



# CHANNEL INSIGHTS

CONNECTING THE CHANNEL PARTNER ECOSYSTEM



## MSPS MUST ENHANCE THEIR CYBER SERVICES BUT HOW?

ISSUE IV 2024

AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION

MSP-CHANNEL.NEWS

### INSIDE

News Review, Features  
News Analysis, Profiles  
Research Review  
and much more...

### Why adding AI should be the new priority for MSSPs

Generative AI is proving disruptive in the security space as it accelerates the arms race between attacker and defender

### Exploding AI demand creates opportunities for UK MSPs

Demand for AI continues to rise to unprecedented levels across the UK organizations plan to expand their use of AI in the next year

### Responsible use of AI: a step into the future for MSPs

Artificial Intelligence is everywhere. It's a topic clients often ask me about, and there's no escaping it's here to stay



# 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

## AI and security – the need for latter day Clint Eastwoods?

➤ You'll find the news pages in this issue presented in a slightly different way. As I was preparing content for these pages, it became rather obvious that the majority of stories concerned AI, closely followed by cybersecurity. And as at least a couple of these stories illustrate, there seems to be an increasingly strong link between these two topics.



Put simply, at a time when organisations are already struggling to address the many cybersecurity challenges they face in an increasingly connected, digital world, AI promises to make the situation a whole deal worse. The glimmer of hope on the horizon? Well, the very same AI that will be harnessed by the bad actors can also be used by the 'good folks'.

Many commentators like to refer to the current state of the cybersecurity landscape as akin to the Wild West. I'm not sure how well the analogy holds up to the deepest scrutiny, but at a fairly basic level, the idea that both the outlaws and the sheriff's party had similar weaponry at their disposal, so it often came down to how smartly they were used, holds good for today's cybersecurity battle. As a fan of Clint Eastwood westerns in particular, I can confirm that it was often brains not brawn (and minimal dialogue from my hero!) that won the day, rather than the firepower at any one side's disposal.

If I can stretch the comparison just a little bit further, Mr

Eastwood often had to encourage and enlist the local civilians who were being terrorised by a gang of outlaws in order to win the day. And so with today's cybersecurity, there's a very real need for the cybersecurity companies and all those businesses which rely on them to enlist the help of all citizens (employees and customers) in the

fight against cybercrime. Primarily, through education, education, education. This should help to eliminate a significant proportion of successful cyber attacks over time, as everyone learns how to spot even the cleverest of strategies designed to fool individuals into handing over control to the bad actors.

Alongside such education, the requirement for businesses to invest in updating their cybersecurity defences is paramount. They'll be needing the benefits of AI-based solutions to combat the negatives of AI-based cyber attacks, alongside the use of developments such as multi-factor authentication practices as standard. The cybersecurity opportunity is no secret to the channel, as more and more resellers morph into both MSP and MSSPs. However, the next step, to become AI-based security champions is an even bigger opportunity – if something of a challenge at the same time. We'll leave post-quantum cryptography for another day... suffice it to say that cybersecurity as possibly the most important IT topic for the foreseeable future is waiting for more champions. Happily, there's no need for these cyber heroes to purchase ponchos, have a four day's growth on their chins, or smoke cigars!

**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.  
© Copyright 2024. All rights reserved. Contents may not be reproduced in whole or part without the written consent of the publishers. 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





## 18 **MSPs must enhance their cyber services, but how**

In a recent report from N-Able and research firm Canalys, it was revealed that 81 percent of Managed Service Providers (MSPs) expect growth in their cyber security offerings within the next three years

## 20 **MSPs and MSSPs must partner to protect against sophisticated cyber attacks**

For many years, cyber security has been baked into the deliverables of Managed Service Providers (MSPs)

## 22 **Storage must form the core of an enterprise cybersecurity strategy**

It's no wonder that in PwC's 24<sup>th</sup> Annual Global CEO Survey, leaders ranked cyberattacks second place amongst the most serious of all possible economic, social, political, business, and environmental threats

## 24 **Why adding AI should be the new priority for MSSPs**

Generative AI is proving highly disruptive in the security space as it accelerates the arms race between attacker and defender

## 26 **Is the API security market finally maturing?**

As with any nascent technology, the channel needed to understand the need for Application Programming Interface (API) security before it could get behind it

## 28 **Boost your MSSP's competitive edge: New strategies for leveraging threat intelligence**

How to best empower your business clients' cybersecurity with critical cyber threat intelligence

## 30 **Strengthening cybersecurity resilience in a changing world**

The data tells us that more and more customers are turning to outsourced security management because they simply can't keep up with the pace and sophistication of cyberattacks



24



## 34 Exploding AI demand creates new opportunities for UK MSPs

In 2024, demand for AI has continued to rise to unprecedented levels across the UK

## 36 The responsible use of AI: a step into the future for MSPs

Artificial Intelligence (AI) is everywhere. It's a topic clients often ask me about, and there's no escaping the fact that it's here to stay

## 38 How Green is Your MSP?

Why sustainability is critical to future growth

## 40 5G Private Networks vs Wi-Fi: What channel partners should know

For years, cellular networks and Wi-Fi appeared settled into their areas of dominance. But in some enterprise use cases, upgrades to cellular technology have handed companies unprecedented choice

## 42 Six months on – how has the UK's first charter for ITMSPs fared?

Until recently, there was no professional charter or recognised standard to guide UK-based MSPs in terms of best practice. For an industry made up of more than 10,000 businesses, employing more than a quarter of a million people, this was a significant gap

## 44 Thriving in tough times: Why Managed Services are imperative

With inflation and interest rates improving but still remaining high, businesses face significant financial pressures, compelling them to prioritise the escalating costs of technology in their strategic planning

## 46 Three ways Managed Services help SMEs think big

Managed Services are rapidly growing in popularity across the IT sector, becoming fundamental for businesses to improve efficiency and infrastructure

## NEWS

06 Workers embrace AI and prioritise skills growth

07 IT Professionals divided over how AI can improve workplace experience

08 75% of enterprises push ahead with AI, despite data governance concerns

09 Research reveals insights for bridging the AI 'gap'

10 Lack of clarity around regulation biggest obstacle to AI adoption

11 AI set to outpace security teams

12 Gen-AI set to be lead driver of business decisions by 2025

14 Cybersecurity - AI a priority

15 The 2024 State of Network Security Report reveals a shift towards multi-cloud environments

16 Growing connection between cybersecurity breaches and skills shortages

17 Annual cybersecurity spending to jump by 50%



**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. Angel Business Communications Ltd. © Copyright 2024. All rights reserved. Contents may not be reproduced in whole or part without the written consent of the publishers. ISSN 2396-9016 (Online)

# Workers embrace AI and prioritise skills growth

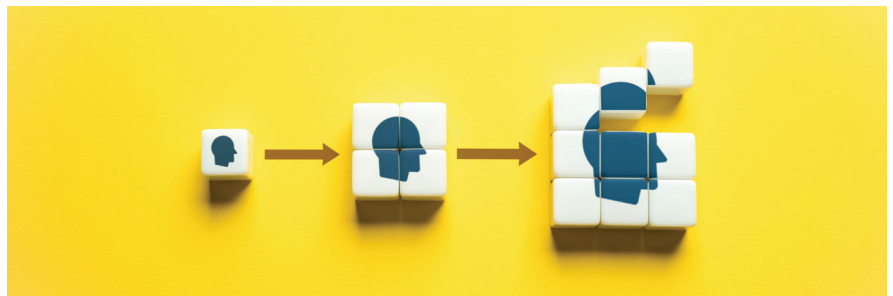
Almost half (45%) of workers say their workload has increased significantly in the past year, as almost two-thirds (62%) say the pace of change at work has increased over the same time.

AMONG MORE THAN 56,000 workers across 50 countries and territories, many say they are prioritising long-term skills growth to accelerate their careers amid rising workloads and heightened workplace uncertainty, according to PwC's 2024 Global Workforce Hopes & Fears Survey, published today.

In the last 12 months, workers say they have experienced rising workloads (45%) and an accelerating pace of workplace change. Nearly two-thirds (62%) say they have experienced more change at work in the past year than the 12 months prior, with two-fifths (40%) noting their daily responsibilities have changed to a large or very large extent. Almost half (44%) don't understand the purpose of changes taking place. In the midst of this growing mix of employee pressures, the findings suggest workers are alert to opportunities elsewhere, and are highly focused on skills growth and embracing AI.

More than one-quarter (28%) say they are likely to switch employer in the next 12 months, a percentage far higher than during the 'Great Resignation' (19%) of 2022. Two-thirds (67%) of those considering moving say skills is an important factor in their decision to stay with their current employer or switch to a new one.

Carol Stubbings, Global Markets and Tax & Legal Services (TLS) Leader, PwC UK, said: "As workers face heightened uncertainty, rising workloads and continue to face financial stress, they are prioritising skills growth and embracing new and emerging technologies such as GenAI to turbocharge their growth and accelerate their careers. The findings suggest that job satisfaction is no longer enough. Employees are placing an increased premium on skills growth in a climate characterised by constant



technological change. Employers must ensure they are investing in their employees and technological platforms to mitigate employee pressures and retain the brightest talent."

Workers embrace AI to ease workplace pressures and unlock personal growth. As employees face heightened workplace pressures, they are also turning to new and emerging technologies such as generative AI (GenAI) to help. Among those employees who use GenAI daily, 82% expect it to make their time at work more efficient in the next 12 months. Employees are also optimistic about opportunities for GenAI to support their growth. Half (49%) of all users expect GenAI to lead to higher salaries – an expectation that's even higher (76%) among employees who use the technology daily. More than 70% of users agree that GenAI tools will create opportunities to be more creative at work (73%) and improve the quality of their work (72%).

Workers are placing an increased premium on skills growth to mitigate their concerns and accelerate their careers. Employees who say they are likely to switch employers in the next 12 months are nearly twice as likely to strongly consider upskilling in that decision than workers planning to stay (67% vs. 36%). This comes as fewer than half (46%) of all employees moderately or strongly agree that their employer provides adequate opportunities to

learn new skills that will be helpful to their careers. Employees who are likely to leave in the next year may be more attuned to skills changes that are needed than the general workforce, with 51% moderately or strongly agreeing that the skills their job requires will change in the next five years (vs. 29% of those unlikely to change employer).

There is particular interest in the impact of AI on skills development, with 76% of all users expecting it to create opportunities to learn new skills at work. However, employers will need to invest heavily in new and emerging technology training and access. Among employees who have not used GenAI at work in the last 12 months, one-third (33%) don't think there are opportunities to use the technology in their line of work, while 24% don't have access to the tools at work, and 23% don't know how to use the tools.

Despite the pace of change, there are also signs of optimism and engagement at work. 60% of workers expressed at least moderate job satisfaction (up from 56% in 2023) while more than half (57%) of employees who view fair pay as important agree that their job is fairly paid. Cost-of-living pressures have slightly eased since 2023 (the proportion of workers with money left over each month has risen to 45%, up from 38%). However, more than half (52%) say they are still financially stressed to some degree.



# IT Professionals divided over how AI can improve workplace experience

Half believe it will improve their work productivity, likely due to GenAI's ability to amplify individual capabilities and get work done quicker.

MANAGEENGINE has published the results of its joint report with Service Desk Institute (SDI).

A split is emerging in how IT professionals use GenAI in their day-to-day roles, with contrasting opinions regarding its benefits on productivity. According to The State of Artificial Intelligence in ITSM – 2024 and beyond, 71% of IT professionals say their organisation is still researching or piloting AI in IT support and ITSM operations.

## Current AI deployments are geared towards end-user experience and enterprise productivity

Virtual assistants for end-user support, assisted knowledge management and assisted self-service are the top three AI-powered technologies currently used in ITSM operations at respondents' organisations. Similarly, respondents believe incident management (79%), knowledge management (73%) and service request management (67%) to be the most impacted by AI. Notably, strategic use cases of AI in ITSM, such as intelligent data analytics for insight and decision-making, saw the lowest level of current adoption. This finding resonates with the fact that 62% of respondents said that integrating AI into their existing tool is challenging.

## Cost Reduction Trumps Innovation in Driving AI Adoption

Kumaravel Ramakrishnan, the director of marketing for ITSM at ManageEngine, said, "The survey reveals two primary motivators of AI adoption in IT and differing levels of their impact on adoption: The first motivator for AI adoption is to streamline processes and reduce costs (81%), while the second is spurring innovation (67%) to differentiate from competition.



"Streamlining processes and reducing costs is more successful in driving adoption, because achieving strategic use cases requires advanced knowledge of GenAI, a clear AI strategy and the right skilled workforce to build out or integrate these solutions. The current AI offerings in the market lower the barrier to adopting AI to automate basic service desk tasks, while strategic AI use cases are yet to be commoditised."

On the other hand, the report highlights challenges to adopting AI:

- 38% cited the lack of skills and expertise in GenAI.
- 29% cited budget constraints.
- 28% blamed the lack of a clear AI strategy.

Although 45% of IT professionals report having a basic understanding of GenAI, there is a significant shortage of GenAI experts.

## Risks stemming from insufficient specialised AI knowledge

The lack of AI-specific knowledge amongst IT teams flags potential risks to organisations. Almost half (48%) have poor or limited understanding of the

compliance and legal issues of AI, and 46% have poor or limited understanding of the risks and security measures.

Meanwhile, one in four do not have governance frameworks in place for the implementation of AI. In contrast, 65% said their organisation understood the risks associated with AI, which is both heartening and could explain the low level of full-scale AI adoption (4%).

David Wright, chief value and innovation officer at SDI, said, "Adapting to AI is not just a technological challenge but a cultural shift within ITSM. This research serves as a wake-up call for ITSM professionals and organisations to prepare for a future where AI is a fundamental part of our service delivery toolkit. The successful integration of AI into ITSM hinges on our ability to synchronise technology with our most valuable asset—our people."

"The future will favour organisations that understand this balance, transforming their operations to not only include AI but also enhance the capabilities and happiness of their human workforce."

