a further opportunity to offer even more value to their customers.

Migrating from legacy tools

Traditionally, organisations have relied on point solutions to manage which employees, partners and machines can access the different applications and network resources. However, there are drawbacks to this approach. All these piecemeal solutions add complexity to management, require integration, and increase costs. Additionally, this approach creates silos, making it difficult to monitor all types of identities – whether human or artificial, located on-premises or in the cloud – in a holistic way.

Indeed, organisations still relying on various, specialised tools may find it difficult to monitor certain groups of users or applications, as some of these tools are only compatible with certain cloud environments or on-premises setups. In these scenarios, administrators are often required to switch between multiple management consoles, gather data from different sources, and create their

It is the who, what, where, when, how, and why of technology access, and is designed to protect personal and corporate data from theft by using 'identity' and 'access' to govern how users interact with data and applications across an organisation's systems and networks

own reports in order to get a complete picture of their systems. In some extreme cases, they might not even manage access for certain types of users, applications or locations, creating both governance and security risks.

The next generation of identity management platforms

Identity and Access Management (IAM) should form the foundation of any modern identity security strategy. In short, it is the who, what, where, when, how, and why of technology access, and is designed to protect personal and corporate data from theft by using 'identity' and 'access' to govern how users interact with data and applications across an organisation's systems and networks. On top of IAM, there are several other solutions that provide more fine-combed visibility, control, and auditing over access rights.

One of these is Privileged Access Management (PAM), which consists of a set of policies, processes, and technologies to secure privileged accounts and monitor their actions which establish control over the elevated privileges of identities on a network. By temporarily elevating privileges for a user just in time with just enough admin to perform critical job functions, PAM helps organisations reduce their digital attack surface, mitigate insider threats, and identify and close any security gaps created by negligence.

There are also Identity and Governance Administration (IGA) tools, which enable enterprises to set and enforce policies about identity and access, which can be applied across the entire enterprise. Features include Identity Governance – encompassing segregation of duties, role management, attestation, analytics, and reporting – and Identity Administration, which deals with account administration, credentials administration, user and device provisioning, and managing entitlements.The crucial difference between these latest solutions and more traditional point solutions is that they can be managed centrally from one cloud-based platform, making it easier for administrators to identify and mitigate risks, as well as streamline the way identities are managed. This platform-based approach also fuels rapid innovation.

Innovation in managing identities

Some of the latest advancements to help organisations strengthen their ability to detect, respond to, and recover from identity-related security incidents, ultimately reducing risks and enhancing overall cybersecurity posture, include:

- **Predictive analytics;** this involves the use of data analysis and predictive modelling techniques to anticipate and manage user identity-related events, behaviours, and risks within an organisation's information systems. It leverages historical and real-time data to make informed predictions about user behaviour, access patterns, and potential security threats. This proactive approach helps organisations enhance their security posture, streamline access management, and improve overall operational efficiency.
- Identity Detection and Response (IDR), which focuses on the proactive detection and rapid response to identity-related threats and incidents within an organisation's digital environment. Similar to predictive analytics, it monitors and analyses user behaviours, access patterns, and other identity-related activities to identify suspicious or unauthorised activities that could indicate a security breach or compromise.
- Centralised and automated approach in identity management refers to the practice of managing user identities, access privileges, and authentication processes in a consolidated and automated manner. It involves maintaining a repository of user information, adopting a single sign-on approach, automating the process of provisioning and deprovisioning, implementing role-based access control, enforcing policies, providing self-service portals, authenticating and authorising users, conducting audits and generating reports, and integrating with other IT systems.

The rise of digital operations has made managing IT security ecosystems challenging. The result is that employees and other users (human and machine) have excessive and/or redundant access to different systems, applications, and data. This is the access they do not require to do their jobs, so represents both a risk to security and compliance.

The channel has a critical role to play in guiding organisations through the selection, customisation, deployment and integration of a centralised identity management platform that fits their exact infrastructure requirements.

Furthermore, partners also have the opportunity to oversee these platforms on an ongoing basis, as a managed service. Not only could this help partner organisations develop new recurring revenue streams, but it will also strengthen their relationships with their customers, helping them to deliver even more of a value-add.

How MSSPs can cost effectively tackle ransomware

Ransomware is now regarded as a top threat, with the commercialisation of these attacks via Ransomware-as-a-Service and nation state sponsored attacks seeing threat actors refine their attack capabilities.

BY MATTHEW RHODES, REGIONAL DIRECTOR FOR MSSPS AT LOGPOINT

FOLLOWING a brief hiatus earlier in 2023, attacks are now on the rise again, with the Mid-Year Cyber Threat Report recording almost 90million attacks during Q2 2023, up 74% compared to the first quarter.

