MSP CHANNEL INSIGHTS

ISSUE III 2026

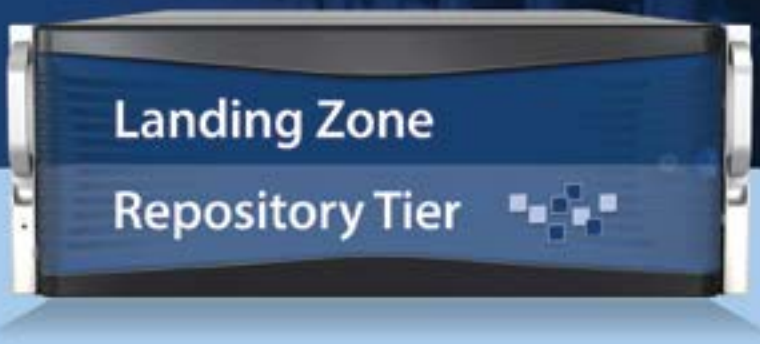
AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION

MSP-CHANNEL.COM

WOMEN IN THE CHANNEL: ADVICE FROM LEADERS SHAPING THE INDUSTRY

EXAGRID
Tiered Backup Storage

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

MSP CHANNEL AWARDS
2025 WINNER

- BACKUP & DR INNOVATION OF THE YEAR
- STORAGE HARDWARE INNOVATION OF THE YEAR
- STORAGE VENDOR OF THE YEAR

Thank you so much to all who voted, and congratulations to our fellow MSP Channel Awards 2025 winners!

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

LEARN MORE >

VIEWPOINT

BY SOPHIE MILBURN
EDITOR

MSPs under pressure: Hybrid IT, tool sprawl, and burnout

HYBRID ENVIRONMENTS have become the default architecture for modern organisations, and that shift is quietly reshaping the operational reality for managed service providers. What once was a clear divide between on-premises infrastructure and a single cloud provider has dissolved into something far more layered: a blended ecosystem of multiple clouds, legacy systems, and edge workloads coexisting at once.

For clients, the hybrid multi-cloud model delivers real value through flexibility, resilience and more control over spending. But for MSPs, it often leads to fragmentation that quickly becomes difficult to handle.

At the core of the issue is tool sprawl. Every environment in a hybrid setup brings its own native tooling. On-prem monitoring systems. Backup solutions. Identity platforms. Security stacks. Then MSPs add their own layers on top - RMM, PSA, SIEM, CSPM, vulnerability scanners, and more. Each tool solves a problem. Individually, they make sense. Collectively, they create a system that is harder to unify, maintain, and operate.

Cloud providers optimise for their own ecosystems, not interoperability. Clients adopt multiple platforms to avoid lock-in, meet regulatory requirements, or leverage best-of-breed capabilities. MSPs sit in the middle of all of this, inheriting the challenge of making it work in practice. The result is constant context switching, duplicated workflows, and fragmented visibility. Over time, that creates operational strain. And then comes burnout.

Technicians aren't just managing systems, they're navigating them. Jumping between dashboards. Responding to alerts across disconnected tools. Maintaining expertise across an ever-expanding stack. Alert fatigue becomes routine. So does the cognitive overhead of remembering which system does what, and how to connect the dots when something goes wrong. Burnout, in this context, isn't just about workload. It's about mental load.

The way forward isn't simply adding more tools. If anything, that often makes the problem worse. MSPs that succeed in this environment are the ones that step back and rethink their approach. They focus on consolidation and integration. On reducing the number of moving parts where possible. A unified operational layer, whether through integrated platforms or carefully curated stacks, can restore visibility and reduce friction. It gives teams something they've been losing: clarity.

There's also a clear role for automation, especially in triage, remediation and reporting, where humans are often doing work that could be handled far more efficiently. But perhaps the most important shift is intentionality. MSPs must move away from reactive tool adoption and toward deliberate stack design. Every tool should serve a clear operational purpose. Not just simply fill a gap or follow a trend.

That means standardising wherever possible, investing in integration, and continuously pruning what no longer serves. Hybrid environments aren't going away. If anything, they're becoming more complex. The MSPs that thrive will not be the ones that accumulate the most tools, but the ones that design the most coherent systems and find simplicity, even in the face of growing complexity.

Contents

Cover Story

Women in the channel: Advice from leaders shaping the industry

Women from across the tech landscape share their experiences, advice, and career insights. Together, their perspectives underline the importance of visibility and continued progress towards a more inclusive industry.

38

NEWS

06

MSP CHANNEL INSIGHTS

Editor
Sophie Milburn
+44 (0)2476 718970
sophie.milburn@angelbc.com

Consulting Editor
Philip Alsop
philip.alsop@angelbc.com

Business Development Manager
Aadil shah
+44 (0)7519 606 813
aadil.shah@angelbc.com

Senior Sales Executive
Graeme Davidson
+44 (0)2476 823124
graeme.davidson@angelbc.com

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

Graphic Design & Multimedia Assistant
Harvey Watkins
harvey.watkins@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

Angel BUSINESS COMMUNICATIONS

MSP-Channel Insights is published eight 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.