# 75% of enterprises push ahead with AI, despite data governance concerns

Three-quarters (75 per cent) of enterprises are pushing ahead with AI adoption, despite data governance and quality concerns, according to research from F5.

IN FACT, 72 per cent of enterprises admitted to facing significant challenges with data quality and scaling data practices, having a significant impact on the output quality of AI models.

Out of the 750 IT decision makers surveyed, a quarter (24 per cent) said that they had implemented generative AI at scale, with employee productivity tools and customer services tools the most common implementation.

“Our report highlights a concerning trend: many enterprises, in their eagerness to harness AI, overlook the need for a solid foundation.

This oversight not only diminishes the effectiveness of their AI solutions but also exposes them to a multitude of security threats,” said Kunal Anand, CTO at F5.



The report also highlighted key barriers to scaling AI technology within the data layer, with 72% of respondents pointing to data quality and the inability to expand data practices as major issues.

Additionally, 53% of respondents identify a lack of AI and data-related skillsets as significant obstacles. When it comes to the infrastructure layer, enterprises express concerns about the cost of computing resources

(62%), model security (57%), and overall model performance (55%).

Commenting on the findings, Roman Kucera, CTO and Head of AI, Ataccama: “Before deploying AI, enterprises must ensure the quality of their data otherwise poor data will impact the accuracy of output. Insufficient or poor quality data with errors and anomalies will undermine the trustworthiness of AI-based insights.”

We see companies that have prioritised data quality in the past becoming the ones making the leap to AI most easily today and enjoying fast time to value. For those starting out on the journey, investing in better AI training, realising operational efficiencies and unlocking data for business users will all facilitate quicker ROI for the business as a whole.”

## Is AI coming for our jobs and our company's data?

CONCERNS that AI could replace existing jobs within mid-market companies are growing. According to Node4's recent independent research, job loss fears top the list of worries that IT decision-makers have about AI use within their organisation. That number breaks down to 37% of CTOs, 29% of Heads of IT, 27% of IT Directors, 26% of CIOs, and 29% of IT Managers. It's also a common fear across each vertical sector covered within the report, with a substantial number of respondents in mid-market finance (36%), private healthcare (27%), insurance (27%), retail (29%) and transport (25%) organisations feeling the same way.

Results from Node4's Mid-Market IT Priorities Report 2024 also reveal respondents are clear about the potentially negative impact that AI could

have on their organisation's IT security: 30% said that AI represents a top cyber security threat over the next 12 months 28% believe AI could expose their organisation to new cyber security risks 25% think AI could accidentally reveal sensitive corporate information This may be why respondents confirmed that dealing with AI-related threats is their top cyber security priority for the remainder of 2024—and why a lack of security is the top barrier to AI adoption.

Node4's research suggests that most mid-market organisations intend to seek help from third parties in addressing their lack of security, as well as other key AI adoption barriers, including poor data availability and data quality. In terms of dealing with a lack of security, most respondents said they would

rely on a mix of cloud providers (50%), retained consultants (40%), and MSPs (34%). A similar proportion said that they would opt for third-party support to deal with a lack of data availability (cloud providers, 50%, MSPs, 42% and retained consultants, 36%) and data quality (cloud provider, 57%, MSPs, 35%, retained consultants 32%).

“IT decision-makers identified potential job losses and cyber security risks as their two top AI adoption concerns,” explains Geoff Barlow, Product and Strategy Director at Node4. “At this stage, it's sensible to take stock and understand not only these key issues, but how AI could also enhance your organisation. Our research suggests respondents are doing precisely that—and with great maturity and informed opinion.”



# Research reveals insights for bridging the AI 'gap'

Transformational AI enterprises are leading the charge, outperforming operational organisations across key business metrics.

VULTR has released a new industry report, *The New Battleground: Unlocking the Power of AI Maturity with Multi-Model AI*. The groundbreaking new study reveals a clear correlation between an organisation's AI maturity and its ability to achieve superior business outcomes, outpacing industry peers in revenue growth, market share, customer satisfaction, and operational efficiency.

Commissioned by Vultr and conducted by S&P Global Market Intelligence, the research surveyed over 1,000 IT and digital transformation decision-makers responsible for their organisation's AI strategy across industries, including healthcare & life sciences, government/public sector, retail, manufacturing, financial services, and more. Of the respondents surveyed, almost three-quarters (72%) are at higher levels of maturity of AI use. The report also includes a qualitative perspective on AI use by enterprises of varying sizes through in-depth interviews with AI decision-makers and practitioners.

"As organisations worldwide capitalise on strategic investments in AI, we wanted to look at the state of AI maturity," said Kevin Cochrane, CMO of Vultr's parent company, Constant. "What we've found is that transformational organisations are winning the hearts, minds, and share of wallets while also improving their operating margins. AI maturity is the new competitive weapon, and businesses must invest now to accelerate AI models, training, and scaling in production."

## The Age of Multi-Model AI

The number of models actively used within an organisation is a reliable measure of its deployed AI capabilities and overall AI maturity. The data reveals that advanced AI adopters leverage a multitude of models simultaneously as part of a multi-model approach. On average, the number of distinct AI

models currently operational stands at 158 with projections suggesting this number will rise to 176 AI models within the next year. This growth highlights remarkable acceleration in AI adoption across industries, underscored by the 89% of organisations anticipating advanced AI utilisation within two years. AI proficiency and maturity is the new business performance battleground AI is poised to permeate throughout the enterprise with 80% adoption anticipated across all business functions within 24 months. This will include AI being embedded across all applications and business units.

As AI builds on its new foothold across businesses, there will be an immense impact on enterprise-wide performance. According to the report, those with transformational AI practices reported that they outperformed their peers at higher levels. Specifically, 50% of transformational companies are performing "significantly better" against industry peers than those at operational levels, while a large majority of AI-driven organisations say they improved their 2022/2023 year-over-year performance in customer satisfaction (90%), revenue (91%), cost reduction/margin expansion (88%), risk (87%), marketing (89%), and market share (89%). Meanwhile, nearly half (40-45%) of organisations say AI is having a "major" impact on market share, revenue, customer satisfaction, marketing improvements, and cost and risk reduction.

"AI's transformative impact is undeniable—it's devouring industries and is becoming ubiquitous in every facet of business operations. This necessitates a new era of technology, underpinned by a composable stack and platform engineering to effectively scale these innovations," said Cochrane.

**AI spending is expected to outpace IT spend**



To fully harness AI's potential, 88% of the enterprises surveyed intend to increase their AI spend in 2025 with 49% expecting moderate to significant increases. Findings related to key infrastructure, partner, and implementation strategies include: For cloud-native applications, two-thirds of organisations are either custom-building their models or using open-source models to deliver functionality. In 2025, the AI infrastructure stack will be hybrid cloud with 35% of inference taking place on-prem and 38% in the cloud/multi-cloud.

Thanks to the skills shortage, 47% of enterprises are leveraging a partner to help them with strategy and implementation, and deployment of AI at scale. Only 15% are leveraging hyperscalers such as AWS, GCP, or Azure.

Open, secure, and compliant are the top attributes of cloud platforms for scaling AI across the organisation, geographies, and to the edge. "For years the hyperscalers have dominated the infrastructure market, relying on scale, resources, and technological expertise, but that is all about to change," added Cochrane. "Over the next decade, everything will be rebuilt with AI at the core, with organisations integrating the principles of cloud engineering into their operations. As a result, we will see the rise of AI specialists and independents as they empower organisations to do transformative work and gain a competitive edge."

# Lack of clarity around regulation biggest obstacle to AI adoption

New study from Freshworks finds that UK business leaders are saving more than 3 hours a week with AI tools but are being held back by unclear regulation.

A NEW GLOBAL SURVEY from Freshworks reveals that despite 65% of business leaders in the UK trusting AI to bring value to their workplace, more than a third (35%) feel that a lack of clarity around regulation is the biggest obstacle they face to adopting AI.

The new research of over 7,000 senior decision makers and managers in 12 countries, including 2,500 from the UK, Germany, France and Netherlands, explores the sentiments, use and value of using AI-enhanced tools in the workplace.

Seeing the value, but slow to adopt UK business leaders estimate that using AI helps reduce their workloads by 3 hours and 7 minutes in an average working week, with 11% claiming AI saves them more than 9 hours a week. Despite this, more than a third (37%) of UK business leaders admitted they currently have no plans to integrate AI into the workplace – with 8% even admitting they do not know if they currently used the tools.



According to senior decision makers and managers across the UK, unclear AI regulation was the main obstacle holding them back from adopting AI tools, with the UK more concerned about regulatory clarity than any other region in the world. Business leaders

in the UK were also the least likely to expect an instant return from AI, instead expecting a timeline of between 1 to 2 years before AI software would have enough business impact to prove it's worth, suggesting UK business leaders expect a longer-term approach to AI tools.

## Trust and adoption of AI

UK business leaders were also the most concerned about security and lack of testing with AI. Nonetheless, nearly 2 thirds (65%) of respondents either completely or mostly trusted AI to bring value to the business and 70% said they would trust AI even more if human review of its outputs was mandatory - echoing global sentiments. Despite concerns about AI bias, 4 in 10 (44%) business leaders in the UK actually trusted in AI's ability to remove human bias.

Many uses for AI-enhanced tools UK respondents shared that they mainly use AI-enhanced software applications for writing or creating content (43%), data analysis (39%) and researching/ brainstorming (35%). 44% feel their work is easier to complete with AI enhanced tools with 42% suggesting they get more work done and over a third (37%) claiming they are excited to use the new technology.

## Skills shortages and job concerns persist

Despite nearly half (49%) of business leaders and managers in the UK considering themselves knowledgeable or experts on AI – a lack of skills within teams was cited as one of the biggest obstacles to AI adoption by a fifth of respondents (23%).

Nearly half (46%) of UK business leaders fear that AI will end up replacing a large amount of the workforce in their field - a sentiment shared by global

counterparts. Two thirds (66%) admitted they are looking for ways to grow their AI skill set to stay as marketable as possible. Despite these concerns, respondents understand the value people bring to the workplace.

The majority (70.5%) of UK respondents feel AI will never be able to completely replace human workers.

## Measuring AI's impact

Increased quality of work (89%) productivity gains (88%), reduced need for other software (82%) and improved customer engagement (80%) ranked the most important measures of AI's business impact. 4 in 10 (40%) believe AI software is already providing a better return on investment than other software their business had implemented.

AI-enhanced tools are transforming workflows, productivity and performance in the workplace the world over. While the adoption of such tools vary between countries, the potential it presents is irrefutable.

"This report exemplifies that AI is delivering tremendous productivity gains at enterprise scale," said Freshworks Chief Product Officer, Prakash Ramamurthy. "Knowledge workers are also seeing strong productivity gains at work, which in turn is sparking strong employee interest in mastering AI skills. Make no mistake, the AI era is firmly delivering on its promise to free up employees for higher-level work and showcasing compelling returns on AI. Leaders across industries perceive AI as a transformative technology capable of delivering significant business impact, from enhanced decision-making and increased operational efficiencies to personalized customer experiences and innovative product development."



# AI set to outpace security teams

“Inside the Mind of a CISO” report uncovers CISO perceptions on AI threats, ethical hacking, and the expertise needed to address the cyber skills gap.

BUGCROWD has released its “Inside the Mind of a CISO” report, which surveyed hundreds of security leaders around the globe to uncover their perception on AI threats, their top priorities and evolving roles, and common myths directed towards the CISO.

## Money & Hiring

Among the findings, 1 in 3 respondents (33%) believed that at least half of companies are willing to sacrifice their customers’ long-term privacy or security to save money. This is explained in part by the fact that 40% believed that less than 1 in 3 companies truly understood their risk of being breached. Speaking of money, nearly 9 in 10 (87%) reported that they were currently hiring security staff and 56% stated that their security team was currently understaffed. And despite some common misconceptions around not needing a college degree, respondents reported that only 6% of cybersecurity leaders don’t have a college degree and over 80% have a degree specifically in cybersecurity.

Despite plans to hire, 70% reported that they planned to reduce the security team headcount within the next 5 years

due to the adoption of AI technologies. Over 90% believe that AI already performs better than security professionals, or at least will in the near future. AI isn’t only seen as a benefit however, over half (58%) believe that the risks of AI are worse than its potential benefits.

**CISO Perspectives on Ethical Hacking**  
Due to concerns around the malicious use of AI by attackers, 70% of security leaders turned towards using crowdsourced security for testing their AI defenses. In fact, more than 7 in 10 (73%) of security leaders view ethical hacking in a favorable light and 75% of them actually have experience with it themselves. With modern day threats being more evasive and adaptive than they’ve ever been – 89% believe there are more threats and they are more serious – it’s imperative that crowdsourced security be the center of an organization’s cybersecurity strategy. Nick-M



“The CISO role is evolving. Given the current risk landscape and the need to prioritize security over resilience, the CISO has more responsibility than ever before,” Nick McKenzie, CISO at Bugcrowd. “Bridging the gap between CISOs and the collective

ingenuity of hackers is key to shielding organizations from the increasing onslaught of AI threats and attacks.”

As the cybersecurity landscape continues to evolve, professionals and organizations must remain ready to adapt to the latest trends and emerging technologies such as AI and the implementation of crowdsourced cybersecurity. The Bugcrowd Platform connects organizations with trusted hackers to proactively defend their assets against sophisticated threat actors. In this way, CISOs can unleash the collective ingenuity of the hacking community to better uncover and mitigate risks across applications, systems, and infrastructure.

## MSP ROUNDTABLE

CONNECTING THE CHANNEL PARTNER ECOSYSTEM

Not every discussion is a  
**heated debate...**

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

**Cost: £5995**

**Contact: Jackie Cannon**  
jackie.cannon@angelbc.com



# Gen-AI set to be lead driver of business decisions by 2025

A third expect Gen-AI to be the lead source of insight for enterprise-wide decision-making.

FOLLOWING a new independent research study, Stratio BD reveals that three in four (75%) IT decision-makers are expecting to increase their use of Gen-AI tools in the next 12 months, with a third (33%) stating that the technology will become the most important source of insight for business decision-making.