It turns out the ransomware window ie the time from compromise to the deployment of ransomware and encryption of data has shrunk. It now stands at 4.5 days compared to 5 days in 2021. Meanwhile, attacker dwell time on networks has halved from 22 days to just 11. So, attackers are getting in, obtaining the data they want, and getting out much faster.

There's also been a significant shift in ransomware practices. Rather than encrypting the data in exchange for a ransom, many operators are now stealing data and threatening to leak it, leading to a rise in extortion-based attacks. Reports suggest that non-encryption ransomware attacks were up 25% between April and June of this year and the attack against the MOVEit file sharing protocol by the Clop group is a perfect example of how devastating these can be.

Struggling to keep up

Defences, however, are not keeping pace. According to the MSSP Automation and Integration report, 65% of businesses saying SOC operations are losing time due to inefficient processes, 57% saying the Mean Time to Detect (MTTD) and MTTR are below goals, and 35% saying they do not have the best process or tools for building detection patterns. This presents MSSPs with a clear opportunity, with many organisations now turning to the channel to provide access to the latest technology to counter the ransomware threat.

The faster infiltration we're seeing with ransomware attacks requires faster detection and defence, which is why it's imperative that monitoring covers the entire information estate, from email to endpoints. Endpoint Detection and Response (EDR) is a tool that can help here as it continuously monitors all endpoint devices for threats that may get past traditional defence mechanisms such as anti-virus, anti-malware and firewalls. Analysis is carried out in real-time and incident response is carried out automatically to speedily mitigate threats and minimise the impact of an attack. EDR can therefore dramatically improve detection, reduce dwell time and increase Mean Time to Response (MTTR).

Yet many businesses cannot afford to invest in EDR, lack the expertise or resource to manage it. This makes it a prime technology for MSSPs to consider, with many looking to add it to their portfolio over the next 12-24 months, according to the report. The difficulty lies in being able to integrate such technologies with their current offerings. MSSPs

don't want to have to bolt together different technologies and dedicate the manpower to managing and customising these, all of which leads to higher overhead costs.

Integrating EDR

Monitoring end user devices, networks, applications, and firewalls is complex and even more so when using point solutions which have different ways of working. Over time, the addition of numerous technologies to the security stack has inevitably lead to siloed operations. Those overseeing these technologies then have to resort to swivel chair monitoring, logging into and reviewing alerts across numerous user interfaces. As these standalone technologies are not integrated, bringing together this information then requires the manual correlation of events and alerts.

A lack of interoperability can often be the reason a customer chooses to outsource to an MSSP due to the complexity involved but it can equally be an issue for the MSSP too. Increasingly, MSSPs are looking at how they can simplify the stack and this is now front of mind when it comes to investing in new technologies. So, when it comes to developing a ransomware-ready solution, MSSPs pre-integrated technologies and one example of this is virtual EDR integrated within the Security Incident and Event Management (SIEM).

A converged SIEM (sometimes referred to as a next generation SIEM) extends the traditional functionality of the SIEM by incorporating additional, complementary tool sets. Adding in EDR, for instance, sees log source analysis also incorporate EDR monitoring so that issues can be captured even earlier. Using agents deployed on the endpoints, data is fed back to the SIEM rather than a separate EDR server so that the EDR operates as another log source. This then means there is no need to extrapolate the threat data to explore the potential impact of a threat. Because this data is compared against the tactics, techniques and procedures (TTPs) outlined in the MITRE ATT&CK framework, this provides a more comprehensive form of monitoring across the network and its endpoints, reducing MTTD and MTTR.

The convverged SIEM can also integrate other threat hunting technologies such as Security Orchestration Automation and Response (SOAR) and User Entity and Behaviour Analytics (UEBA). SOAR brings together data from disparate sources and then uses automation to ingest and analyse alerts. It can prioritise threats, make recommendations and carry out automated actions including automated response through the use of pre-built and customised playbooks. Post-incident, it can also provide automated case management and reporting.

UEBA works by building baseline parameters of 'normal' behaviours that are tailored to each individual user. When behaviours then stray outside of these parameters, these are automatically flagged to security analysts for their review. So in the case of a ransomware attack, the exfiltration of data via a particular endpoint which went against that user's usual work pattern would trigger an alert.

A combined effort

But integration doesn't just reduce complexity, it also paves the way for the MSSP to take a less reactive and more proactive stance. Rather than being alert and event driven, the MSSP can offer more proactive services such as threat hunting and emerging threat detection. This is because assimilating these tools together enables far more effective endpoint interrogation and faster threat detection and incident response (TDIR).