ISSN 2396-9016 (Online)

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

A deep dive into Huntress's 2026 Cyber Threat Report

Delving deep into the organised playbook of modern cybercrime, this article exposes the scale and sophistication transforming cyber criminals into a global force.

IN THE REALM of cybersecurity, an evolution unfolds where cybercriminals adopt the efficiency and scale of legitimate enterprises. The Huntress 2026 Cyber Threat Report examines this transition, revealing how organised cybercrime has escalated into a global threat.

Cybercrime, now the third-largest global economy, projects costs of $12.2 trillion annually by 2031. This surge is fuelled by criminal enterprises crafting scalable business operations, akin to legitimate companies but with nefarious objectives.

Attackers have shifted from traditional hacking methods to the strategic hijacking of trusted tools. The use of remote monitoring and management (RMM) tools surged by 277%, as criminals leverage these for stealthy intrusions, overpowering traditional hacking techniques.

Manipulating human tendencies has become a cornerstone in the cybercriminal strategy. The ClickFix method, a highly effective social engineering technique, accounted for over half of malware loader activity. This method exploits routine behaviours, such as solving CAPTCHAs, to infiltrate systems stealthily.

Ransomware groups have evolved from swift lock-and-encrypt attacks to comprehensive data theft and extortion strategies. This shift extends the 'time-to-ransom' phase, as perpetrators sift through and extract valuable data before any encryption activity occurs.

Innovations in identity threats have fostered new attack vectors, with abuse of mailbox rules and OAuth permissions becoming prevalent. These tactics support business email compromise and other identity-driven attacks, allowing criminals to penetrate corporate defences invisibly.

By examining telemetry from over 230,000 protected organisations, Huntress sheds light on this. The report highlights key cyber trends, identifying vulnerabilities and proposing strategies to counter these burgeoning threats.

The cybercriminal realm continues to mature, moving away from flamboyant exploits to streamlined, scalable operations aimed at maximising impact. Recognising and utilising trusted tools, exploiting human behaviours, and leveraging stolen credentials have become the mark of a well-oiled underground economy poised for future growth.

This trend towards streamlined efficiency suggests a future where artificial intelligence might further automate attacker tactics, necessitating robust identity protection strategies and vigilant monitoring of trusted channels. As cyber threats become more pervasive, organisations need a comprehensive approach to stay ahead of these ever-evolving adversaries and protect their digital assets.

Agent Commander: Veeam's solution for AI security challenges

Veeam has launched Agent Commander, a solution designed to combine data resilience with AI security, providing organisations with visibility and control over AI systems and associated risks.

VEEAM SOFTWARE has introduced Agent Commander, a solution designed to help organisations identify AI risks, protect AI systems, and remediate AI errors. The launch follows Veeam's acquisition of Securiti AI, combining capabilities from both organisations into a unified platform for managing data and AI environments.

Agent Commander aims to provide organisations with visibility and control across their data and AI estates. A key feature is its ability to reverse certain AI-related actions where necessary, enabling businesses to address risks while continuing to expand AI usage within defined controls.

As AI becomes more embedded in enterprise operations, data risk and AI risk are increasingly interconnected. Organisations often operate with distributed controls and separate systems for protection, governance and recovery, which can limit holistic oversight. This fragmentation can result in sensitive data being used in ways that are not fully monitored or governed.

Agent Commander introduces a unified control plane intended to deliver contextual visibility, policy enforcement and recovery capabilities. The platform integrates data resilience, data security and AI risk management into one operational framework.

Central to the solution is Veeam's Data Command Graph, an intelligence engine that maps real-time connections between data, identities, AI models and autonomous agents across production and backup environments. It is designed to identify risk scenarios involving compromised identities, exposed data and automated processes by analysing how these elements interact.

The platform supports organisations in detecting AI risks such as shadow AI and anomalous agent behaviour, applying governance controls to AI pipelines, and reversing AI-driven actions when required. It is positioned to provide context-aware recovery with limited disruption to operations.

By combining AI-related visibility with data resilience capabilities, the solution reflects an approach where AI protection and recovery are integrated into existing infrastructure. As AI moves further into operational use, the platform is intended to support organisations in managing governance, security and recovery within a single system.

UK IT professionals report high confidence in AI and cybersecurity readiness

THE LATEST survey reveals UK IT professionals lead Europe in confidence regarding future-proofing their operations with AI and cybersecurity measures. According to research by TOPdesk, involving over 6,000 IT professionals across Europe, 45% of UK respondents believe their IT functions are fully future-proofed. This is higher than their counterparts in Switzerland, Austria, Germany, and Belgium.

The enthusiasm for AI's role in future-readiness is evident, with 49% of UK professionals considering it a cornerstone. Yet, full integration remains elusive as only 36% of organisations achieve maturity in AI adoption. This means realising AI's benefits, like embedding it thoroughly across all departments and ensuring it delivers measurable value.