Seeking to understand the current status of Gen-AI adoption across a variety of global markets, Stratio BD surveyed data and IT decision-makers across the UK, Spain and LATAM to map the extent to which Gen-AI is understood and has been implemented within corporate systems. These findings highlight the pace at which Gen-AI tools are delivering value to organisations throughout the world, and just how swiftly their benefits are being recognised by the organisations which have quickly realised the potential for their integration.

The international research found that over a quarter of respondents plan to integrate Gen-AI into their core business processes within the next six months, while a third of decision-makers believe their roles will be fully integrated with the technology in the next year.

Stratio BD's research also demonstrates that data and business leaders are actively enthusiastic about its transformative power for business deployment. Over three quarters of those surveyed said they have a clear view of what the technology could achieve for their organisation, while two thirds agreed that senior leadership were as informed as they could be with respect to how Gen-AI could help their business thrive.

This enthusiasm is further reflected in three-quarters (75%) of respondents feeling excited about the increased use of the technology within their



organisation, dispelling the myth that Gen-AI is a threat on employees' jobs. In addition, two fifths of the professionals believe that Gen-AI will in fact create more time to focus on other areas of strategic focus within their organisation.

Even in the face of this enthusiasm and initial adoption, the survey findings also highlight that active implementation is still lagging behind organisational understanding of the technology.

Only 29% reported that Gen-AI has already been implemented into their organisation's core processes, while over one in ten (11%) of IT decision-makers reported that the business is either trialing Gen-AI but has no plans to implement it on an organisation-wide level, or that their businesses have no plans to implement Gen-AI whatsoever.

Óscar Méndez, CEO and Founder of Stratio BD, says: "This disconnect between organisational understanding of Gen-AI and its active implementation shows that businesses are not yet fully accessing the true benefits of Gen-AI. Our research finds that almost all of those surveyed (99%) agree that organisations are actively missing out on opportunities by not using Gen-AI, particularly surrounding automation (63%), generating new ideas (59%) and optimising operations (52%). This could represent a significant competitive advantage, which business' competitors may be swift to exploit."

One of the standout areas highlighted by the survey was Gen-AI's demonstrable ability to enhance business results from interrogating internal data, particularly when it comes to time savings. For example, three-fifths of those not using Gen-AI were satisfied with the time taken to complete data queries, while nearly everyone (92%) using Gen-AI were either very satisfied or satisfied on this front. Likewise, lingering concerns over security and accuracy are still hampering the implementation of Gen-AI. Questions over whether the data produced by Gen-AI is accurate enough to inform decision-making was the most frequently (38%) listed obstacle to implementation, followed by concerns over data quality and accessibility (31%) and concerns over bias and privacy (28%).

Méndez continues: "These lingering worries over privacy and security remain despite the leaps forward which AI technology has recently made in tackling these issues. While concerns persist regarding data accuracy and quality for informed decision-making, our findings underscore the business imperatives for enterprise-level solutions that ensure the precision and security of Gen-AI generated data. Those responsible for AI and data insights within their organisations are very aware that without such measures, the transformative potential of this technology to feed business success will remain unrealised.

"Stratio BD is at the forefront of this revolution. Not only does our Gen-AI product enable businesses to capitalise on the efficiency advantages of Gen-AI, but it also ensures that the data produced by Gen-AI is accurate and can be trusted to inform decision-making. The only obstacle that remains for business leaders when it comes to capitalising on the Gen-AI boom is the boundaries of their collective imaginations."





# SDC AWARDS 2024

SAVE THE  
DATE  
28.11  
2024

Leonardo Royal City London

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](mailto:awards@sdcawards.com)

<https://sdcawards.com/home>



# Cybersecurity - AI a priority

91% view the adoption of artificial intelligence as a priority, highlighting vulnerability assessment and threat detection as key benefits.

ARTIFICIAL INTELLIGENCE and Machine Learning (AI and ML) are recognized as important parts of the future of cyber security and cloud security. But how integrated are these technologies in cyber security functions currently? A recent survey by Check Point and Cybersecurity Insiders asked hundreds of professionals from across different industries how they've been using AI so far, how much of a priority it is for their companies, and how it has impacted their workforces.

Several questions on the survey asked respondents about the state of AI in their organizations' cyber security plans as of today, including how fully implemented it is and how that implementation is going. Their responses paint a picture of an industry that is moving slowly and cautiously, and perhaps hasn't gone as "all-in" on AI as some may expect. Organizations still seem to be evaluating the benefits and risks associated with AI and ML tools, and businesses are moving carefully to establish firm best practices that comply with relevant regulations.

When asked to describe their organization's adoption of AI and ML in cyber security, 61% of respondents described it as being either in the "planning" or "development" stages – significantly more than the 24% who categorized it as "maturing" or "advanced." Additionally, 15% of those surveyed said that their organizations haven't implemented AI and ML into their cyber security efforts at all. Clearly, while the selling points of AI for cyber security efforts are persuading many businesses to start exploring their potential, few businesses have fully embraced them at this point.

Another question on the survey got more specific, asking respondents "Which cyber security (cloud) functions in your organization are currently enhanced by AI and ML?"

The answers are illuminating, with malware detection leading the way at 35%, with user behaviour analysis and supply chain security following right behind. Towards the bottom of the list, fewer organizations look to be using AI for security posture management or adversarial AI research. Taken together with the responses to the previously discussed question about the overall state of AI, the data shows that individual applications of AI and ML in cyber security are still far from being universal.

One reason that AI adoption hasn't raced along at a faster pace is the challenge of navigating a rapidly shifting regulatory landscape. In these early days, laws and government guidance is still evolving around AI and cyber security. Businesses can't afford to take risks when it comes to compliance and keeping up with these rapid changes can be complex and resources intensive.

How are organizations approaching AI for cyber security going forward? Despite the slow and cautious adoption of AI in cyber security so far, it's almost universally regarded as an important priority going forward with 91% ranking it as a priority for their organization, and only 9% of those surveyed said it's a low priority or not a priority at all. Respondents clearly see the promise of AI to automate repetitive tasks and improve the detection of anomalies and malware, with 48% identifying that as the area with the most potential.

Additionally, 41% see promise in reinforcement learning for dynamic security posture management using AI – especially interesting when compared to the only 18% who are currently using AI for this function. The excitement is obvious – but there are challenges in the way of realizing this potential. Beyond specific applications, respondents were asked to identify

what they see as the biggest benefits of incorporating AI into cyber security operations. The most popular answers included vulnerability assessment and threat detection, but cost efficiency was the least-popular answer, at just 21%. Likely due to the pricey challenge of regulatory compliance and the cost of implementation, AI isn't currently viewed as a significant money-saving tool for most who answered.

Additional questions on the survey provided insight into professional concerns and a lack of clarity about some of the fundamentals of AI and cyber security. On the subject of the impact of AI on the cyber security workforce, it's apparent that this is still an open question without clear answers yet. 49% identified new skills being required by AI, and 35% noted redefined job roles. And while 33% said that their workforce size has been reduced as the result of AI, 29% said that their workforce size has actually increased. Implementing AI into cyber security is clearly a work in progress, and while greater efficiency is a promise that might be realized in the future, for now many businesses are actually having to hire more people to integrate the new tech.

Notably, there was a significant split in the answers to the question: Do you agree with the following statement: "Our organization would be comfortable using Generative AI without implementing any internal controls for data quality and governance policies"? While 44% disagreed or strongly disagreed with the statement, 37% said that they would agree or strongly agree. It's very rare to see such a substantial split on a question like this on a professional survey, and that split seems to indicate a lack of consensus – or perhaps simply a lack of awareness regarding the importance of internal controls and governance policies when AI is involved.

# The 2024 State of Network Security Report reveals a shift towards multi-cloud environments

Research found that organisations are prioritising security, seamless integration, and compliance in hybrid cloud environments with Cisco, Palo Alto Networks, AWS and Microsoft Azure among the leaders.

ALGOSEC has released its annual 'The State of Network Security Report' providing a broad view of network security in hybrid cloud environments, identifying the most popular strategies adopted by security professionals. The report sheds light on key market trends and highlights the solutions and technologies that are in demand and why, helping organisations to navigate the complexities of modern network security.

Based on two comparative surveys conducted in H2 of 2022 and 2023, AlgoSec's research evaluated market leaders including AWS, Microsoft Azure, Check Point, Palo Alto Networks, Cisco and more, identifying significant shifts in cloud platform adoption, deployment of firewalls and Software-Defined Wide Area Network (SD-WAN), as well as Secure Access Service Edge (SASE) implementation.

Key findings from the report include: Security, continuity, and compliance driving cloud platform selection – When selecting a cloud platform, organisations prioritise seamless integration, compliance, and robust security features. While the overall adoption of cloud platforms has grown,

the ranking of different vendors has remained relatively stable. Azure continues to be the most widely used platform, closely followed by AWS, which has shown the fastest pace of growth.

The growing adoption of SD-WAN – The move towards remote working and cloud computing has been the catalyst for the increased deployment of SD-WAN, ensuring secure and reliable connections across multiple locations. That is reflected in the report, with a steep decline in the number of organisations that had no SD-WAN solution from 55.2% in 2022 to 34% in 2023.

The rise in SASE adoption – With network infrastructures becoming more complex, SASE has become a popular solution for organisations, consolidating multiple security functions into a single, unified, cloud service.

The report found the rate of SASE adoption has increased year-on-year, with notable growth of Zscaler implementation from 21.9% in 2022 to 37% in 2023, and Prisma access implementation from 16.2% in 2022 to 22.8% in 2023.

The increasing importance of firewalls in cloud estates – With more businesses looking to secure corporate resources across complex cloud networks, firewall implementation has increased as a result, providing organisations with the means to safeguard against external threats.

The rate of adoption has risen significantly, with only 7.1% of respondents saying they had no firewalls deployed in 2023 - a sharp drop from the 28.4% recorded in 2022.

The persistence of hybrid networks – Despite the general shift towards cloud adoption, on-premise data centres and device rollouts remain a significant feature of the network landscape.

"According to our research there has been greater adoption of cloud-based network security solutions across the board", said Eran Shiff, VP Product of AlgoSec. "However, there is still progress to be made in the SD-WAN and SASE space. By identifying the key trends and the most popular solutions on the market, we can provide some much-needed clarity into the complex world of network security."





# Growing connection between cybersecurity breaches and skills shortages

Nearly 90% of organizations experienced a breach in the last year that they can partially attribute to a lack of cyber skills, and 70% attribute increased cyber risks to the skills gap.

FORTINET has released its 2024 Global Cybersecurity Skills Gap Report, which highlights ongoing challenges related to the cybersecurity skills shortage impacting organizations around the globe. Key findings from the report include:

- Organizations are increasingly attributing breaches to the cyber skills gap.
- Breaches continue to have significant repercussions for businesses, and executive leaders are often penalized when they happen.
- Certifications continue to be highly regarded by employers as a validator of current cybersecurity skills and knowledge.
- Numerous opportunities remain for hiring from diverse talent pools to help address the skills shortage.
- The Cyber Skills Gap Continues to Impact Companies Worldwide

An estimated 4 million professionals are needed to fill the growing cybersecurity workforce gap. At the same time, Fortinet's 2024 Global Cybersecurity Skills Gap Report found that 70% of organizations indicated that the cybersecurity skills shortage creates additional risks for their organizations. Other findings that highlight the impact of the growing skills gap on companies across the globe include: Organizations are attributing more breaches to a lack of cyber skills. In the past year, nearly 90% of organizational leaders (87%) said they experienced a breach that they can partially attribute to a lack of cyber skills, up from 84% in the 2023 report and 80% the year prior. Breaches have a more substantial impact on businesses. Breaches have a variety of repercussions, ranging from financial to reputational challenges. This year's survey reveals that corporate leaders are increasingly held accountable for cyber incidents,

with 51% of respondents noting that directors or executives have faced fines, jail time, loss of position, or loss of employment following a cyberattack. Additionally, more than 50% of respondents indicate that breaches cost their organizations more than \$1 million in lost revenue, fines, and other expenses last year—up from 48% in the 2023 report and 38% from the previous year. Boards of directors view cybersecurity as a business imperative.

As a result, executives and boards of directors increasingly prioritize cybersecurity, with 72% of respondents saying their boards were more focused on security in 2023 than the previous year. And 97% of respondents say their board sees cybersecurity as a business priority.

Business leaders widely regard certifications as validation of cybersecurity knowledge, and those who hold a certification or work with someone who does notice clear benefits. This year's survey also found that:

- Candidates with certifications stand out. More than 90% of respondents said they prefer hiring candidates with certifications.
- Leaders believe that certifications improve security posture. Respondents place such high value on certifications that 89% said they would pay for an employee to obtain a cybersecurity certification.
- Finding candidates who hold certifications isn't easy. More than 70% of respondents indicated that it is difficult to find candidates with technology-focused certifications.

As the cyber workforce shortage persists, some organizations diversify their recruitment pools to include candidates whose credentials fall outside traditional backgrounds—such



as a four-year degree in cybersecurity or a related field—to attract new talent and fill open roles. Shifting these hiring requirements can unlock new possibilities, especially if organizations are willing to pay for certifications and training. The report also found that: Organizations continue to have programs dedicated to recruiting from a diversified talent pool. Eighty-three percent of respondents said their organizations have set diversity hiring goals for the next few years, in line with last year's report but slightly down from 89% in 2021.

Diversity hiring varies from year to year. Despite ongoing recruitment targets, female hires are down to 85% from 89% in 2022 and 88% in 2021; hires from minority groups remain unchanged at 68% and up slightly from 67% in 2021; and veteran hires are up slightly to 49% from 47% in 2022, but down from 53% in 2021.

While many hiring managers value certifications, some organizations still prefer candidates with traditional backgrounds. Despite many respondents saying they value certifications, 71% of organizations still require four-year degrees, and 66% hire only candidates with traditional training backgrounds.