A lack of interoperability can often be the reason a customer chooses to outsource to an MSSP due to the complexity involved but it can equally be an issue for the MSSP too. Increasingly, MSSPs are looking at how they can simplify the stack and this is now front of mind when it comes to investing in new technologies

The event logs and flat files capture behaviour from systems and applications hosted on servers enabling forensic investigations and threat hunting to be carried out by the IR team. This means that, in the event of an attack, the logs can be used to determine how the attack gained access and moved across the network during the investigation.

As those endpoint logs and telemetry are being fed into the SIEM they can be enriched using contextual information from the MITRE ATT&CK framework to see which tactics, techniques and procedures were used. They can also be configured with compliance standards to save time and resources during audits. MSSPs can and should be looking to extend their capabilities to address the ransomware threat but what they don't want to end up with is a bloated resource-hungry stack. They need to expand their offerings but also need to reduce complexity so at some point have to adopt a convergent approach and combine functionality.

Convergence of complementary technologies promises to greatly emancipate MSSPs as they'll no longer be as restricted when it comes to choosing which technologies to offer. Combining multiple threat hunting solutions over a single platform, for instance, ensures the MSSP remains competitive while gaining from much better network visibility, control and lower maintenance demands by using one solution - benefits they can then pass on to their customers.

MLOps and LLMOps – How do they differ?

With the rise in Big Data, followed by the Artificial Intelligence renaissance, many organisations have started considering how to leverage large amounts of data effectively, seamlessly and efficiently. That is how MLOps emerged. However, recently we observed an outbreak of a new technology, called Large Language Models (LLM). In principle LLM are models, so the question is how can we ensure high standards of the LLM solutions using already known methods?

BY ALEKSANDRA SIDOROWICZ, MACHINE LEARNING ENGINEER AT FUTURE PROCESSING

Introducing MLOps & LLMOps

MLOps is the intersection of processes, people and platforms that enable businesses to gain stable value from machine learning. It streamlines development and deployment via monitoring, validation and governance of machine learning models.

By adopting an MLOps approach, data scientists and machine learning engineers can collaborate and increase the speed of model development and production, encompassing experimentation and continuous improvement throughout the machine learning lifecycle.

LLM (Large Language Model) is a type of machine learning model that can perform a variety of tasks, where instructions are given in natural language rather than a code. As they can be used to seamlessly generate images and text, LLMs are an exciting development in the technology sector.

LLMOps encompasses the practices, techniques and tools used for the operational management of large language models in production environments. Like MLOps, LLMOps requires a collaboration of data scientists, DevOps engineers and IT professionals.

Understanding the Differences

In general, the operational requirements of MLOps can be applied to LLMOps, but there are a variety of differences between the two practices which require a unique approach to training and deployment. Therefore, it's important for businesses to consider how machine learning workflows change with LLMs.

Fine-tuning

Whilst most machine learning models are created and trained from scratch, LLM start from a foundation model and are fine-tuned by engineers with new data to improve performance. The reason behind this is partly explained in the name - Large Language Models. These models are neural networks with literally billions of parameters.

That makes training the entire network extremely expensive, hence transfer learning methods are so commonly used. This allows specific applications to become more accurate using less data and fewer IT resources. Parameter-Efficient Fine-Tuning (PEFT) is an exemplary group of fine-tuning methods for open source LLMs, while OpenAI provides an API to do this inside their infrastructure.

Human Feedback

LLMs have seen major improvements in recent years as a result of reinforcement learning from human feedback. As LLM tasks are open ended, human feedback from end users is critical in evaluating the application's performance and it allows engineers to make the necessary changes within their LLMOps pipeline.

Performance Metrics

Traditionally, machine learning models have clearly defined performance metrics which are simple to calculate. LLMs, however, use a different set of standard metrics and scoring, such as bilingual evaluation understudy (BLEU) and Recall-Oriented Understudy for Gisting Evaluation (ROGUE). Nonetheless, the choice of the right metric for LLM is more demanding and will depend strongly on the type of task that you want to solve with it.

Chains

The vast majority of LLM applications focus on binding many external systems together with off-the-shelf LLM, rather than building a new LLM from scratch. That is why tools such as LangChain have become so popular. LangChain facilitates the process of building LLM-powered applications with their suite of tools, components and interfaces. An example of such integration can be a Q&A chatbot, backed by an external knowledge base kept in a vector database.