Despite the United Kingdom's optimistic outlook, several challenges persist. Predominantly, skill shortages and investment gaps continue to impede progress. Approximately 28% of respondents cite a lack of skilled professionals as a significant challenge, while 27% highlight insufficient investment in AI implementations.

Moreover, along with staffing and funding obstacles, numerous UK IT teams face another persistent issue: integration with existing business systems, affecting around 20% of professionals. They find coordination and seamless functionality daunting when incorporating AI into diverse platforms.

For UK organisations to maximise AI's potential, industry experts advocate a comprehensive approach. This entails investing in robust processes, clarifying roles, and ensuring cooperation across departments. True future-readiness will be achievable when organisations put these foundational elements in place.

The insights by TOPdesk extend beyond their traditional software capabilities, advocating for a strategic direction in enhancing IT assets. Their experience in helping more than 5,000 global organisations positions them to help guide UK IT sectors toward holistic digital transformations.

AI vs. human: Assessing cybersecurity performance

Hack The Box's report examines the impact of AI on cybersecurity task performance, analysing productivity changes and performance differences across experience levels.

HACK THE BOX (HTB) has published findings from its latest AI-Augmented vs. Human-Only Cybersecurity Performance Benchmark Report. The research draws on data from its NeuroGrid Capture The Flag (CTF) competition, which compares AI-augmented and human performance on cybersecurity tasks.

The results show that AI integration can increase task completion speed depending on the proficiency of the AI-augmented team. Key findings indicate that AI-enabled teams completed tasks faster, generating up to 4.1x more output for elite teams and 1.4x more across all teams within a set timeframe.

AI-augmented teams also recorded a 70% higher challenge solve rate compared to top human-only teams, achieving a 3.2x higher solve-rate ratio across all participants.

The benchmark included 1,078 teams — 120 agentic AI teams and 958 human teams — participating in 36 cybersecurity challenges across nine technical domains and four difficulty levels over a three-day period.

The report highlights that the effects of AI adoption vary across experience levels and that workforce development strategies may need to account for these differences:

- **Early Career:**
  AI can support less experienced teams in completing more challenges but may also lead to reduced efficiency in some cases. These teams were observed to be 12.5% slower on average, sometimes becoming dependent on iterative or unstructured workflows without sufficient oversight.
- **Mid Career:**
  Mid-level operations saw the strongest improvement on medium-difficulty tasks, with a peak advantage of 3.89x.
- **Elite Teams:**
  While the relative advantage in solve rate narrows at higher experience levels, AI-augmented elite teams demonstrated a speed increase, completing challenges 312% faster.

The findings suggest that automation of routine and mid-level tasks can deliver measurable productivity gains. At the same time, the report notes that over-reliance on automation in judgement-based tasks may affect long-term skill development and resilience.

The competitive advantage lies not only in adopting AI tools, but also in developing the capability to effectively manage, validate, and govern AI-driven workflows within cybersecurity operations.

Cybersecurity alerts: Ransomware incidents and new security threats

Barracuda Networks unveils ransomware findings; swift breaches and outdated systems are key vulnerabilities. How businesses can adapt to evolving threats.

BARRACUDA NETWORKS, a cybersecurity company, has reported that 90% of ransomware incidents in 2025 exploited firewalls through unpatched software or vulnerable accounts. In the fastest case observed, the time from breach to encryption was three hours, reducing the opportunity for detection and response.

The findings are detailed in the Barracuda Managed XDR Global Threat Report, which outlines common attack methods and security gaps. Drawing on thousands of real-world incidents, the report shows that attackers frequently use legitimate IT tools, such as remote access software, and exploit unprotected devices. It also identifies risks linked to outdated encryption, disabled endpoint security and unusual login or privileged access activity.

Key findings:

- Ninety per cent of ransomware incidents involved the exploitation of a CVE (a classified software vulnerability) or a vulnerable account. Attackers were then able to gain network access and conceal malicious activity.
- The fastest case observed involved Akira ransomware and progressed from breach to encryption in three hours, limiting the window for defenders to respond.
- Sixty-six per cent of incidents in 2025 involved the supply chain or a third party, up from 45% in 2024, as attackers targeted weaknesses in third-party software.
- Ninety-six per cent of incidents involving lateral movement resulted in ransomware deployment. Lateral movement typically indicates that attackers have compromised an endpoint and are extending their access within a network.

> Merium Khalid, Director of SOC Offensive Security at Barracuda, said organisations — often operating with limited resources and multiple security tools — must protect identities, infrastructure and data against attacks that can develop rapidly.

- The most widely detected vulnerability was CVE-2013-2566, a flaw in an outdated encryption algorithm found in older systems, servers and embedded devices.

The report advises organisations and managed service providers to take practical steps to reduce risk, including identifying and addressing unpatched software and misconfigurations.

Merium Khalid, Director of SOC Offensive Security at Barracuda, said organisations — often operating with limited resources and multiple security tools — must protect identities, infrastructure and data against attacks that can develop rapidly. She noted that overlooked issues, such as dormant applications, unused accounts or misconfigured security features, can increase exposure.