## Annual cybersecurity spending to jump by 50%

Although companies and organizations worldwide have already significantly increased their cybersecurity budgets, the total spending on cybersecurity tools and services will skyrocket in the coming years.

DESPITE the maximum efforts to prevent and minimize cybercrime damage, cyber-attacks, including ransomware attacks, data breaches, cyber espionage, phishing, and cyber espionage, are still the biggest threats in the business sector.

The fear of cybercrime is quite understandable, considering the amount of money stolen in cyber attacks each year.

In 2024 alone, the annual cost of cybercrime is expected to hit a shocking \$9.2 trillion. Over the next four years, this figure is forecasted to jump by 70% and hit a head-spinning \$13.8 trillion. So, it's not surprising that companies and organizations continue spending more and more money on protecting their business.

The Statista Market Insights survey shows that total spending on cybersecurity jumped by 60% over the past six years, rising from \$115 billion in 2018 to an expected \$185 billion in



2024. However, the following years are set to witness just as impressive growth.

Statista expects the annual spending on cybersecurity to continue growing by an average of \$17 billion per year, resulting in a market revenue of \$272 billion by 2029. Cyber solutions will remain the market's largest and highest-grossing segment in the following years.

Between 2024 and 2029, global cyber solution revenues are expected to grow by 67% and hit \$148.3 billion, making up 55% of the market's total. The security services segment is forecasted to grow much less, with revenues rising by 27%

to \$123.6 billion. Companies to Spend \$2.15 Trillion on Cybersecurity in a Decade And while \$272 billion in total cybersecurity revenues is a huge number, the cumulative figures are even more shocking. Statistics show that companies and organizations worldwide will spend over \$2.5 trillion on cyber solutions and security measures in a decade.

Despite the significant investments in cybersecurity, the total spending remains a fraction of the total cost of cybercrime.

According to Statista, the projected damages from cybercrime in a decade will be a staggering 33 times larger than the total cybersecurity spending, amounting to \$82.8 trillion.

This figure is more than the GDP of the world's ten largest economies, underscoring the need for increased investment in cybersecurity.

## Sustainability a top focus for tech investment

LOGICALIS reveals sustainability is a key priority for tech leaders in 2024. According to its tenth annual CIO Report, which surveyed over 1,000 CIOs globally, almost all (92%) CIOs are investing in sustainability initiatives or technologies this year.

In the face of global economic uncertainty, the commitment to the green agenda among CIOs stands resolute with CIOs at the heart of their organisation's sustainability strategy. 96% of tech leaders said they are already involved in their company's overall sustainability planning and target setting and 93% said they believe IT is core to successfully delivering on their organisation's environmental objectives. An overwhelming 90%

also said they assess the sustainability credentials of new suppliers before working with them.

Sustainability continues to be recognised as a necessary investment by businesses as it not only benefits the environment but also reduces energy consumption and operational costs. However, there are still stumbling blocks to overcome.

Most (93%) see challenges in attaining their environmental goals, with 43% stating that collecting data distributed across the organisation is a challenge. A similar number are not completely confident that their organisation knows how its digital estate is performing against environmental goals. Reflecting on the findings at Logicalis's Global

CIO summit in London, Bob Bailkoski, Logicalis CEO said: "Investing in sustainability is not only the right thing to do, it's a commercial imperative for business. We know that a reduction in carbon and energy consumption also means lower costs, and with regulations on carbon reporting becoming more stringent, prioritising sustainability now will serve CIOs well later.

"We're working very closely with our partners to ensure there is carbon accountability on our part in the outcomes we deliver through technology and, through visibility tools like our Digital Fabric Platform, we're empowering customers themselves to better manage the carbon performance of their IT estate."



## MSPs must enhance their cyber services, but how?



In a recent report from N-Able and research firm Canalys, it was revealed that 81 percent of Managed Service Providers (MSPs) expect growth in their cyber security offerings within the next three years.

The report stated that cyber security will provide the biggest growth opportunity for MSPs, who will be looking to expand their services beyond the basic detection of attacks.

**BY OLIVER SPENCE, CEO OF CYBAVERSE**

CYBERCRIME has become a critical threat to all digital businesses, but very few have the internal resources to keep pace with adversary techniques. Organisations simply don't have the tools, skills or resources to manage security effectively in house. Unsurprisingly, this has driven them towards MSPs.

MSPs have been delivering IT and basic security services to these businesses for years, but as cybercrime becomes increasingly sophisticated, and AI continues to innovate for adversaries, the need for more advanced detection, remediation and response is skyrocketing.

This is a great opportunity for MSPs and it provides the sector with more potential to profit from the \$2 trillion cyber security market.

But the one drawback comes down to internal resources. With an increased need for cyber services from clients, this could place additional strain on MSPs, who are suddenly being relied upon to deliver cyber expertise, without necessarily



having the inhouse resources to support the need.

Plus, as security offerings expand, this introduces new tools into the MSP environment, meaning there are more technologies to learn and more dashboards to navigate across, which potentially burdens resources and drains the time of team members.

But is there a way to tackle these important challenges?

Is it possible for MSPs take advantage of the business opportunities cyber has to offer them, without overstraining their own internal resources?

### Streamlining security

The increased requirement to deliver enhanced security services provides both an opportunity and challenge for MSPs.

There is an opportunity to deliver more value to customers, which will in turn positively impact the MSP bottom line. But the challenge all comes down to internal resources.

Suddenly MSPs are being relied on to provide advanced cyber services, but many don't have the internal skills or resources to deliver this. Plus, with the introduction of new tools and dashboards, this adds further strain to teams who will struggle to manage security efficiently across all of their client's varying platforms.

To address these challenges, MSPs need to find a partner that not only possesses the technical skills to deliver client security projects, but also to support them as they introduce new security tools into their environment, so they have a more efficient way to manage security for their clients.

Fortunately, these important goals can be achieved by partnering with dedicated Managed Security Service Providers (MSSPs).

MSSPs are experts in the field of cyber security and they possess the skills needed to deliver the advanced security services organisations need. Today, MSSPs and MSPs can forge strategic relationships to better serve the security needs of clients.

When it comes to identifying an MSSP partner, MSPs must look for a business that understands the unique challenges they face and wants to work alongside them to help them grow and better serve their customers.

The MSSP must be flexible and deliver real value to MSPs, allowing them to purchase the services their clients need, plus offering them tools that allow MSPs to manage and monitor the security of their clients in a more streamlined view.

For instance, some MSSPs have developed platforms which are specifically designed to cater to the needs of MSPs. Providing the ability to streamline cyber security management, while offering MSPs with the ability to pull all their clients' security efforts and data into one place, enabling them to easily track, manage and remediate threats.

These platforms also allow MSPs to easily track and manage security in real-time, which allows them to keep on top of their clients' security efforts. Additionally, MSPs can view real-time data on penetration testing, vulnerability scans and regulatory compliance and some platforms have a marketplace where MSPs can purchase vital cybersecurity services for their clients, allowing them to tailor their security offerings to better serve their individual clients' needs.

MSPs have always been a trusted security partner for organisations, but as cybercrime continues to escalate many businesses today need more specialised defences to keep their critical assets secure.

These businesses are turning to MSPs to deliver these enhanced services, which provides new revenue opportunities for the industry. But, with few MSPs having dedicated cyber specialists on their teams, this is adding pressure to their businesses.

Fortunately, MSSPs could be the solution.

By establishing strategic relationships with MSSPs, MSPs can deliver on their client's new security requirements. This allows them to help improve the cyber defences of their clients, while continuing to deliver the other important IT services their clients continue to rely on them for. Without overburdening resources, while safe in the knowledge their clients' security is being managed by experts in the field.





## MSPs and MSSPs must partner to protect against **sophisticated cyber attacks**

For many years, cyber security has been baked into the deliverables of Managed Service Providers (MSPs). These organisations have packaged basic security tools into their offerings to help protect clients against routine security threats. Until recently, it has been a good model.

**BY MARK ROBERTSON, CHIEF REVENUE OFFICER AND CO-FOUNDER AT ACUMEN**

ORGANISATIONS have been provided with a one-stop-shop for all their IT and security needs, while MSPs have released a lucrative revenue stream through the upselling of cyber security tools.

But the time has come for this model to change.

These basic cyber protections are no longer a match for the sophisticated cyber attacks we are seeing today. Over the last few years, cyber attacks have evolved from technical nuisances into business destroying threats. Ransomware has become mainstream,

while criminals now impersonate employees or business leaders and trick organisations out of millions in a matter of minutes. Furthermore, the ubiquity of certain software is leaving organisations exposed to vulnerabilities, which are providing criminals with limitless access into their networks. Cyber attacks are no longer just basic technical threats, they destroy business-as-usual, so organisations' defences must be robust enough to meet this challenge.

The traditional security services that have been delivered via MSPs are no longer enough to keep





organisations safe. Instead, these defences must be enhanced, so they are catered to the evolving nature of attacks today and delivered round-the-clock, 365 days a year, embedding both technical tooling and human expertise.

But for many MSPs, these are skills and resources they don't hold inhouse. MSPs are not experts in the field of cyber, they often don't run their own inhouse Security Operations Centres (SOCs) and they don't have the resources to manage security on a 24/7 basis for their clients.

So how can they overcome this challenge, where they can still cater to the evolving security needs of their clients, without overburdening teams or drastically changing the overall function of their business?

It turns out Managed Security Service Providers (MSSPs) might just be the solution.

### Establishing new relationships to deliver bespoke cyber protection

MSPs and MSSPs have worked in close proximity for many years, but today it is more important than ever that they strengthen their relationships to enhance the security services offered to organisations.

While MSPs have increasingly been relied on by their customers to provide basic cyber security services, very few have the resources needed to protect against the sophisticated attacks we are seeing today. But this problem can be tackled by partnering with MSSPs and outsourcing the security needs of their clients.


Trusted MSSPs will work 24/7, helping keep their clients safe in cyber space. They will boast SOCs where they can monitor the security status of organisations in real-time, allowing them to detect and respond to attacks as soon as they happen.

Furthermore, MSSPs will possess all the best security tooling and human expertise to keep clients safe. Security is their business, it is their focus and expertise, so they are always up to date with the latest attack trends, and they have all the inhouse resources needed to manage security effectively.

When MSPs outsource the security of their clients to MSSPs, this can free up internal resources, provide customers with more advanced cyber defences while delivering new recurring revenue opportunities. Rather than MSPs purchasing tools internally and upskilling staff, they can partner with trusted MSSPs, who are experts in the field of cyber and have unrivalled knowledge of today's attack landscape.

Furthermore, cyber security is no longer an issue that should be rolled into IT. Cyber attacks are all-encompassing, they are no longer siloed to IT. Today successful attacks can damage the share price of an organisation, put customers and employees at serious risk and even threaten the future on a business. With the impacts of attacks never being isolated to IT, this means defences must be business-wide as well. MSSPs can support organisations with their security strategies, ensuring all staff are trained effectively and processes are adopted to ensure cyber security runs business-wide, and not just within the IT department.

Cyber is a key challenge for all organisations today and MSPs and MSSPs have a duty to protect their clients. When MSPs don't have the inhouse resources to cater to the evolving security needs of their clients, partnering with MSSPs is an effective solution. This means MSPs don't have to make unnecessary investments or overburden internal resources, but they can continue to serve their customers, keeping them safe even in the face of today's most sophisticated attacks.



# ROUNDTABLE


CONNECTING THE CHANNEL PARTNER ECOSYSTEM


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

**Cost: €5995**

**Contact: Jackie Cannon**  
[jackie.cannon@angelbc.com](mailto:jackie.cannon@angelbc.com)

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







## Storage must form the core of an enterprise cybersecurity strategy

It's no wonder that in PwC's 24<sup>th</sup> Annual Global CEO Survey, leaders ranked cyberattacks second place amongst the most serious of all possible economic, social, political, business, and environmental threats. Ransomware attacks represented 12% of breaches of critical infrastructure in the last year.

**BY JAMES 'JT' LEWIS, DIRECTOR OF CHANNEL SALES FOR EMEA AND APJ AT INFINIDAT**

CYBER SECURITY EXPERTS have estimated that global cybercrime costs will exceed 7.5 trillion Euros this year, according to CyberSecurity Ventures. Enterprises run on data and when it's hacked or corrupted by cybercriminals, the disruption can topple an operation overnight, with multi-million Euro consequences.

The irony is that if the fallout from a cyberattack happened that quickly, it may be less problematic to recover from. Remedial action should be started immediately and any damage minimised. The actual problem is much more insidious because when cyber attackers target an enterprise, they usually wait for almost 6 months before taking action.

This increases their ransom power and without the right data controls, the victim's only option may be to concede to whatever financial demands are being made. In that timeframe, their primary data, the live data your business operations depend, on could have been exposed to all kinds of criminal activity.

For this reason, enterprise storage has become a main target of cybercriminals for the most damaging and hard-to-detect ransomware and malware attacks. One reason why enterprises still get trapped is because a cybersecurity strategy tends to focus on keeping criminals out in

the first place, rather than accepting that attacks will most likely happen and there is an impetus for having a watertight strategy. The wolf will definitely keep knocking and will get inside your house. So, what steps can you take?

Firstly, cybersecurity's emphasis must widen, to address three areas - detection, resilience and recovery - and plug the vulnerability gap that cybercriminals have been exploiting. Combining resilience (the ability to instil defensive security measures to repel attacks), detection (the ability to know when data is corrupted and whether a known good copy of data is free of ransomware or malware), and recovery (the ability to bounce back and recovery with a known good copy of the data) from cyberattacks, is the key to hardening storage infrastructure.

Converging cyber resilience, detection, and recovery on an integrated enterprise storage platform is an advancement over former siloed approaches that rely on disparate tools and technologies. It makes the cyber capabilities more air-tight and ensures a rapid recovery of data within minutes to thwart cybercriminals, nullifying ransom demands and minimising downtime or damage to the business.

There are some key features of enterprise storage that need to be in place to ensure cyber resilience against today's cybercriminals, all of whom are highly skilled technology experts. These include ensuring the immutable nature of the data, recovered from a copy you can trust.