Looking to the future

The key benefits of MLOps and LLMOps are efficiency, scalability and risk reduction. Both principles allow data teams to achieve faster model and pipeline development, deliver higher quality models, and streamline deployment to production. They also enable vast scalability and management, as dozens of models can be overseen, controlled, managed, and monitored for continuous integration, delivery, and deployment. One can inherit most of the principles from MLOps to LLMOps.

However, it is important to be aware of the underlying differences, which are typical for LLM applications but not so common for other machine learning applications. Today they can be quite challenging to tackle, but with the advancement and growing popularity of LLMs, these challenges become more manageable.

As we look ahead, MLOps and LLMops will continue to grow in importance as more organisations consider scaling their AI efforts. Both models will help businesses automate their machine learning life cycles, improve the quality of their processes, and better leverage data to make decisions.

Whilst it is unchartered territory for many companies, leveraging AI at scale will ensure businesses can derive the utmost value from their machine learning investments.

Generative AI: is asking the right question more important than knowing the answer?

AI may have started a revolution, but those that will rise to the top will be those in touch with the most human of traits: creativity, empathy and perhaps above all – the curiosity to ask the right questions and get the right answers.

BY GAURAV DHILLON, CEO OF SNAPLOGIC

COMPUTER SCIENTISTS have been working on AI for a long, long time. The first, albeit extremely primitive, generative AI systems can be dated back to the 1950s and, over the course of the last 70 years or so, developments have been steady and impactful, both for business and personal use. Yet despite this long period of research and development, in the last year alone it seems like the AI revolution has crept up on us, exploding into the fore with the release of new, highly capable large-language models. Now, everyone has the power of a highly accessible and increasingly advanced large-language model at their fingertips.

Whether you want a shopping list or an essay on quantum mechanics, generative AI solutions can instantly churn out an answer built on enormous databases and billions of parameters.

So, should we be worried about our jobs?

Well not exactly. Just like the tractor didn't replace the farmer, and the calculator didn't replace the mathematician, AI won't replace humans, it will just help us complete basic tasks faster, more affordably, and more easily than ever before. Think about that calculator example - most maths tests now let you bring calculators in with you – why? Well, just because you have the tool doesn't necessarily mean you can find the answer. Similarly, just because you have ChatGPT doesn't mean you are able to get precisely what you want out of it. It's now vital that employees know how to make the most out of generative AI so that they can use it to the best of its potential.

The new wave of AI has in many ways spawned a second 'Socratic age' where the Socratic method of asking powerful and insightful questions is the key to unlocking doors and finding the right outcomes.

In the same way a new vital skill for business people will be asking the right questions, or as we are now calling it 'prompt engineering' – constructing text prompts that can be more effectively and efficiently interpreted by Generative AI tools to get exactly the desired outcome. With the right prompt, business users can now translate business intent into technical delivery, in seconds.

So asking the right questions is critical, but as important perhaps, is knowing the limitations of GPT models - as with any developing tech, no one knows how the proliferation of AI will play out in the long run. What we do know is that right now whilst ChatGPT and other tools have created exciting new opportunities, they have simultaneously amplified the need for genuine talent.

Learn how to put AI to work for you

Think of your favourite book or TV show – let's say, just to keep the AI theme going, that it's Star Trek. If you ask a generative AI software to give you a screenplay for an episode of Star Trek it will no doubt give you one, which at first glance might look scarily competent. However, on closer inspection you soon realise that it's likely just an amalgamation of the data points it has available, and thus gives you an episode of wholly uneventful, uninteresting and inhuman dialogue.

There will be no real fun or creativity. AI simply can't replace this humour, emotion and empathy, nor substitute genuine human talent.

AI could however, certainly prompt a scriptwriter with ideas or suggest characters or plot points as a starting point. Knowing how to best use generative AI is almost as valuable as having the tool itself. Think of AI as a teammate, someone who has great knowledge and ideas but also needs a great deal of oversight, training and guidance.

In a business sense this is even more true. There have long been products that can fully automate repetitive, manual tasks, like reporting for the finance department or onboarding apps and data for the IT staff. But the addition of generative AI capabilities to these tools, which can now interpret natural language prompts to instantly and intelligently glue together data and save valuable employee time, doesn't take away from employees, rather it gives them the time and space to be more creative and focus on more skilled problems where human insight is vital.

These generative AI enhancements make complex tasks like building data pipelines and workflows as easy as typing a short prompt - connecting businesses to their data like never before. "Generative Integration" in this way has been described as 'the holy grail of LLM use' as it allows business leaders to join together company databases, apps and teams. As Generative AI and LLM models are built on the datasets underneath them, ensuring data is accessible, transferable and usable by these models is essential to drive digital transformation and stay ahead of the curve.

Are questions the new answers?