The findings are based on Barracuda Managed XDR data collected during 2025, including more than two trillion IT events, nearly 600,000 security alerts and over 300,000 protected endpoints, firewalls, servers and cloud assets.

NinjaOne reveals AI-powered vulnerability management solution

NinjaOne introduces a real-time AI-powered vulnerability management solution that helps IT teams identify and fix security issues more efficiently.

NINJAONE has launched NinjaOne Vulnerability Management, a solution designed to help IT teams identify, prioritise, and remediate vulnerabilities more quickly. Unlike traditional approaches that rely on periodic scans and manual intervention, this solution aims to provide integrated, real-time visibility and remediation.

Traditional vulnerability management methods can leave organisations exposed for extended periods. Legacy technologies and infrequent scans may increase risk and delay remediation.

NinjaOne's approach uses artificial intelligence and automated patching workflows to address vulnerabilities more promptly and accurately.

The solution provides real-time visibility, integrated remediation, and reporting within a single platform.

This centralisation aims to allow organisations to identify, remediate, and patch vulnerabilities efficiently, while enabling security teams to focus on higher-priority incidents.

By analysing millions of data points across its system, NinjaOne's AI-driven platform seeks to reduce manual effort and improve resource utilisation, supporting closer collaboration between IT and security teams.

Key benefits include:

- **Real-time visibility and reduced vulnerability time:** Continuous AI-powered assessments aim to provide up-to-date insights into software vulnerabilities, including offline devices, helping to minimise exposure.
- **Integrated detection and autonomous remediation:** Detection is directly connected to automated patching workflows, seeking to enable prioritisation and application of patches across Windows and Linux systems.
- **Minimal impact on device performance:** Vulnerability identification is performed server-side using existing device data, avoiding intrusive scans or performance issues.
- **Audit-ready compliance:** The solution automatically captures vulnerability and remediation metrics, supporting regulatory adherence with minimal manual effort.

By combining AI-powered assessment with integrated remediation, NinjaOne Vulnerability Management seeks to allow organisations to manage risk more effectively while streamlining operational workflows.

AI and Cybersecurity: The future of phishing defence

2025 marked a turning point in cybersecurity, as AI transformed both phishing techniques and the tools used to combat them, ushering in a more complex digital arms race.

IN 2025, AI technology played a growing role in cybersecurity, influencing both attacker methods and defensive strategies.

According to the Kaseya INKY Email Security Report, AI-generated phishing tactics became widely used in phishing attacks.

The report outlines how AI can be used to produce highly convincing and scalable phishing messages, reducing the reliability of traditional warning signs such as poor grammar, suspicious domains, and obvious links. As a result, defenders are increasingly required to assess the intent and context of emails rather than relying solely on conventional indicators.

Phishing continues to be a leading vector for cyberattacks, accounting for 26% of cybercrime-related complaints filed with the FBI and contributing to financial losses, including $2.8 billion associated with Business Email Compromise. A large proportion of these attacks—up to 82%—target organisations with fewer than 1,000 employees, indicating the exposure of small and mid-sized businesses (SMBs) to cyber threats.

The report also states that among the more than 4.5 billion emails processed by the INKY system in 2025, 281 unique brands were impersonated. Using AI-generated layouts, attackers are able to more closely replicate legitimate communications from financial and retail organisations.

AI is also being applied in defensive tools. INKY reports using generative AI-driven detection models, including intent-based labelling, multi-label classification, and computer vision techniques, to improve threat identification. These approaches are being developed alongside changes in phishing methods, such as the use of calendar invitations, protected document prompts, and callback phone numbers.

As AI continues to influence both attack techniques and security tools, organisations are increasingly adopting updated approaches to address evolving phishing activity.

CrowdStrike Falcon aims to enhance AI governance and endpoint security

CROWDSTRIKE has introduced enhancements to its Falcon platform, extending AI security capabilities and reinforcing the endpoint as a central point for AI threat management.

The updates aim to address the increasing autonomy of AI agents, which can execute commands and access data directly on endpoints. Traditional security methods have limited ability to govern these operations. CrowdStrike's new features provide real-time oversight and monitoring of AI activity.

As AI adoption grows, the need for endpoint security rises. CrowdStrike identifies numerous AI applications across enterprise devices, covering approximately 160 million unique instances. To manage this, the platform seeks to offer:

- **EDR AI Runtime Protection:** Provides visibility of AI actions in progress, enabling teams to track and respond to suspicious behaviours.
- **Shadow AI Discovery:** Detects AI applications and assesses their potential security impact.
- **AIDR for Endpoint:** Monitors desktop AI applications to identify threats and enforce compliance.

Beyond endpoints, AI agents operate across SaaS platforms, cloud environments, and web interfaces. CrowdStrike's intended features include:

- **Shadow SaaS and AI Agent Discovery:** Monitors AI activity, permissions, and potential vulnerabilities across popular platforms.
- **AIDR for Copilot Studio Agents:** Provides real-time monitoring for Microsoft Copilot Studio, detecting data leaks and other threats.
- **AIDR for Cloud:** Secures AI workloads in cloud environments against prompt-based threats.
- **AI Data Flow Discovery for Cloud:** Tracks data movements in real time to support management of potential data exposure.