Air-gapping to separate the management and data planes to protect the data. A secure forensic environment, to analyse the data thoroughly and ensure the fastest recovery speeds possible is critical.

Immutable snapshots allow the end user to roll back the clock and recover guaranteed, uncorrupted copies of their data, before the execution of any malware or ransomware code introduced by an attacker. Immutable snapshots ensure data integrity because they prevent data copies from being altered or deleted by anyone. Even internal systems administrators are locked out of immutable snapshots manipulation. The enterprise can be confident that any disruption or damage caused by the intrusion is minimal.

Logical air gapping adds a further layer of security, by creating a safe distance between the storage management layer and the immutable snapshots. There are three types of air gapping. Local air gapping keeps the data on premises, remote air gapping makes use of a remotely hosted system and hybrid air gapping combines the two.

Fenced forensic environments help speed up the recovery process by providing a secure area to perform a post-attack forensic analysis of the immutable snapshots. The purpose here is to carefully curate data candidates and find a known



good copy. The last thing an enterprise wants after an attack is to restore data infiltrated with malware or ransomware.

Once these core elements are present within your storage infrastructure, the whole restoration can progress like clockwork. It's why our focus as an organisation is dedicated to educating IT leaders about the need for a convergent, tripartite approach. One that combining cyber resilience, detection, and recovery on a single storage platform. Reliance solely on backups and preventing attacks is no longer enough to secure storage systems.

# MANAGED SERVICES SUMMIT NORDICS

1 OCTOBER 2024

STOCKHOLM WATERFRONT



# SAVE *the* DATE

TO DISCUSS  
SPONSORSHIP  
OPPORTUNITIES: 

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

**Peter Davies**  
peter.davies@angelbc.com  
+44 (0)2476 718970

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

<https://nordics.managedservicessummit.com>

Angel  
BUSINESS COMMUNICATIONS

ITEUROPA

ANGEL  
EVENTS



## Why adding AI should be the new priority for MSSPs

Generative AI is proving highly disruptive in the security space as it accelerates the arms race between attacker and defender.

**BY INNES MUIR, REGIONAL MANAGER, MSSPS, UK, EIRE AND ROW, LOGPOINT**

ACCORDING TO the Mission Critical: Unlocking the UK AI Opportunity Through Cybersecurity report, just over a quarter of organisations (27%) are using AI to strengthen their security which means it's a nascent sector, presenting the Managed Security Service Provider (MSSP) with a golden opportunity to seed the market. In fact, the report states that in order to keep systems secure, most businesses will need to invest in innovative AI-enabled solutions from external partners.

But for the MSSP, integrating AI challenges the business model. Until Language Learning Models (LLMs) such as ChatGPT, Google PaLM and Gemini, and Meta's LLaMA burst onto the scene, most MSSPs were focused on consolidating the cyber stack to make their operations more streamlined and efficient. There's a tendency for point solutions to duplicate functionality and multiple solutions can result in swivel chair operations as the security analyst needs to consult each of these different systems when investigating an incident. All of this adds up to wasted resource.



### Consolidate or expand?

Now, instead of consolidating their operations, MSSPs are faced with the problem of having to expand the portfolio and the headaches this brings. New AI-enabled cybersecurity solutions will need to be integrated and their output understood in conjunction with the rest of the stack. The security analyst, too, will need to adapt to new ways of working, using prompts to interrogate data. The AI solution itself will also need to be properly configured to ensure there is no danger of misinformation or data leakage from the organisation or its customers. And, with AI swelling the stack still further, there is the potential for opportunities to be missed. For example, if the information being made available by the AI is not understood it won't be utilised and so becomes a wasted opportunity.

It's this ability to understand the output from AI solutions that is going to be fundamental to MSSPs monetising these services. If there is output that is ignored, the value of the offering cannot be realised



and this is something we've seen before. When MSSPs began to invest in Security Orchestration Automation and Response (SOAR), there was a great deal of excitement over the ability of the technology to automate threat detection and incident response (TDIR). SOAR utilises playbooks that can then see processes kick-in to deal with specific incidents without the need to involve the security analyst and so it can effectively fill any expertise gap the MSSP may have. But it has not always been fully exploited.

The reality is that SOAR has only partially been utilised by some MSSPs despite its game changing abilities. These providers are primarily using it for data consolidation, enrichment and normalisation, which while valuable in its own right is only a fragment of what the solution can do. What's more, these processes all happen behind the scenes so are not customer-facing. So, whereas SOAR could be a differentiator, providing concrete proof to the customer that the MSSP is able to dramatically reduce Meant Time to Detection (MTTD) and Mean Time to Response (MTTR), that's not happening. Instead, MSSPs are only scratching the surface of what it can do.

### Where AI will add value

Similarly, AI-powered cybersecurity solutions have the power to dramatically increase the abilities of the MSSP to manage security processes. The technology lends itself to numerous scenarios because it can be used to analyse large tracts of data and detect anomalies through the use of machine learning. GenAI now takes this a step further because of its ability to not just interpret and predict but generate text and images.

In a cybersecurity context, GenAI can be used in TDIR to increase the speed and accuracy of response. Early research by a team at the Technology Innovation Institute in the UAE has shown that the technology was able to identify 14 attack types with 98% accuracy, for instance, and the expectation is that this will equip SOC teams to respond instantaneously.

Gen AI can also be used to augment endpoint detection and response (EDR) and log analysis. One of the problems many encounter with using a Security and Incident Event Management (SIEM) solution is a high false positive rate due to their success at detecting suspicious or anomalous activity so the challenge that remains is to qualify these alerts.

Looking for correlations of events or observations using contextual threat prioritisation (CTP) can significantly reduce false positive rates. This is where the SIEM uses its detection logic to target tactics, techniques, and procedures (TTPs) in line with a framework such as MITRE ATT&CK. Observations are enriched with the tactics, techniques and procedures (TTPs) identified in the framework but using GenAI these can be further

refined by extracting relevant observation rules from threat intelligence or threat reports.

We can also expect GenAI to be used in other security practices. To help with attack simulations, for example, by mining information from multiple sources to create convincing attack scenarios. To rapidly reverse engineer code and look for vulnerabilities. And it will prove highly effective in a governance, risk and compliance (GRC) context by enabling information to be distilled and reports created and summarised.

### A call to arms for MSSPs

What this means for the MSSP is that they will need to find ways of working with technology partners to develop suitable AI solutions, enabling them to maximise current investment in machine learning and automation solutions. Bringing these elements together will then enable them to offer an end service greater than the sum of its parts because of its abilities to supplement and enhance outputs that give almost intuitive results at speed.

For the MSSP, expanding the portfolio with AI will therefore generate value but it will also enable it to expand its multi-tenant SOC without compromising on service delivery. While it can ingest high data volumes from endpoints and alerts which can be analysed in the SIEM it can also provide detailed customised investigation and remediation advice so that the service is both more efficient and more tuned to the customer.

Looking to the future, Gartner predicts that over 80% of enterprises will be using GenAI technology by 2026, suggesting it's going to become an essential part of operations. During that same time frame, the NCSC predicts the UK will 'almost certainly' see AI increase the volume and impact of cyber attacks and see an evolution in TTPs. Therefore, not only is there a clear demand from the market but MSSPs simply cannot ignore the threat posed by AI attacks. It may seem to go against the grain to look at expanding the portfolio but the reality is that those that fail to do so are liable to be left behind.



## Is the API security market finally maturing?

As with any nascent technology, the channel needed to understand the need for Application Programming Interface (API) security before it could get behind it. While security vendors attempted to seed the market ahead of the curve several years ago, this saw them peak too early. Channel resellers were being told budget was allocated to web application firewalls (WAFs), not API defence, with the two being seen as interchangeable. This caused the channel to question whether they really needed to offer API threat detection and mitigation at all.

**BY ANDY MILLS, VP OF EMEA FOR CEQUENCE SECURITY**



**BUT FAST FORWARD TO NOW** and API traffic has become the dominant form of communication, comprising 71% of all internet traffic in 2023. The WAFs which were being used to defend them have been revealed to be too rigid, using signature-based rather than behaviour-based analysis causing them to struggle to find and block attacks that appear legitimate. Similarly, API gateways, which offer some rudimentary protection such as rate limiting and IP block lists, primarily perform a management function. Both struggle to address the visibility, inventory tracking, risk assessment, and threat prevention requirements needed to adequately protect APIs.

API attack paths have also grown in number and sophistication, leading the OWASP API Security Project to revise its API Security Top 10 of attack types in 2023. It was a step deemed necessary due to APIs having created a massive attack surface and the fact that attackers are now combining attack types to achieve their aims. For instance, whereas before an attacker might have discovered an API that was unmonitored and resorted to business logic abuse, they're now using that API to return user information and then craft a bot driven attack to leverage this access, effectively combining three of the tactics, techniques and procedures (TTPs) identified in the OWASP list (API9, API1 and API6).



## A widening attack surface

Digital ecosystems, increasingly reliant upon this API infrastructure for service delivery, are now finding themselves under attack. In the retail space alone, we observed that bot attacks against APIs increased by 50% during the second half of 2023. In January 2024 there was found to have been a 20% year-on-year increase, with 1 in 4.6 organisations targeted every week.

So, what does this mean for the channel? Principally that demand is increasing and that markets such as retail, telecoms and finance, which have been the brunt of most attacks, are much more receptive to the idea of dedicated API security. There's now been a sea change in the levels of awareness in the market which is now all too painfully aware of the need for API security, and the channel is beginning to take notice.

Those who've been watching the space will have noticed that some of the big players have been quietly adding API to their security portfolio. Notable examples include the acquisition of API security start-up Wib by F5 in February, and Akamai announced the release of API Security in August 2023 and is eyeing NoName to boot.

## Understanding API security

So, do resellers, SI's and VARs now need to look at API security with fresh eyes? It's certainly now a key addition to the portfolio for those involved in the provision of security, cloud and digital transformation services. Many of these will already have related offerings in the form of WAF and DDoS protection and bot protection, making API security a natural bedfellow. In fact, API security should ideally be considered hand-in-hand with bot mitigation because so many of the multi-faceted attacks are automated. Having the capability to provide a solution that defends against both shows the provider has an understanding of the unique challenges associated with API protection. However, such solutions have limitations that attackers have learnt to exploit.

The majority utilise IP address blocking but adversaries have now figured out how to get past this by rotating through IP addresses. Whether the attack is low and slow or high volume, the solution will look to block IP addresses from which an attack originates but the adversary then simply switches to another IP address and continues the attack. In effect, the adversary stays one step ahead of and outpaces or even overwhelms the defence. It's relatively easy to overload a WAF which typically has a limited capacity to cache IP addresses. We've seen instances where an adversary has overwhelmed the system by cycling through over 2million IP addresses in 24 hours.

It's also important to realise that APIs have some unique characteristics that determine how they are

secured. API exploitation can be due to the API going unmonitored, because it hasn't been correctly decommissioned or due to a lack of authentication controls. But equally the API be securely coded and monitored and still be compromised due to business logic abuse. This effectively sees the API's functionality subverted, and it can only be detected using an API security solution that utilises continual monitoring, behaviour-based analysis and TTP fingerprinting. It's for these reasons that API security is a very different beast.

## Compliance as a driver

Crucially, we're now at the stage where the market is set to burgeon further due to another driver: compliance mandates. GDPR already refers to the need to ensure the confidentiality, integrity, availability and resilience of processing systems and services.

In effect, this means any unmonitored APIs involved in data processing would be considered in breach. However, other standards are also now being revised to single out API security.

The latest iteration of the Payment Card Industry Data Security Standard (PCI DSS) version 4, for instance, which is set to become mandatory for most merchants and processors from April 2024 now refers to API security in requirement 6 (Develop and Maintain Secure Systems and Software). When it comes to attacks, section 6.2.4 states the need to mitigate attempts to bypass application features and functionalities through the manipulation of APIs.

With both attacks and compliance ramping up, it's small wonder that the latest Global Market Insights report released in April 2024 predicts these drivers will boost demand and see the API security market surpass \$11bn by 2032, making it a compelling offering for the channel. With even the behemoths looking to get in on the action, it's clear that we're only at the start of that growth curve.

There will, of course, inevitably be some contraction in the space due to this M&A activity, which makes it vital that channel partners look for vendors who can go the distance. Key considerations include whether the proposition aligns with emerging compliance and security demands in terms of TTPs, whether they have a strong presence in those markets that are experiencing attacks (i.e. retail, telecoms and finance) and if their solution is comprehensive enough to offer unified API protection that covers the entire API lifecycle.

Look to see how innovative their product line-up is. Does it offer other capabilities such as bot mitigation or shift-left testing to improve API security pre-production? And how high a priority is given to channel partnerships. Performing these evaluations will enable those channel providers who want to take advantage of a now receptive market to get in and maximise returns with the right partner.



# Boost your MSSP's competitive edge:

## New strategies for leveraging threat intelligence

How to best empower your business clients' cybersecurity with critical cyber threat intelligence.

### BY GROUP-IB

LEADING STATISTICS underpin that the digital threat landscape is growing increasingly complex while the cybersecurity skill gap needed to secure businesses and their perimeters is getting wider. As cyber incidents continue to surge, businesses struggle to adapt to the evolving demands of cybersecurity and resilience.

This evident gap has led to pressing demands on Security Operations Centers (SOCs) and Managed Detection and Response (MDR) providers to offer proactive cyber support: real-time monitoring of networks, systems, and endpoints, threat detection, incident handling, response, and more.

As the Managed Security Service Provider (MSSP) and MDR markets are expected to see double-digit compound annual growth rates in the next several years, adapting and improving service offerings remains essential for MSSPs worldwide to participate in this positive uptick.

A critical component of these improvements is offering precise, actionable, and continuous Cyber Threat Intelligence (CTI) capabilities so businesses can identify the most susceptible risks and defend themselves in the most resourceful and effective manner.