As generative AI develops, so too will our understanding of how best to use it. Ultimately, in the not too distant future every employee will be a potential prompt engineer, and as a first step business leaders should look to train their employees to help them make the most out of these tools.

AI has the power to truly transform the future workplace and augment workers' existing skills so they can tackle more complex tasks and ultimately, the impact of Gen AI will be felt most by those whose work lives will be significantly more creative, more engaging and more meaningful when they are free to work on the things that actually matter to them.

Empathetic and understanding business leaders who want to retain and make the best of their employees, must therefore consider the power of AI in adding to jobs rather than simply the fears of taking from them.

So - whilst AI may have started a revolution, those that will rise to the top will be those in touch with the most human of traits: creativity, empathy and perhaps above all – the curiosity to ask the right questions and get the right answers.

Becoming a digital enterprise

Why businesses need to look beyond the 'digital' to succeed in their digital transformation program

BY CHRIS DAPLYN, MANAGING DIRECTOR FOR NORTH-WESTERN EUROPE AT VALTECH

AMONG UK BUSINESS decision-makers, 85% believe digitalisation is more important than ever. However, with 71% saying they are worried that they've failed to deliver on the promise of digital transformation and 72% saying the business has no clear path to reach its digital transformation goals and is moving too slowly to make any meaningful change, there is clear uncertainty on how businesses can meet their digital goals and draw true value from their digital transformation program.

For many businesses, the key to unlocking true potential in their digital transformation journey is through a shift in mindset, looking beyond the digital and focusing on company-wide processes to see long-term results.

With the economic conditions currently so uncertain, transformation programmes rooted in 'should be more digital' rather than the 'must improve the business' are likely to be reduced, paused or broken into disparate projects. When they become too piecemeal and lacking in coordination, that's when digital transformation projects often fail.

Without a 'North Star' goal guiding the way, businesses fail to realise the true business transformation they set out to achieve.

Overcoming these issues requires tapping into the human side of digital transformation, whether that be fostering internal partnerships, breaking down hierarchical structures internally or adopting a process-oriented mindset when looking to evolve a business's digital strategies.

Shifting perceptions and embracing change

A major problem we see when implementing a digital transformation project is an internal resistance to change. It's not uncommon for individuals and departments across a business to want to see change, as long as it doesn't impact them, be that through changing departmental structures or altering internal processes. However, business leaders often entrust a digitalisation project to the IT department.

This is where businesses need to focus on the human side of digital transformation. To ensure a successful digital transformation, business leaders need to encourage a company-wide shift in mindset that views improving a business's digital ability as a path to value across the whole company, rather than a necessary evil. For many, this will mean embedding the objectives into company culture, through transparent communication and cross-department collaboration.

Fostering internal partnerships and removing human siloes

For businesses to become more digitally mature, they will often focus on breaking down siloed tech systems, resulting in a more efficient and flexible tech stack. But for projects to really stick, the same needs to be done with the human siloes that stand in the way of successful collaboration. From the top-down, businesses should strive to implement ways to foster internal partnerships, across departments, ensuring

transformation in embedded across the businesses as a part of a unified mindset and culture for all employees. This change should start from the c-suite working together to agree on goals and a vision for transformation to span the entire company, setting unified measures to track progress and ensure a level of accountability amongst employees.

This mindset will then trickle down into all departments, into the more detailed workstream delivery, ensuring steady progress and removing the 'digital' centric view that has often been at the centre of failed projects.

Customer centricity

When it comes to common mindset, fostering a culture built around customer-centricity can enable a digital transformation program designed around human-to-human experiences. Siloed departmental structures and hierarchical cultures, with minimal support from managers, can act as a hindrance. Breaking down these barriers can involve bringing in new ways of workings, prioritising employee empowerment and setting unified goals: make it clear how customers expectation will be met. Data is certainly needed in this case to provide businesses with the necessary insights to inform the decision-making process and make connections across departments to ensure human-to-human experiences are delivered to a high standard.

Looking long term with measurable leaps

It is also crucial to remember that your digital transformation program is not a one-stop shop, it's an ongoing process. This makes it sound unattractive and a money pit, but it doesn't need to be. If you are guided by a long-term vision but are able to business case and prove out the value of incremental steps, you can deliver short term results for the business while still focussing on the longer-term goal.

Balancing the long-term and short-term requirements of a project is often where business leaders fall short. Especially when it comes to funding. All too often, people focus on short-term budget such as paying for software licences and

infrastructure budgets. Focusing on short-term 'quick fixes', that produce instant results can seem appealing, especially when under pressure from stakeholders across the business. But neglecting to consider the legacy debt you are building or organisation change management costs which will inevitably come further down the line, will risk a project's longevity.