These enhancements aim to provide comprehensive oversight of AI activity across endpoints, cloud, and SaaS environments, helping organisations monitor and manage AI-related security risks.

Spirent reveals domain-trained AI for enhanced network testing and assurance

Spirent introduces Spirent Luma, an AI solution enhancing network testing with automated troubleshooting and expert-level data interpretation.

SPIRENT COMMUNICATIONS has announced the launch of Spirent Luma, an agentic AI solution designed to support network testing and assurance.

The domain-trained AI aims to accelerate automated troubleshooting, provide clearer insights, and deliver consistent interpretation of complex test data. The objective is to reduce manual effort and minimise uncertainty in analysis.

Spirent, now integrated with Keysight Technologies, is known globally for its test and assurance solutions for next-generation networks and devices. Luma is built on this expertise and has been developed over time using accumulated knowledge in network testing.

Initially compatible with Spirent's core network test platform, Landslide, Luma integrates into existing testing workflows. It is designed to operate within current processes without requiring significant changes.

Unlike general-purpose AI models, Luma is intended to function within secure IT lab environments and apply its capabilities to testing scenarios.

Key capabilities include:

- **Domain-Trained Intelligence:** Luma is developed using Spirent's understanding of 3GPP and network-specific requirements to address CSP-grade testing challenges.
- **Seamless Workflow Integration:** Embedded within the Landslide platform, Luma operates within secure lab environments and supports root cause analysis using established tools.
- **Accelerated Troubleshooting:** The system assists in interpreting logs and test data, supporting a faster transition from raw data to actionable insight.
- **Scaling Expertise:** The interface is designed to reduce reliance on specialist knowledge and broaden accessibility across user groups.

The introduction of Luma represents the first stage of a wider initiative by Spirent to integrate agentic AI across its testing, assurance and automation portfolio.

The approach focuses on embedding functionality within existing processes so that users can move from data to decision-making without introducing additional tools or major workflow changes.

Following its integration into Landslide, further developments are planned for Spirent's VisionWorks service assurance and Velocity test and lab automation solutions. These updates are intended to enhance testing and operational processes through additional AI capabilities.

This AI-based approach aligns with Spirent's strategy to improve speed and accuracy across the network lifecycle. Alongside operational efficiencies, the solution is intended to support clearer interpretation of network performance data.

The Luma series will be demonstrated at MWC Barcelona in early March at the Keysight Technologies booth, where attendees can review the capability in context.

In summary, Spirent Luma marks a development in network testing by integrating AI-driven assistance into established workflows. The initiative reflects ongoing efforts to incorporate AI capabilities into testing and assurance environments.

CHANNEL INSIGHTS 2026 ROADSHOW

MSP CHANNEL INSIGHTS ROADSHOW

SECURE YOUR 2026 PARTNERSHIP

Taking the MSP Channel on the Road
2026 Regional Series

Join the **most targeted regional MSP event series** designed to **connect vendors** with engaged, growth-focused Managed Service Providers across **seven key markets**.

REGISTER NOW

Why Partner With This Series?

Pan-European Reach With Local Market Impact

Seven strategically selected cities put you directly in front of active MSP communities in:
Manchester • Birmingham • London • Dublin • Munich • Utrecht • Copenhagen

Decision Makers in the Room

Meet **senior MSP leaders** with real buying authority actively seeking new partnerships and solutions.

Curated Conversations That Convert

Benefit from **expertly crafted content, expert panels, and structured networking sessions** designed to create meaningful, high-value connections.

Beyond the Event

Your visibility **doesn't stop when the doors close**. Gain post-event amplification through digital coverage, content sharing and ongoing brand presence.

SCAN ME

msp-roadshow.com

Women in the channel: Advice from leaders shaping the industry

Women from across the tech landscape share their experiences, advice, and career insights. Together, their perspectives underline the importance of visibility and continued progress towards a more inclusive industry.

THE CONVERSATION around **women in tech** is sometimes described as "overdone," but its importance has never diminished. Progress in this space relies on **consistency, visibility,** and an **ongoing commitment to spotlighting and celebrating the voices shaping the industry**. Representation is not a one-time achievement, but something that must be continuously reinforced to drive meaningful, lasting change.

Inspired by a recent podcast episode exploring the **experiences, challenges,** and **opportunities** for women across the tech and channel landscape, this article brings together voices from across the industry to **share their insights.**

From **cybersecurity** and **marketing** to **leadership** and **channel strategy**, these perspectives highlight that there is no single path into tech, and no single definition of success. Instead, what shines through is a shared emphasis on curiosity, resilience, and the power of community. Whether it's stepping into the unknown, challenging expectations, or lifting
others along the way, these women are not only navigating the industry, **they are actively shaping its future**.

Together, their words offer both **practical advice** and **powerful encouragement** for anyone considering a career in tech, or looking to grow within it.