Despite its importance, many MSSPs are not utilizing their CTI capabilities to their fullest potential. In their latest report titled "Hype Cycle for Security Operations, 2023," Gartner mentions, "Many organizations have no formal TI program or dedicated analysts to use TI solutions, like a TIP, or interpret the value from bespoke TI reports. Rather than focus on indicators like IP addresses, domains, and hash values, they allocate too few resources to human-readable or advanced TI solutions."

To help MSSPs leverage threat monitoring for across-the-board incident detection, let's explore three use cases where effectively integrating CTI into your MDR services can dramatically transform a client's security posture, shifting their stance to being proactive rather than reactive.

These use cases emphasize the need for adversary-centric intelligence that provides actionable insights into potential threats, enhancing the accuracy of threat predictions and personalizing security measures to address specific organizational vulnerabilities.

Let's dive into the advanced tactics that can elevate your MSSP and MDR efficiency, ensuring your SOCs can transcend traditional limitations and proactively defend against emerging threats.

How can MSSPs create a high impact through their CTI offering

#### **Use case One: Analytical workbench insights that empower your SOC team**

What are SOC analyst teams' most useful Cyber Threat Intelligence (CTI) sources? CTI has become a staple in the cybersecurity community, empowering analyst teams with information attributed to threat actors. To track these actors easily, you can start with a customized threat landscape dashboard with a single glass pane to monitor attacks. Start gaining and combining the information broader than regular indicators sources, for example, analyzing region-based cyber criminals and nation-state actors, threat



landscape, threat bulletins, analyst reports, and more.

MSSPs need upgraded tools for SOC analysts to investigate and research threats with a visual graph. This graph allows for easy exploration of the relationships between threat actors, their infrastructure, and the tools they use. This visual aid lets analysts delve into details with just a click, speeding up the incident response.

Another unique feature that gives your analysts an advantage during an incident is the ability to detonate suspicious files on the same Threat Intelligence platform and submit them to a reverse engineering team. You don't need the reverse team in-house with the instrument but can outsource that capability. Also, the in-depth analysis of the vulnerabilities targeted by malware and threat actors aids in patching prioritization.

Using these instruments and clearly understanding the threat landscape, you can track actors targeting your clients, their industry, partners, and other entities of interest. This approach enables you to offer managed security services based on which adversaries are most likely to be interested in a specific company or industry. At the same time, you provide tailored and actionable data, regardless of a company's cybersecurity maturity.

#### **Use Case Two: Adding value for your client through insights: leaked and stolen credentials, round-the-clock monitoring**

Proactively tracking client credential leakage can help MSSPs identify potential threats before they lead to significant damage. This approach helps mitigate immediate risks and maintains clients' trust and confidence in your services. Identifying compromised data early, such as user accounts, top-management and VIP personal accounts, payment card information, and breach databases, ensures that security measures can be taken before attackers exploit these vulnerabilities.

Real-time monitoring for public compromised data allows MSSPs to detect threats promptly. Group-IB Threat Intelligence, for example, can create alerts whenever a compromise is detected, covering user accounts, breached databases, and bank cards. These proactive notifications enable MSSPs to immediately secure their clients' assets, preventing potential financial damage and maintaining operations in the first steps of potential incidents.

This boosts client satisfaction and trust. Clients benefit from round-the-clock monitoring, ensuring their sensitive information is constantly protected. This approach strengthens MSSPs' positioning as reliable and proactive cybersecurity partners.

#### **Use Case Three: Advanced competitive advantage with monitoring of dark web and public repository** Adding 24/7 real-time monitoring of the dark web

and public repositories to MSSP portfolios enhances its client security experience. With advanced Threat Intelligence solutions, MSSP can access the industry's largest dark web database and set alerts for clients' mentions in underground forums, instant messengers, and markets. This proactive monitoring, combined with Threat Hunting, helps identify threats early, ensuring timely intervention and prevention.

At the same time, monitoring public repositories for compromised data is equally crucial. MSSPs can detect usernames, passwords, bank card details, Trojan configuration files, and logs published on sites like Pastebin and GitHub. Group-IB Threat Intelligence alerts MSSPs to these compromises, allowing immediate response and risk mitigation.

### **Recommendations**

These advanced Threat Intelligence use cases enable MSSPs to track relevant risks, prepare clients to counter threats in real-time, and help prepare the customer against threats "in the wild." Offering continuously advanced insights and proactive threat management strengthens client confidence and ensures robust protection against emerging threats.

As trusted partners in helping businesses with threat exposure and risk management, MSSPs should remain steadfast in addressing and managing evolving cybersecurity challenges. For more tips on making your MSSP and MDR more efficient, look at our resource.

A non-negotiable need for businesses, and in turn, MSSP providers, is contextual, relevant, and actionable threat intelligence to deliver industry-leading services to their clients. To achieve swift TI activation and seamless integration into your security processes and services, leverage Group-IB's proprietary Threat Intelligence. The platform provides updated critical threat intelligence, constantly enriched by unique research from Group-IB threat analysts and our global Digital Crime Resistance Centers (DCRCs), which act as first response units to effectively track and combat active local threats.

Learn more about enabling Group-IB Threat Intelligence capabilities to ensure real-time detection and response, improve mean time to action, reduce inconsistencies, and increase reliability.

If you're looking to completely revamp your SOC capabilities, start by learning about implementing or updating your CTI program with our resourceful eGuide: [The Art of SOC](#).

Join our dedicated Telegram channel (to get an invite, email us at [mssp@group-ib.com](mailto:mssp@group-ib.com) or contact our experts to learn more about Group-IB's complete portfolio of cybersecurity products, services, and MSSP programs.



## Strengthening cybersecurity resilience in a changing world

The data tells us that more and more customers are turning to outsourced security management because they simply can't keep up with the pace and sophistication of cyberattacks. And they expect that the expertise of their MSSP partners will detect and stop attacks quickly.

**BY HUGO BISHOP, REGIONAL SALES DIRECTOR, NORTHERN EUROPE, STELLAR CYBER**

MANY MSSPs have evolved their SOCs over several years, amassing as many as 30-50 discrete cybersecurity tools, only a handful of which are used by any one analyst. Detecting and responding to complex, multi-vector attacks in this environment requires swivel-chair integration of disparate signals – essentially two or more analysts correlating signals they've found. An MSSP may be evaluating between 10 and 100Tb/day of data, with analysts who are buried in alerts and unsure which they should be prioritising; it's no wonder many large data breaches have taken weeks or months to discover.

The fundamental challenges boil down to this:

- **Reducing** the amount of data presented.
- **Correlating** multiple, related threat signals to

reduce the time analysts need to detect complex attacks.

- **Guiding** analysts about how best to address threats, further reducing response time.
- **Automatically stopping** many threats by communicating with firewalls and other systems.

Today, dozens of the largest global MSSPs have adopted new SOC platforms that reduce manual data interpretation, making it faster and easier to spot threats. With the right platform, these organizations have been able to reduce Mean Time to Detect (MTTD) by as much as 8X, and reduce Mean Time to Remediate (MTTR) by up to 20X.

Here are some essential considerations for





choosing a SOC platform that eliminates swivel-chair integration and detection delays.

### Built-in functionality

A good SOC platform should reduce deployment time. It significantly helps if a range of key cybersecurity tools (NG-SIEM, NDR, and UEBA, for example) are built into the platform. Getting all of these in one console under a single license reduces costs as well as training time. Today's eXtended Detection and Response (XDR) platforms are a good example.

### Data integration

MSSPs monitor and secure networks and other IT systems by collecting and interpreting data from throughout the infrastructure, and it's extremely rare to have a stack of security tools that shares a common data format. But an effective SOC platform should easily integrate data from any source, including not just firewall or server logs, but EDR systems, identity management systems, clouds and applications. Then, it should automatically normalize that data into a common format for storage in a data lake. Unlike Closed or Anchored XDR platforms, which typically integrate only with discrete tools from the same vendor, Open XDR platforms are built to integrate with most or all third-party security tools, eliminating vendor lock-in, and giving visibility and protection across the whole attack surface.

### Detection

An effective platform must evaluate the ingested data and automatically detect common threats. This eliminates 90% of manual detection by converting terabytes of data to thousands of alerts per day. The leading SOC platforms have incorporated AI technology, specifically Machine Learning (ML), to accomplish this.

### Signal correlation

It is impossible for human analysts to quickly correlate related signals from disparate consoles.

The SOC platform should automatically analyse collected data and correlate related signals to reveal multi-vector attacks, using a combination of customizable playbooks and Graph Machine Learning (Graph ML) to detect suspicious behavior. Ideally, the platform should then also prioritise attack incidents in order of severity.


### Analyst assistance

A strong MSSP SOC platform can further speed resolution of complex threats by using Generative AI (Gen AI) to provide instant responses to analysts' questions. This capability provides further operational efficiencies by reducing the number of analyst decisions to 10-100/day and cutting threat response times by up to 400%. For example, an analyst can ask, "Show all the incidents where data was exported between 12-9AM," or "Which emails went to domains in Russia?"

### Hyper automation

A few SOC platforms are now adopting Hyper Automation features as well. These platforms use ML and bidirectional integration with security infrastructure systems to shut down attacks. For example, the platform might notify a CRM platform to stop a user from sending email and attachments to Russia, or cause an identity management system to invalidate a user's spoofed login credentials.


The speed and sophistication of cyberattacks accelerates unabated, the complexity and array of cyber security tooling continues to spiral, and there aren't enough security analysts in the world to keep up. In fact, there are more than 3 million security jobs going begging worldwide due to a shortage of analysts. To prosper in this environment, MSSPs must adopt AI-driven, highly integrated SOC platforms that reduce this complexity, deliver cost and operational efficiencies, and enable fast and accurate detection and response for their analyst teams.



# ROUNDTABLE

CONNECTING THE CHANNEL PARTNER ECOSYSTEM


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



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

**Cost: €5995**

**Contact: Jackie Cannon**  
jackie.cannon@angelbc.com





## Exploding AI demand creates new opportunities for UK MSPs

In 2024, demand for AI has continued to rise to unprecedented levels across the UK. In fact, according to a new report, over 80% of organizations plan to expand their use of AI in the next year.

**BY CHRIS SHAW, MANAGER UK CHANNEL, AVEPOINT**

THIS EXPLOSION of demand has led to substantial new investment in AI hardware and software. It's also created exciting new opportunities for MSPs, with £118 billion in available services projected to be on the table, per Jay McBain of Canalys.

As the AI revolution accelerates, more UK MSPs are engaging with AI to better serve their clients. This means providing both the technical support to enable AI, as well as the technical support systems that are necessary for its continued success. In this article, I'll talk about how and why MSPs are helping end users do more with AI all around the country and world.

AI demand is broad across UK industries, regions. Government research recently found that 68% of large businesses in the UK use at least one

AI technology. According to the 2024 AI and Information Management Report, ChatGPT is still the most popular AI tool, followed by Microsoft Copilot and then Google Gemini. Many other organizations, meanwhile, have created bespoke tools that don't require software from an external vendor.

With use and availability expanding rapidly, it's become clear that demand for AI transcends industry and region, which is good news for MSPs and their customers. Research finds that most AI-adopting organizations are using the technology to streamline business operations (64%), enhance customer insights (57%), and enact cost reduction and resource optimization (55%). These activities don't just apply to one industry – they're broadly applicable objectives that work across industries and regions.



As more businesses and organizations adopt AI, they'll need greater support to get the technology running to its fullest, and that's where MSPs come in. By providing essential services and support systems, MSPs can help their customers succeed while making significant advancements toward their own business goals.

### Information management is critical

Research shows that organizations with a mature information management strategy are 1.5x more likely to realize the full benefits of AI, which highlights the importance of information management to AI-adopting organizations. And yet, in spite of this, over 50% of companies are using AI without an acceptable use policy in place – a basic component of any information management strategy.

In addition, only 5% of organizations put governance as part of their cybersecurity strategy. This suggests that many companies have not properly prepared their organizations or enterprise data for the arrival of AI.

To craft mature information management strategies, companies should implement automated processes, consistent classification, and structured governance across the board, which means a curtailment of manual processes, inconsistent classification, and ad-hoc governance. In the UK, MSPs can help aid

this transition by providing customers and end-users with the technical support and support systems that they need to ensure that AI tools run smoothly.

Cybersecurity concerns linger – MSPs can help. When it comes to adopting and using AI, more organizations are paying attention to AI-related cybersecurity concerns. While AI is a powerful tool, it does have risks that can be exploited by bad actors.

Data breaches and exposures, privacy violations, and cybersecurity attacks all loom as potential sources of risk. For example, 45% of organizations experienced at least one instance of data exposure during AI implementation. By providing customers and end-users with complete support and technical systems, UK MSPs can help ease data exposure concerns and limit cybersecurity risks before, during, and after AI implementation.

Moreover, AI software vendors understand the substantial value of working with MSPs and are doing so in greater numbers. According to Canalis, MSPs now operate in a £400+ billion market, which means that they have a greater role than ever to play in both the evolution of AI enterprise technology, and the evolution of enterprise technology more generally. As AI becomes even more widely and maturely used across industries, the opportunity for MSPs and their customers will only continue to grow.

## MSP ROUNDTABLE

CONNECTING THE CHANNEL PARTNER ECOSYSTEM

Not every discussion is a  
**heated debate...**



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

**Cost: £5995**

**Contact: Jackie Cannon**  
jackie.cannon@angelbc.com

ANGEL  
EVENTS





## The responsible use of AI: a step into the future for MSPs

Artificial Intelligence (AI) is everywhere. It's a topic clients often ask me about, and there's no escaping the fact that it's here to stay. Managed Service Providers (MSPs) are at the forefront of innovation, constantly adapting to meet the ever-changing needs of our customers. And AI is no longer just a buzzword, it's going to shape the future of our sector.

**BY IAN WHARTON, TECHNICAL ARCHITECT AT PRINCIPLE NETWORKS**

GENERATIVE AI - AI systems capable of creating content - has already become part of everyday life. Answering questions, sales prompts, drafting emails, writing articles and generating images, you name it, it can probably do it. However, it's not all positive.