Similarly, when balancing immediate customer expectations and strategic decisions, it is important to ensure activity doesn't fragment or become consumed by short-term, customer led goals, delaying the crucial strategic decisions which can ensure long-term success.

The bottom line? Businesses can get the most out of their digital transformation by looking long term with measurable leaps. Focusing on the internal changes and the human side of a transformation project will allow businesses to drive longevity and ensure real business change. Whilst there needs to be long term vision and strategy, those involved need to see progress and value along the way. Breaking a digital transformation journey down into these 'measurable leaps' can ensure that everyone, across the business, buys into the fact that the transformation is bringing about change and delivering that crucial business value.

Technologists should focus on proactivity, not reactivity, to deliver on Industry 4.0 goals

As we seek to build smarter factories, embrace new business models and streamline operations, manufacturers of all shapes and sizes are seeking to integrate the latest technologies, whether or not they use the term 'Industry 4.0'. A poll by Digital Catapult revealed that investment in deep tech solutions, amidst commitments to innovation, remain a key priority for business leaders in 2023 across the UK manufacturing industries.

BY GREGG OSTROWSKI, CTO ADVISOR, CISCO APPDYNAMICS

BUT AS MANUFACTURERS look to double down on their Industry 4.0 transformation programs over the next 12 months, they cannot afford to overlook the need to monitor and optimise IT performance at all times. As we have seen over recent years (firstly in the consumer market but now also in a business context), customers are simply not willing to tolerate poor digital experiences. And therefore, it's vital for organisations to equip their IT teams with the tools and insights they need to optimise application performance at all times; otherwise they risk being unable to maximise their Industry 4.0 investments. The headaches manufacturing IT departments are caused by data noise from Industry 4.0 programs The move to cloud is widely recognised as critical in supporting and scaling Industry 4.0 strategies.

Modern application architectures, built on technologies such as microservices and Kubernetes, present huge benefits for manufacturers in terms of faster innovation velocity, increased agility and greater reliability and resilience. This explains why

most manufacturers are now deploying multiple cloud environments to support their innovation initiatives.

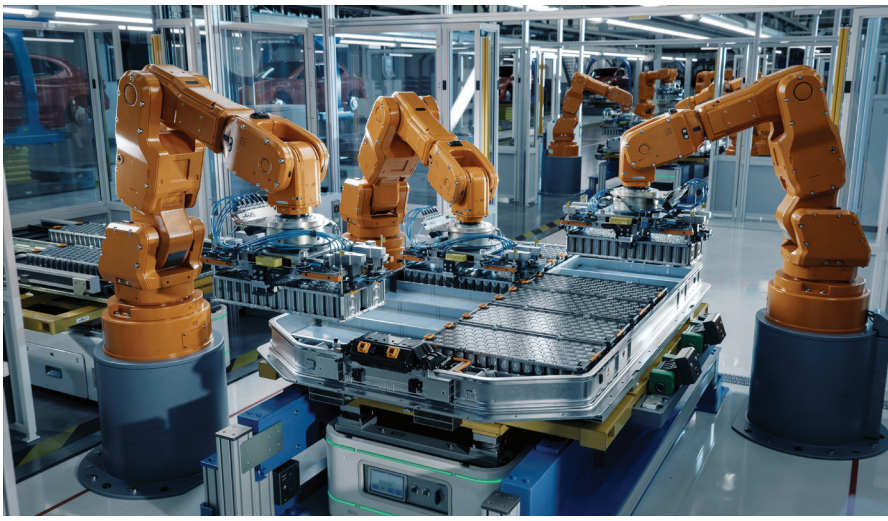
But many organisations are now finding themselves being held back by a lack of visibility across public and hybrid cloud environments. In particular, they're struggling to get visibility into applications and underlying infrastructure for large, managed Kubernetes environments running on public clouds. The distributed and dynamic nature of cloud native applications makes it extremely difficult for technologists to pinpoint the root cause of issues, due to new application behaviors and fault modes and data volumes which far outweigh what humans (and traditional monitoring tools) can handle. Cloud native technologies such as microservices and Kubernetes rely on thousands of containers and spawn a massive volume of metrics, events, logs and traces (MELT) every second.

This explosion of data is now becoming a major headache for IT teams. Most are unable to cut through the overwhelming volumes of data that are coming at them from every corner of their IT estate, and therefore they're constantly scrambling to identify and understand issues before they impact end user experience.