WOMEN IN THE CHANNEL

KIRSTY SWALES, ENTERPRISE SECURITY ENGINEER AT TENABLE

"The technology industry has taken important strides towards inclusivity, driven by rising awareness and more organisations championing women. Yet retention remains a challenge that just won't budge. Visible female role models matter. Without them, confidence can waver for those considering journey within the tech industry.

"For businesses, hiring women in tech is about supporting them, investing in their growth and creating environments where they can truly thrive. Mentorship programmes and inclusive hiring practices can make a meaningful difference, but sometimes the best candidate isn't the one who ticks every box. Instead, they're the one who brings a fresh perspective and a different mindset.

"If my journey has taught me anything, it's that you don't need to have it all figured out from day one. My advice to women in tech is to stay curious, embrace confidence and be yourself. We deserve to be in this industry just as much as anyone else. Find your allies, build strong support networks and lean on mentors along the way; it truly makes all the difference."

ERIN MCLEAN, CHIEF MARKETING OFFICER AT CYNOMI

"Early in my career, I was at a networking event and asked a very accomplished chairwoman how she overcame adversity in a male-dominated field. Her answer stayed with me: she said she was successful because she never thought of it that way, she just focused on doing the work.

At the time her answer caught me off guard, but over the years I've come to appreciate the clarity in that mindset. You can't be so focused on whether you belong that you miss the opportunity in front of you.

Personally, I believe we have a responsibility, especially in fields like cybersecurity, to make that path more visible and more accessible for others. When I speak to women entering cyber today, I want them to see what's possible and to know they're included.

Progress isn't just about individual resilience, it's about community. We need to lift each other up, make space at the table, and lead in a way that's supportive, collaborative, and grounded in respect. That's how we create lasting change."

LARISA LUCACIU, BUSINESS TRANSFORMATION LEADER – UKI VECTOR AT LENOVO

"A career in tech is not just about technical expertise, it is also about curiosity, resilience and having the confidence to keep stepping into spaces where you can learn, grow and have an impact.

One of the biggest lessons I've learned is that you do not need to know everything before taking the next step. Some of the best opportunities come before you feel fully ready, so stay curious, make yourself visible and back yourself. That is often where the real growth happens!"

STEPH HACKNEY, SENIOR CHANNEL MARKETING MANAGER, UKI & NORDICS AT OPENTEXT

"My advice for anyone looking to get into the industry is to just go for it! The channel is full of opportunity, and one of the things that makes it so exciting is the sheer number of directions your career can take. Whether you're drawn to marketing, enablement, partner strategy, or something more technical, there's space to explore, experiment, and find the area that truly ignites your passion.

Career paths don't have to be linear - in my experience they rarely are, and I've seen many of my peers grow their careers into new and interesting areas. Every role, project, and challenge you take on builds skills and perspective that you carry forward, even if the next step looks completely different on paper. Some of the most valuable growth comes from saying yes to opportunities that stretch you, feel unfamiliar, or push you slightly outside your comfort zone. Don't be afraid to chase those opportunities. The channel rewards curiosity, adaptability, and people who are willing to learn and evolve. If you're open to trying new things and backing yourself, you'll grow faster and shape a career that's genuinely fulfilling and uniquely your own."

NICOLA SANER, CEO AT CHORUS

"In my opinion, the tech industry doesn't need more people who fit a single mould, it needs people who are willing to challenge it with broader perspectives, different ways of thinking, and more diversity at every level. More female leaders in tech won't just change who sits around the table but will also help shape what the future of technology actually looks like – what gets built, who it's built for, and the values that underpin it.

One of the most important things I learned early on in my career is that very few people genuinely have it all figured out. Progress doesn't come from having a perfect plan, it comes from being brave enough to take the first step, curious enough to keep learning, and confident enough to ask questions along the way. Growth often happens when you say yes to opportunities that feel uncomfortable, when you explore areas others may shy away from, and when you trust yourself to figure things out as you go (too much procrastination can be damaging to a strategy).

Tech is constantly evolving, and success isn't about knowing everything already...it's about being open, adaptable, and willing to challenge assumptions, including your own. If more women felt empowered to step into leadership without waiting to feel "ready," the industry would be more innovative and more representative of the world it serves."

MELISSA L. DIRECTOR OF CHANNEL ENABLEMENT & EXPANSION AT CYNOMI

"The biggest piece of advice I ever received? Never stop learning. Our industry is evolving every single day and so should you. Whether it's picking up one new tool, digging into a process, or adopting a best practice, it all compounds over time. The resources are out there: blogs, podcasts, books, peer groups- you just have to be intentional about seeking them out. And that means actually setting time aside in your already busy day or week to do it.

Also, don't overlook the people around you. We have some of the most brilliant minds in this space, and knowledge sharing has been my secret sauce. To this day, I am always looking and listening for new and innovative ways to be bigger, better, and more bad*ss. Growth doesn't stop and neither should you."

HAYLEY CARTER, CEO AT ESSENTIA

"At conferences, it's almost instinctive to glance at someone's lanyard when you're introduced. Since founding my MSP, I've noticed a consistent reaction when I introduce myself as Founder and CEO. Is most commonly shock, a moment of visible surprise, often followed by, 'Wow, so it's your business?' or 'You're the founder?'