Conversational AI leaks - the loss of data where chatbots are involved - are on the rise and now pose an increased threat to organisations and their customers. Another challenge is shadow AI practices, where staff start using unsanctioned AI tools and further expose the business to threats, or introduce AI hallucinations - misinformation generated by AI models - into their work.



It all raises questions about whether MSPs need to restrict access to AI tools, or are there responsible ways to use them?

### Navigating a complex landscape

Eighteen months ago, most people had not heard of tools like ChatGPT, Gemini or Microsoft Copilot, and now they are used by millions, not just socially but often in a work environment. While there is no doubt that generative AI offers huge potential to help employees and organisations become more productive, taking care of lots of administrative and process-driven tasks so that we don't have to, we are still at a point in time where these tools do not have the proper vetting and control mechanisms

in place. Without the necessary governance and security features, generative AI poses more risks than there are benefits.

For example, in May 2023, electronics giant Samsung reportedly banned generative AI tools after discovering an engineer accidentally leaked sensitive internal source code when uploading it to ChatGPT. The concern for organisations is that data shared with AI chatbots gets stored on external servers owned by companies operating the service, and there is no easy way to access and delete it. Generative AI tools store chat histories by default and use these conversations to train future Large Language Models (LLMs). Users can change this setting manually, but it still needs to be clarified if it can be applied retrospectively, leaving organisations vulnerable.

On the one hand, these platforms offer huge potential for employees to collaborate and become more productive, but on the other, they pose a great threat for compromising data integrity and customer confidentiality, leading to non-compliance and possibly fines.

Until appropriate guard rails can be put in place, it's recommended that MSPs implement stringent access controls, firstly to ensure only authorised individuals can access sensitive information, which is best practice in any security posture, but also restricting access to the tools themselves. While nobody is under any illusion that one day we will be in a much better position for safe and compliant use of these types of AI tools, until then it is vital to prioritise data governance, transparency and accountability to protect organisational and customer data.

### The responsible use of AI

Let's not just focus on the negative though. AI will also be the fastest way to monitor and identify cybersecurity threats automatically, removing the need for human intervention and speeding up the remediation process.

For example, one of the biggest challenges for MSPs is the sheer volume of data passing through networks and applications. How do security teams guarantee this data remains secure, private and out of harm's way? Implementing AI algorithms to analyse aggregated data from various sources, including network devices, endpoints and security appliances, can transform how organisations detect and respond to cybersecurity threats.

AI-based security tools are adaptive and self-learning. As your network environment evolves and new threats emerge, AI algorithms can adjust their behaviour and defences, leveraging feedback loops to improve and continuously scale.

AI will also continuously monitor data to detect suspicious activity, identify threats and prioritise

security alerts based on their severity and potential impact, allowing security teams to focus their resources on addressing and resolving the most critical issues.

One of the most significant benefits of AI-based security tools is they provide IT managers with reliable, evidence-based information. The ability to analyse patterns and anomalies in network traffic means the AI can alert IT personnel of the threats that require human review, and this is getting better at an exponential rate. Now, it's a case of learning to read and analyse the AI's recommendations appropriately, as well as manage and refine its rules to train it according to your purposes.



### It's a marathon, not a sprint

Delivering effective AI services requires a holistic approach, encompassing authentication, access rights management, data tracking and leakage prevention. Implementing mechanisms such as multi-factor authentication and biometric verification is the first line of defence when trying to prevent unauthorised access to services and data. The same approach should be applied to the use of AI tools. Managing employee access rights ensures the right people have the right permissions to access the tools needed to do their jobs. Understand who will be using them and why. Integration with existing infrastructure is another crucial consideration, as you must ensure compatibility with current systems and processes.

If we're to use AI responsibly, adhering to regulatory compliance is non-negotiable. Addressing mitigation bias, fairness, and accountability are central to responsible use. It's imperative to evaluate the cost of implementing and maintaining AI-based tools against the potential benefits and return on investment in terms of threat detection and response capabilities.

AI is coming, but you should remain in control of how it is safely introduced into organisational processes. An environment designed for the responsible use of AI keeps customer data secure and lays the foundation for future success. While there is a lot to get excited about, for now MSPs should be adopting a caution-first approach.



# How Green is your MSP?

Why sustainability is critical to future growth.

BY ANDY VENABLES, FOUNDER AND CTO AT POPX



**ADOPTING ENVIRONMENTAL, Social and Governance (ESG) protocols** has become the norm for many organisations. It goes beyond regulatory compliance and enters the realm of corporate responsibility. For MSPs, this means providing the most reliable ICT services whilst also being responsible and forward-thinking about minimising the environmental impact. Creating more sustainable managed services is a collective responsibility, so here we look at some of the innovative ways that this can be achieved.

Automating value from what you already have. Increasing resource capacity without hiring more people is the holy grail for MSPs but this is easier said than done. Technology and automation are the founding principles for achieving this but not every MSP has the latest systems and tooling in place for comprehensive Service Management. There needs to be an overall shift away from managing tasks and inputs to creating workflows that ensure routine tasks are done accurately and efficiently. It is much easier, safer and cost-effective to scale your operations with workflows, rather than recruiting more and more staff as you grow your customer base.

Using workflow automation, routine tasks such as ticket routing, issue escalation, and client onboarding can be streamlined, freeing up valuable time and resources for more strategic initiatives. Additionally, standardised workflows maintain consistency in service delivery, so that best practices are followed across all client engagements. Leveraging workflows allows improved collaboration and communication



between your teams. By defining clear processes and assigning responsibilities within automated workflows, team members can easily track the status of tasks, identify bottlenecks, and collaborate more effectively to resolve issues.

This enhanced visibility into operations helps you identify areas for improvement and continuously optimise processes. Centralising documentation and knowledge within workflow management systems, your MSP can facilitate smoother transitions during staff turnover and ensure that institutional knowledge is retained within the organisation. Ultimately, by embracing workflow automation, MSPs can operate more efficiently, deliver a better service to customers and drive business growth.

**Machine Learning and Artificial Intelligence**  
As well as leveraging Service Management platforms like ServiceNow, MSPs can also harness the power of Machine Learning (ML) and Artificial Intelligence (AI). One interesting way these techniques can contribute to environmental sustainability is through predictive analytics. By analysing historical data that reveal patterns, algorithms can forecast future service demands, enabling MSPs to optimise resource allocation and minimise energy consumption. This proactive approach helps reduce unnecessary server loads, cooling requirements and overall energy usage, ultimately lowering the carbon footprint of an MSP's operations.

These predictive powers can accurately identify issues early or before they even happen. For example, alerts can be raised to carry out proactive



maintenance on equipment, reducing the probability of system outages and emergency repairs, which cause unnecessary customer frustration and excess resources to fix.

AI-enabled insights and decision support can empower you to make data-driven decisions that prioritise sustainability by identifying inefficiencies and implementing targeted improvements to reduce waste and environmental impact. For example, algorithms can analyse data from various sources, such as energy consumption metrics and service utilisation patterns, to identify opportunities for optimisation and resource conservation.

### Staying lean

The best MSPs take the approach of an athlete. They stay lean to avoid poor performance because they need to be agile and streamlined, as this will help prevent system outages from occurring. To improve resilience, staff need to be ready and well-trained in multiple disciplines to prevent them from being over-staffed, encouraging operational efficiency.

From a lean technology perspective, running physical servers and hardware on-site requires a lot of power. To manage increased electricity usage, MSPs can adopt virtualisation to help reduce the number of servers. In some cases, cloud technologies from third-party vendors may be available to help minimise local energy consumption, although it could be argued that this simply moves the energy burden somewhere else. However, by consolidating consumption in this way it is more likely the cloud provider can find more efficient management methods that being centralised allows.

Cloud and SaaS providers of IT applications and infrastructure are ideally placed to scale their platforms and optimise them based on a larger pool of customer demand, reducing over-provisioning

To manage increased electricity usage, MSPs can adopt virtualisation to help reduce the number of servers. In some cases, cloud technologies from third-party vendors may be available to help minimise local energy consumption, although it could be argued that this simply moves the energy burden somewhere else

and wastage. It is important to remove obsolete technology from your operations, but it is only one part of the strategy. Once again, we suggest a deep dive into your operating model and analyse what can be optimised, enhanced or decommissioned and swapped out for a better solution.

### Embracing a sustainable future

MSPs that adopt green practices will likely see benefits far beyond energy savings. These include improved brand image, attracting eco-conscious customers and creating new services. As people want to work for socially and environmentally responsible companies that adopt the latest technologies and techniques, this will help boost employee morale and attract top talent.

The shift to greener practices is not just about being sustainable or following rules, it's about future proofing MSPs. As the world looks to modern working practices that embrace cleaner and lower energy-dependent solutions to take care of our daily business needs, sustainability is no longer a nice-to-have but a must-have.

## MSP ROUNDTABLE

CONNECTING THE CHANNEL PARTNER ECOSYSTEM

### Not every discussion is a heated debate...

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

Cost: £5995

Contact: Jackie Cannon  
jackie.cannon@angelbc.com





# 5G Private Networks vs Wi-Fi:

## What channel partners should know

For years, cellular networks and Wi-Fi appeared settled into their areas of dominance. But in some enterprise use cases, upgrades to cellular technology have handed companies unprecedented choice.

**BY DARRYL BRICK, VP PARTNER SALES AT CRADLEPOINT**

FOR PARTNERS who've been around awhile, the 5G vs Wi-Fi debate may seem a little tired. However, the debate persists, and technologies continue to co-exist, as each have as both Wi-Fi and cellular continue to evolve. Wi-Fi is a type of wireless local area network (WLAN) that is favored for supplying wireless connectivity to the home, office, campus and other facilities ok with “best effort” connectivity in many environments but best suited indoors. Cellular connectivity is the dominant player outdoors, on mobile phones and many other devices when Wi-Fi and other connectivity options are unavailable.



Recent events and connectivity ecosystem evolution have triggered significant changes to the dynamic between technologies. As Wi-Fi and

cellular networks have been upgraded through new standards releases, the roll out of 5G has brought increased capacity, coverage, mobility, speeds, and lower latency. Meanwhile, Wi-Fi 6 is getting closer to cellular with increased capacity, coverage, and higher speeds. Both have inherent strengths and weaknesses.

Another important shift is that, cellular has become an attractive alternative to Wi-Fi for enterprises — specifically for those looking for greater support for business critical applications, wanting complete control of their network. This is evident in the rise of private cellular networks, PCNs, among today's enterprises. Helping drive this growth in enterprise PCN are changes to spectrum policy, including the allocation of licensed spectrum for enterprises.



With the increased availability of licensed or shared spectrum, enterprise companies can operate their own PCNs and exercise complete control over the network, and as such will be looking for partners who can support them in this journey

With the increased availability of licensed or shared spectrum, enterprise companies can operate their own PCNs and exercise complete control over the network, and as such will be looking for partners who can support them in this journey. As the enterprise evolves, three major wireless technologies are increasingly co-existing: public cellular, private cellular and Wi-Fi.

However, thanks to PCNs and the enhanced performance they provide in the form of increased coverage, mobility, reliability, security, and predictable network performance — enterprises will be looking for partners who can offer them the choice of these technologies depending on their need.

### Why are PCN deployments increasing?

So, why may some enterprises be opting for private 5G or LTE over Wi-Fi? One of Wi-Fi's limitations includes reliability. Because Wi-Fi operates on unlicensed spectrum, it may be available but not necessarily useable because of signal interference, traffic congestion or a minimal coverage area. In terms of security and capacity, Wi-Fi also comes up short when compared to a private 5G network. For example, private cellular networks can eliminate credential-based attacks thanks to SIM-based authentication. Network users must have approved physical SIMs or electronic SIMs will be able to access the network, giving enterprises more control over who enters their network. Also, even if a bad actor gets their hands on a device with an approved SIM, they'd only have access to the portions of the network for which that device is approved.

In terms of mobility, cellular networks are deterministic — meaning the network determines how to assign cellular clients to the cellular network access points (APs), and when to handoff to another cellular AP based on signal strength, QoS (quality of service) standards assigned by the enterprise network administrator, and other identifiers. Since Wi-Fi networks are not deterministic, this vastly improves the network reliability for mobile devices that roam between cellular APs in a PCN.

Providing connectivity for large areas isn't easy. When it comes to coverage, in many situations private cellular networks make a lot more sense as well. Often, private cellular can cover 10x the space outdoors compared to traditional Wi-Fi. For example, Ericsson is working with the Port of Tyne to provide site-wide connectivity through a cellular private

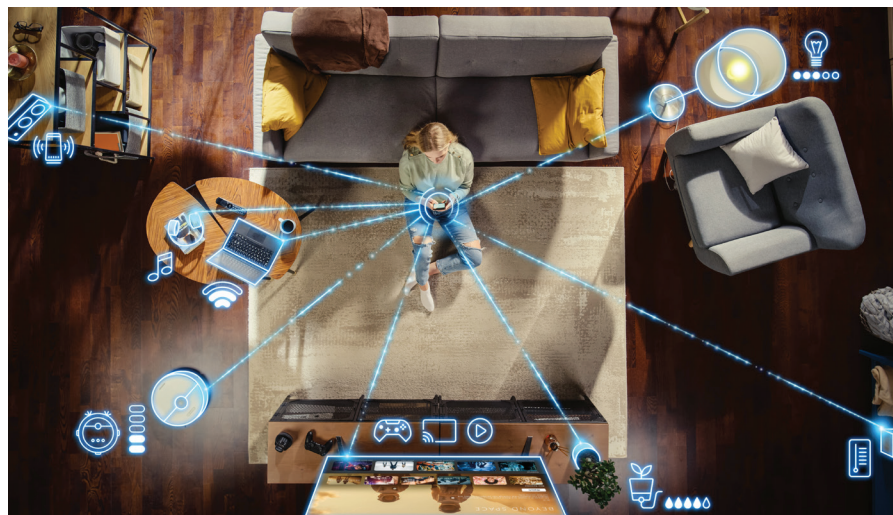
network which will support autonomous navigation, remote crane operations, connected drones and wearable technology.