Worryingly, in our latest Agents of Transformation 2022 report, 65% of technologists admitted that they feel overwhelmed by the soaring volumes of data being caused by rapid innovation and spiraling complexity. IT teams are stuck in firefighting mode and the consequences of this are severe - firstly, they're unable to ensure seamless digital experiences for customers, suppliers and employees, which could have profound implications for the business. And secondly, they're unable to spend time on strategic priorities, and in particular the innovation initiatives which are central to their organisation's Industry 4.0 ambitions.

Cloud observability can allow IT teams to remain proactive and keep Industry 4.0 programs on track Without doubt, monitoring performance is far more challenging in a software-defined, cloud environment, where everything is constantly changing in real-time. Traditional approaches to monitoring are based on physical infrastructure – IT departments operate a fixed number of servers and network wires - they are dealing with constants. This then provides fixed dashboards for each layer of the IT stack. But with cloud computing, organisations are continually scaling up and down their use of IT, based on real-time business needs.

Most monitoring solutions simply aren't able to handle dynamic and highly volatile cloud native environments. Technologists are unable to cut through the crippling data noise when troubleshooting application performance problems caused by infrastructure-related issues that span across hybrid cloud environments. Nor do they



have unified visibility across what is increasingly a sprawling and fragmented IT estate.

In order to get back on the front foot and adopt a more proactive approach to managing application performance, manufacturers need to implement a modern, cloud native observability solution which allows their IT teams to manage and optimise increasingly complex and dynamic applications and technology stacks, and enables them to monitor the health of key business transactions distributed across their entire technology landscape.

With real-time insights from the business transaction's telemetry data, technologists can quickly identify the root cause of issues and expedite resolution, ensuring that their applications are consistently performing at an optimal level, without any disruption or downtime. And critically, particularly given that technology investment is likely to come under closer scrutiny as the economic slowdown continues, this level of insight into business transactions will allow business and IT leaders to measure and report on the performance and ROI of their Industry 4.0 initiatives on an ongoing basis.

This explosion of data is now becoming a major headache for IT teams. Most are unable to cut through the overwhelming volumes of data that are coming at them from every corner of their IT estate, and therefore they're constantly scrambling to identify and understand issues before they impact end user experience

Harnessing IT to power AI and GPT

Today, it appears IT leaders cannot open a web browser without learning how artificial intelligence (AI) and generative pre-trained transformer (GPT) technologies can save businesses time, resources, and money. Unfortunately, they might also come across stories about how enterprises have endured a disaster due to AI and GPT being applied in the wrong use case and with bad data.

BY AJOY KUMAR, CLOUD ARCHITECT AT BMC

ACCORDING to a recent Gartner webinar poll of more than 2,500 executives, 38 percent indicated that customer experience and retention is the primary purpose of their generative AI investments. This was followed by revenue growth (26 percent), cost optimisation (17 percent), and business continuity (7 percent). In addition, Forrester has warned that if generative AI makes things easier, it also makes doing bad things easier.

Many enterprise IT teams are now trying to decipher how to best take advantage of these technologies' without risk. One key attraction with sophisticated technology, is its promise to automate processes and reduce the work of gathering and correlating data across industries. For example, AI and GPT could lessen the time it takes IT to find and solve problems and communicate results in an undeniably human, conversational manner that will resonate with end users and customers. This is one of the many use cases for GPT in today's sophisticated IT environments.

Automation is key

AI and GPT rely on the consumption of large volumes of data in an environment, as well as the ability to quickly correlate real-time events and alerts with known incidents and their respective fixes. These technologies can be used as embedded capabilities in experience and service monitoring tools, enabling IT teams to speed problem identification and resolution.

Essentially, AI and GPT technologies can quiet the noise of multiple events and alerts, while providing valuable insights to IT teams faster than humanly possible. The number of alerts generated from numerous monitoring tools has long been an issue

Search is a useful tool, especially when delivering answers directly related to the search query. With AI and GPT embedded in search technologies, service managers and IT operators can place more trust in knowing the search results will apply to the issue at hand

when managing sophisticated IT environments. However, with GPT, IT teams have the tools to determine which alerts represent a critical incident and which can be disregarded as noise.

Identifying problems and intelligently resolving Many IT environments have various monitoring tools that generate alerts when an incident occurs. However, when you factor in service tickets generated from end users, the task of relating the events to the service request can rapidly become overwhelming for IT teams. IT operators attempting to understand how to resolve problems and close the service tickets will benefit significantly from GPT technologies that can generate problem resolution.

AI and GPT can provide considered, plain-language summaries of how issues have been resolved in the past and how that knowledge can be applied in the current situation. For example, GPT can generate root-cause reports by deciphering a cluster of related tickets and distilling key resolutions from this. This eliminates wasted time for IT and speeds service availability for end users and customers.