It makes me wonder: is that response because of my age, or because I'm a woman? I genuinely believe that, in most cases, there's no ill intent behind the reaction.

Still, I look forward to the day when women in business are met not with surprise, but with the recognition and respect deserved.

And to anyone considering a career in the tech industry: don't let those moments of surprise discourage you, let it drive you even further."

"Don't let those moments of surprise discourage you, let it drive you even further."

LAURA JEAN ROMERO, FIELD MARKETING MANAGER AT CONCENTRIC AI

"As a kid who struggled through every math and science class, I never imagined I'd end up working in AI and Cybersecurity. Beyond the academic hurdles, I simply didn't grow up seeing women in STEM, and the fields themselves were still in their infancy in the 90s.

My career has been built on saying "yes" to the unconventional and unexpected. It's essential to remain open to the "wrong" opportunities. Every role I took—even those outside my initial plan—allowed me to stack skills and make connections. For anyone entering tech today: just get your foot in the door. Your first job doesn't have to be the dream; it just needs to be the bridge. Look for the transferable skills that will carry you to where you actually want to be. Even your worst job will teach you something, help you make a new connection, reveal something new about yourself, or provide clarity around what you really want in life."

DANIELLE KINSELLA, SENIOR DIRECTOR, EMEA AT GIGAMON

"If you want to succeed in the channel, you can't simply wait for opportunities, you need to create them by building strong relationships, showing genuine interest, and staying persistent. Those who invest in meaningful connections across their ecosystem are the ones who tend to do well.

A real enthusiasm for the sector makes a difference, particularly in how you support partners and look after customers. Over time, that approach pays off but it's not the whole story. Building a successful career also requires resilience, as progress is rarely straightforward and setbacks are part of the process.

What really sets people apart is a willingness to keep learning, contribute where it matters, and remain consistent."

SAZIKAZI MQINQWANA, MARKETING EXECUTIVE AT BDR GROUP

"Being a woman in tech doesn't mean you have to be in IT. It means you bring your unique perspective to an industry full of opportunity. In tech marketing, your creativity, curiosity, and ability to connect ideas with people are just as powerful as any code.

My advice to the next generation? Lean into your strengths, speak up, and don't let narrow definitions of 'tech' limit where you can go. You belong here and you can shape the future in ways only you can."

GABI BALDWIN, DIGITAL MARKETING SPECIALIST AT INDEX ENGINES

"You don't have to know everything to belong in tech or cybersecurity. Ask the questions. Raise your hand for the project. Sit at the table even if you feel a little underqualified. Growth in this industry often comes from stepping in before you feel fully ready and learning as you go. The industry needs strategic thinkers, creative problem solvers, and strong communicators just as much as it needs deep technical expertise, and that opens the door for more people to build a path here than they might initially realise.

Representation plays a bigger role than people realise. When you see women leading and owning their space, it shifts what feels possible. That visibility can be the difference between someone holding back and someone deciding to go for it. It creates a ripple effect, giving others permission to step in, speak up, and aim higher as they grow in their careers."

CHERYLE CUSHION, SVP MARKETING AT CTERA

"I've been in technology for most of my 30-year career, building marketing engines within organisations from very young and small to very large and complicated. And my key takeaways as I look back to anyone thinking about taking this same path include:

Focus first on understanding problems, not tactics. Get close to customers, sales, and product so you can clearly explain who you serve, what pain you solve, and how your work create revenue for the business.

Treat data and technology as the centre of your universe. Define the important information that moves the needle on the business and understand how it flows through each tool so you can connect activity to pipeline, retention, and expansion in a way that earns trust from finance, engineering and most importantly sales.

Early in your career, intentionally build range. Seek roles that expose you to the various marketing roles - brand, demand generation, product marketing, and lifecycle - across different company types – small, medium and large - so you understand the whole gotomarket engine and find which piece of it you love.

Finally, remember your longterm leverage is people, not campaigns. Invest in communication, storytelling, and emotional intelligence so you can align crossfunctional teams and lead across generations. This skill matters as much, if not more, as tactical expertise in modern tech organisations."

> "Invest in communication, storytelling, and emotional intelligence."

SUNEETHA UPPALAPATI, HEAD OF CLIENT PLATFORM SOLUTIONS AT WAVEMAKER

"So much is evolving around us—and that's exactly why clarity matters more than speed. Success isn't defined by the technology or tools you manage, but by the outcomes and experiences you consistently deliver for your customers.

Focus on the problems that truly move the needle for your clients and take ownership of the outcomes you drive. Use technology with purpose and intention—to simplify complexity, reduce cognitive load, and enable teams to operate with confidence.

Sustainable growth in this space comes from a combination of operational excellence, customer obsession, and continuous learning—the ability to adapt is what sets great teams apart.

Measure your growth not just by what you've learned, but by the impact you've created—for your customers, your team, and your organisation."