Then, there's the question of reliability. Many warehouses and industrial environments now use sensors and other devices to connect or have more visibility into their operations and machinery requiring the constant sharing of data between machinery or to a database. When it comes to automation and robotics, the lower latency that private 5G offers means greater control for enterprise users. Then there's the way 5G combines with edge computing, which provides near real-time processing by bringing data processing to the point of data creation, such as a factory or warehouse floor instead of the cloud. The low latency necessary for real-time data transfer, the control of the network across which that data transfers, and the inherent security a PCN provides that data is why PCNs are more reliable.

### Simple and secure

Lastly, what's become increasingly difficult for the enterprise to ignore is that with the maturation of private cellular solutions, the current value proposition for Wi-Fi to support business and mission critical applications continues to shrink.

PCN solutions are not only more comprehensive but enterprises will find it's easier than ever to deploy and manage them after deployment. Meaning, it is critical channel partners take note of its benefits now before they fall behind the competition in offering this dynamic technology.







## Six months on – how has the UK’s first charter for ITMSPs fared?



Until recently, there was no professional charter or recognised standard to guide UK-based MSPs in terms of best practice. For an industry made up of more than 10,000 businesses, employing more than a quarter of a million people, this was a significant gap.

**BY BEVERLY BOWLES, HEAD OF CYBER AT SCOTLANDIS**

WHEN THE DESIGNERS of Monopoly were deciding what to include on their shiny new board game, it probably seemed like a no brainer for water and electric to be the featured utilities. Two services vital to the success of any city. However, if the board was being designed today, there’s every chance that data centres, connectivity or even IT service providers would be included in those squares – so vital are they to the success and growth of a modern economy.

OK, OK, so maybe Hasbro won’t be rushing to redesign the iconic board, but the point stands. Reliable, secure IT services are absolutely vital. Not just for businesses but for the success of the wider, digitally fuelled economy. And with more and more businesses turning to managed service providers (MSPs) to supply these services, it’s an industry that carries a lot of responsibility on its shoulders.

A fact that makes it all the more remarkable that, until recently, there was no professional charter or recognised standard to guide UK-based MSPs in terms of best practice. For an industry made up of more than 10,000 businesses, employing more than a quarter of a million people, this was a significant gap.

Although it was a gap others had started to look at, they often aligned to Cyber Assessment Framework guidelines. This was all well and good except for the fact that by adhering to such a high standard it would essentially have excluded all but the very largest ITMSPs operating in Scotland.

That's why, six months ago, following the rapid growth of our IT managed services community and lots of feedback from our members, we decided to develop our own charter for MSPs. One that was fit for purpose and provided a practical, helpful guide for those operating in the industry.

This wasn't something we could have done without the support of ITMSPs across Scotland, as well as funding from Scottish Government, and the spirit of cooperation was absolutely vital throughout the process. As the first of its kind in the UK, the charter provides a framework that establishes the standards that customers should expect of IT managed service providers.

Since we first started developing the charter, we've worked closely with IASME and are grateful for their continued support. Moving forward, we look forward to also engaging with NCSC and UKC3 as well as other groups representing MSP's, like COMPTIA, Network Group and Cyber Resilience Units. Forging these partnerships will help us continue to raise the bar and enhance cyber resilience across the UK and throughout the supply chain.

We now have more than 20 MSPs who have signed up to the charter and the number is increasing all the time. The feedback along the way has been largely positive and constructive but has informed tweaks to the charter and how it's used.

We've seen an encouraging and consistent improvement in overall standards, especially when it comes to areas like cyber security and data protection. It's also allowed us to develop a better understanding of emerging threats and areas where some members may be vulnerable.

Working together, we've developed a comprehensive set of questions for customers to ask potential managed service providers to help ensure they get the most appropriate service. We're also creating a categorisation based on the ScotlandIS capability directory to ensure there is a clear guide, detailed in layman's terms, to the services that are available, so they can choose the most appropriate service.

All of this is aimed at giving businesses the information they need to make an educated choice that means they are signing up to the right service for them.

Any minor challenges we've encountered have been largely overcome as a result of the community working closely together. We aren't interested

in pricing models and product lists; we're solely focused on helping the sector provide a better service to customers and protecting our members from bad actors. There is a recognition of how important it is to raise standards within the sector and build cyber resilience throughout the supply chain as well as the benefit of joint working to achieve this.

It hasn't all been smooth sailing though and we've certainly learned a lot along the way. For example, balancing a desire to be inclusive with the necessity to maintain a minimum standard is always tricky. We also need to ensure that we're not just creating an echo chamber of like-minded organisations that all agree with each other.

One thing's for certain - the last six months have certainly been informative. Launching the UK's first charter of this type certainly hasn't come without its challenges but we're confident that the industry has benefited from the process and customers are getting a better, less confusing service as a result. We're already in conversations with similar organisations across the UK about expanding the project and it's exciting to think that, before long, the Scottish blueprint may be rolled out across a much larger footprint.

As more organisations come on board and the charter is adopted across other regions, it is vital that we ensure it continues to meet the needs of all signatories. Ultimately, this will mean expanding the working group and adopting an assurance process to ensure that all members meet the criteria of the standards within the charter. This will be a challenge but we're very much looking forward to working with other organisations like UKC3, Welsh Cyber Resilience Unit and Northern Ireland Cyber Cluster to achieve this.







# Thriving in tough times:

## Why managed services are a business imperative

In today's economic climate, with inflation and interest rates improving but still remaining high, businesses face significant financial pressures, compelling them to prioritise the escalating costs of technology in their strategic planning. The challenges are complex, covering not only the initial expense of new implementations, but also the ongoing cost of managing the technology through its entire lifecycle.

**BY CHARLES COURQUIN, DIRECTOR, SYMATRIX**

THE INTEGRATION and harmonisation of disparate systems, coupled with the costs of operation, maintenance and upgrades, further strains budgets. Enterprises must navigate this intricate landscape, balancing innovation and operational efficiency with stringent cost control to ensure they remain competitive and resilient in an ever-evolving digital world.

### The skills dimension

When it comes to technology expenses, one of the biggest issues many businesses face is associated with the people they have in place to support it. IT

skills shortages and recruitment difficulties have become a costly challenge across multiple business sectors. Many organisations lack the internal capability to drive their organisations forward because their IT teams don't have the right skills and are finding it difficult to acquire them.

That's a problem that is unlikely to ease soon. As the baby boomer generation retires, for example, there is a lack of experienced workers in many areas of the economy, with manufacturing, construction, and healthcare among the sectors worst affected. Alongside this, technology is constantly evolving





and therefore the skills required to work with it are becoming increasingly complicated.

As a consequence, recruiting new people remains challenging and it is costing businesses considerably. Symatrix recently polled 200 IT decision-makers, working for large businesses, all of whom are involved in buying or managing technology for their businesses.

Over three-quarters of respondents (77%) said their organisation's IT recruitment costs have increased over the past three years – and nearly half (45%) said costs have increased by more than 10%.

Nearly a quarter (22%) estimated that IT skills shortages are costing their businesses more than £100,000 a year in recruitment fees, temporary staffing, increased salaries, investment in employees starting out their careers and colleagues bringing new starters up to speed over time.

Vacancies are still high and companies struggle to fill them quickly which means that their costs ramp up. The survey found 27% of companies take more than two months to fill a vacancy today, which is up on the figure for two years ago.

Despite moving past the pandemic's job market disruptions, recruitment challenges persist, escalating businesses' direct and indirect expenses through prolonged vacancies and reduced operational capacity.

### Finding a way forward

In real terms, managing IT systems using internal resource is expensive for many businesses. More than a third (36%) of respondents whose businesses manage at least part of their IT systems in-house, are spending more than £250,000 a month on doing so. Moreover, 42% of those managing IT fully in-house said they find the process of receiving vendor updates in the cloud to be costly overall. And that is likely to be at least in part down to skills shortages.

The use of managed services will be key as businesses strive to make cost savings in the current difficult economic times. Beyond pure cost savings, however, a managed services approach is also likely to help organisations to achieve enhanced value over time. When asked about their previous experience with enterprise software, 100% of respondents that were using managed services only had achieved a return on their investment and a higher proportion of those respondents also recorded a return on investment (RoI) within a year compared to those managing IT fully in-house.

61% of businesses currently running their IT in-house believe they could save more than £50,000 per year if they were to use a managed services provider, which begs the question why they have not moved to managed services already? In fact, over three quarters (76%) of businesses who are using



managed services estimated that they had saved more than £50,000 a year since they started to use the outsourced capability.

It is further evidence that with a higher return on investment and quicker realisation of benefits, the use of managed services holds the key to thriving in the current challenging economic landscape, and beyond.

As businesses navigate the complexities of the current economic environment, leveraging expertise outside the organisation emerges as a strategic imperative, enabling organisations to not only survive but to thrive and innovate. This shift not only promises immediate financial relief but also positions companies for sustainable growth and competitive advantage in the future, highlighting the importance of managed services as a critical component in the modern business landscape.

In real terms, managing IT systems using internal resource is expensive for many businesses. More than a third of respondents whose businesses manage at least part of their IT systems in-house, are spending more than £250,000 a month on doing so. Moreover, those managing IT fully in-house said they find the process of receiving vendor updates in the cloud to be costly overall

## Three ways Managed Services help SMEs **THINK BIG**

Managed Services are rapidly growing in popularity across the IT sector, becoming fundamental for businesses to improve efficiency and infrastructure. With the rapid pace of technological advancements, internal IT teams aren't equipped to meet the growing demands of the online world, meaning it is becoming increasingly beneficial for SMEs to outsource a reliable delivery of IT.

**BY ADAM GACA, VICE PRESIDENT OF CLOUD SOLUTIONS AT FUTURE PROCESSING**



HOWEVER, in comparison to their larger counterparts, SMEs face tougher constraints. According to the World Economic Forum, 67% of small businesses are fighting for survival, and require diverse support mechanisms to stay competitive. Therefore, it remains unsurprising that over 85% of organisations recognise the importance of adopting new technologies to drive transformation and long-term growth. Managed Services offer a cost-effective solution, enabling SMEs to increase efficiency and business output, based on their demand.

### **Enhanced agility**

In simple terms, a Managed Service is a comprehensive IT support model, which handles

all internal processes, infrastructures and applications to ensure consistent and reliable delivery of IT. However, with continued business growth, IT inefficiencies can quickly rise to the surface, which for SMEs with typically traditional, stretched resources can prove overwhelming. Utilising Managed Services creates automated improvements and frees up operational resources to focus on priorities and increase operational agility.

For instance, Managed Service Providers (MSPs) can implement and manage large volumes of infrastructure by applying the necessary tools to ensure a smooth running IT service. This is achieved via remote management and cloud-based services, eliminating downtime and freeing up internal resources, allowing SMEs to redirect their focus to their main priorities.

By adopting digital tools, SMEs can unlock their full business potential and enhance agility by exchanging resources spent on stretched IT infrastructure and implementing them elsewhere. Managed Services can also scale business support through upskilling professionals within specialised areas, reducing any existing skill gaps, and improving business operations.

### **Boosting efficiency through Managed Services**

In the turbulent landscape, SMEs need to remain as efficient as possible to ensure they maintain a competitive advantage, which is challenging with comparably less resources than bigger companies.



Building an efficient system is imperative to SME's survival. Using new technology can propel the business to the next level, alongside the major competitors. The offer of flexible models through a Managed Service tailors the extent of collaboration necessary to support SME transformations, ensuring they remain as efficient as possible.

Each model offers a wide range of involvement options, from a specialised service retained by the business, a co-managed service and a fully remotely Managed Service. This allows SMEs to tailor specific IT models appropriate for their individual needs. As a result, the service provider can build a fully customised solution for maintenance and support of outsourced processes.

SMEs who have onboarded Managed Services have found an increase in production processes by 26% as a result of leveraging technology at scale. Using the service to transform long term digital roadmaps and infrastructure, can aid SMEs in meeting high-level objectives through increased productivity and efficiency.

### Building technology resilience and staying current with IT trends

It is becoming increasingly difficult for SMEs to keep up with emerging technologies, where approximately 25% of SMEs cite this as a top challenge impeding business growth. Managed Services, however, help SMEs build resilience by maintaining a competitive edge in the market, without stretching resources to sustain continued growth.

Following the pandemic, a surge of digital security risks affected businesses, with increased opportunities for hackers to exploit SMEs' lack of appropriate security measures. This spike in cyber crimes calls for an increase in provisions, education and infrastructure for businesses, which can come

Using the service to transform long term digital roadmaps and infrastructure, can aid SMEs in meeting high-level objectives through increased productivity and efficiency

at a large cost, not available at the disposal of SMEs without a competent and up-to-date service provider.

As we continue to embrace new technology, the next best is already taking over, making it impossible to maintain IT resilience, especially for SMEs who may be using outdated software. Businesses using outdated software are vulnerable to cyber attacks which negatively impact productivity, reduce compliance to industry regulations, and make it more difficult to scale and sustain the business.

A Managed Service is a cost-effective solution which enables SMEs to adopt the latest technology, improving their cybersecurity and providing added flexibility, through enabling businesses the freedom to purchase exactly what they need.

### The bottom line

Onboarding a Managed Service removes several issues from the equation and is the simplest way to ensure all hardware and software is maintained at its highest running level. Working behind the scenes to ensure businesses are protected, SMEs have the confidence to transform - at a fraction of the cost. In addition, keeping on top of advancing technology is the key to enabling SMEs to compete with industry leaders, providing a future-proof platform with stronger resilience, strategic value, and competitive advantage.

## MSP ROUNDTABLE

CONNECTING THE CHANNEL PARTNER ECOSYSTEM

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



- Based around a hot topic for your company, this 60-minute recorded, moderated zoom roundtable would be a platform for debate and discussion
  - Moderated by an editor, Phil Alsop, this can include 3 speakers
  - Questions prepared and shared in advance
- Cost: €5995**

**Contact: Jackie Cannon**  
jackie.cannon@angelbc.com

ANGEL  
EVENTS