Searching seamlessly

Search is a useful tool, especially when delivering answers directly related to the search query. With AI and GPT embedded in search technologies, service managers and IT operators can place more trust in knowing the search results will apply to the issue at hand. GPT can power service desk agents and end users in their quest for adequate, applicable answers with their company's digital workplace. AI and GPT tools will deliver the best and most likely answer quickly, which speeds time to resolution for IT and employees alike.

Virtual agents get smarter

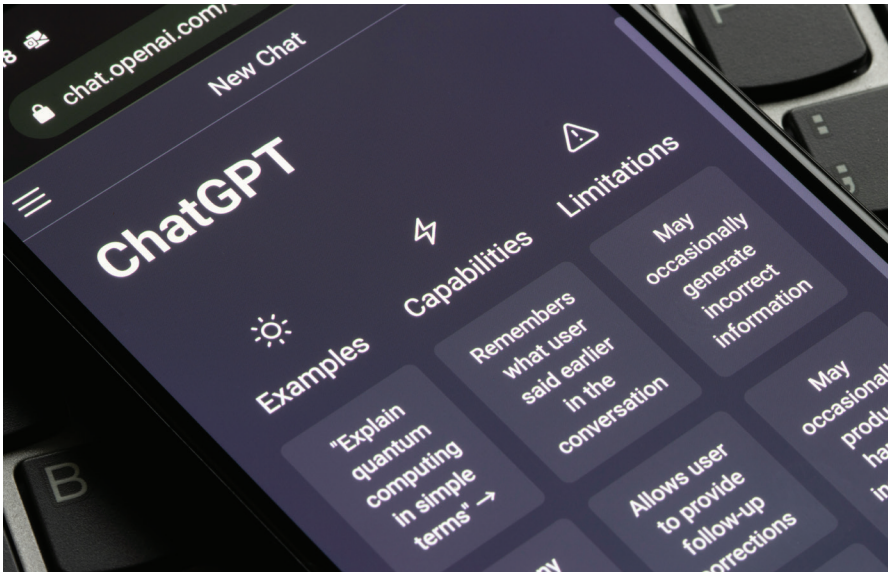
Because of its natural language processing, GPT can enable virtual chat agents to communicate more humanly than ever before. Using its access to volumes of enterprise data, GPT can search and find the quickest, best response for any query. On top of that, it can relay the information in plain language that is easy to understand and implement. Again, the power to speed issue resolution will provide infinite benefits to an enterprise company by easing the load on IT teams. This enables end users to help themselves, and gives customers access to the best information and smartest tools to answer their questions.

Changing risk prevention with DevOps

Organisations embracing development operations (DevOps) likely live by the "fail fast, fail often, recovery quickly" mantra when implementing changes. With GPT, failing is not an option because the technology can tell users what is likely to happen when they deploy specific changes. Generative AI-driven technologies can be integrated into the DevOps toolchain, which enables developers to see the potential impact of a change prior to releasing it. Drawing from the lessons of past failures, AI and GPT can anticipate the impact of a change or release to a business service and identify the change risk level, even before implementation.

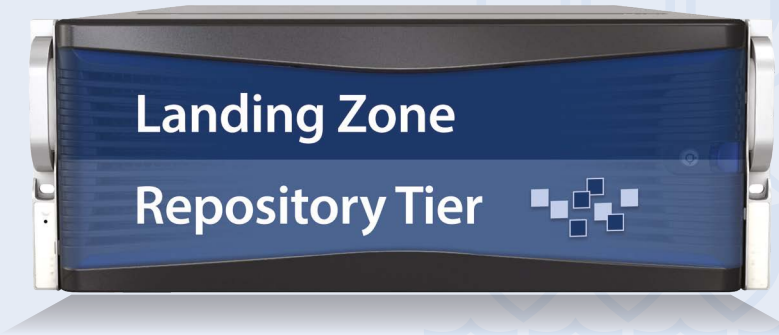
AI and GPT is intriguing IT leaders as it evolves in readily available apps and within enterprise environments. Savvy technology leaders will learn how to apply the technologies in their companies to relieve human staff of tedious data collection and correlation, and speed up time to resolution and repair. End users and customers can also enjoy the benefits of AI and GPT when it empowers them with the knowledge to help themselves.

Going forward, AI and GPT will continue enabling enterprise IT departments to streamline problem identification, resolution processes, and much more. To gain these benefits, IT leaders must devise intelligent strategies to embed the technology within their organisations and harness its power to drive an autonomous digital enterprise.



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 >