Taken together, these perspectives show that there is not a single route into the channel or the wider tech industry. Success comes from curiosity, resilience, and a willingness to keep learning. It's also shaped by the people around you. Support networks, shared knowledge, and making space for others all play a part in driving meaningful progress.

A huge thank you to all the contributors for sharing their experiences so openly. Their insights show what's possible when women are supported, visible, and given the space to grow. And when that happens, the impact goes beyond individual success. It strengthens the industry and helps shape a future that's more inclusive, more balanced, and more reflective of the world it serves.

"Measure your growth not just by what you've learned, but by the impact you've created—for your customers, your team, and your organisation."

Introducing Voices in the Channel:
A new podcast from MSP Channel Insights

We're excited to launch Voices in the Channel, a brand-new podcast hosted by Sophie Milburn, available both on our MSP Channel Insights website and on Spotify. This podcast offers a personal perspective on the industry, bringing listeners closer to the real people, stories, and ideas shaping the channel today.

UNLIKE TRADITIONAL industry coverage, Voices in the Channel highlights the real-life experiences of professionals working across every part of the ecosystem.

From recruitment challenges and overcoming stereotypes, to the role of women in tech, inclusivity, young entrepreneurs, and fast-growing businesses, we focus on the human side of the industry. Each episode shines a light on the individuals driving change, sharing insights and inspiration for anyone connected to—or curious about—the sector.

Our first five episodes set the stage for the series:

- *AI in Marketing with Erin McLean, Chief Marketing Officer at Cynomi* – exploring how artificial intelligence is reshaping marketing strategies.
- *Women in the Channel with Steph Hackney, Senior Channel Marketing Manager at OpenText, and Larisa Lucaciu, UK&I Strategic Partnerships Leader at Lenovo* – a candid conversation about challenges, progress, and opportunities for women in tech.
- *Scaling a Business in the Modern Market with Jay Ball, CEO of Flotek Group Limited* – practical insights on growth strategies and navigating today's competitive landscape.
- *Generational Differences in the Workplace with Steven Heinsius, Vice President of Product Management & Marketing EMEA at Weston-Comstor* – exploring how different generations approach work and how to foster inclusive work environments.
- *Recruitment, Retainment, and Culture with Hayley Carter, CEO of ESSENTIA* – a deep dive into people-focused strategies that build strong, resilient teams.

Episodes will be released every Thursday at 4 PM, making it easy to tune in and stay informed about the trends, ideas, and conversations that matter.

Whether you're an established professional, just starting your journey in the industry, or simply interested in the people making it thrive, Voices in the Channel delivers thoughtful, engaging, and authentic discussions.

Listen on our website or subscribe on Spotify to join the conversation.

MSP CHANNEL INSIGHTS

CHANNEL INSIGHTS 2026 ROUNDTABLE

MSP CHANNEL INSIGHTS ROUNDTABLE

Engage Directly with MSP Decision-Makers

Engage in **industry-leading discussions** at **MSP Channel Roundtables**, where experts convene to **shape the future** of managed services. **Join us** for insightful dialogues and unparalleled networking opportunities

SECURE YOUR 2026 PARTNERSHIP

VIRTUAL ROUNDTABLE

KEY BENEFITS:

- Direct access to **MSP decision-makers**
- Thought **leadership** positioning
- **Multi-channel promotion** to MSP audiences
- **Exclusive** networking opportunities
- Access to **MSP Channel Insights Community**

EXCLUSIVE TO VIRTUAL:

- **Online Interactive Roundtable discussions**
- Video interviews and sponsor exposure
- **Access to delegate registration lists and digital promotion**

CONTACT DETAILS:

Aadil Shah
aadil.shah@angelbc.com

SCAN ME

AUDIENCE INCLUDES MSPS, MSSPS, VARS AND IT RESLLERS

80,000+ CHANNEL PROFESSIONALS ACROSS UK, EMEA AND US

msp-channel.com/roundtables

Scaling Flotek: A closer look at one of the UK's fast-growing MSPs

Flotek Group has grown rapidly in a market known for complexity and fragmentation. In this exclusive conversation, CEO Jay Ball discusses the thinking behind that growth, from early structural decisions to a careful balance of acquisitions and organic expansion, and how the business is continuing to evolve as it scales.

The idea behind Flotek

THE FOUNDATIONS of Flotek were shaped by a clear view of where the market was falling short. Reflecting on his experience after exiting a communications business in 2019, Ball explains that, despite clear signs of convergence, the industry had not yet adapted to that reality.

Instead, the market remained fragmented. As Ball puts it, "you either have communications providers attempting to bolt on managed IT, or IT providers offering only basic communications." In both cases, he notes, there was "a lack of depth, mutual respect and true understanding between the two disciplines." This disconnect was not just theoretical, it was visible in day-to-day operations, where different teams struggled to align around shared priorities and commercial models.

That friction created a clear opportunity for a different kind of business. What was missing, in Ball's view, was "a genuinely blended model with skilled specialists on both sides, backed by strong commercial leadership." Flotek was built to address that gap directly. It was founded "to bring those two worlds together properly, not as an afterthought, but as a single, well architected service with the right people, structure and ambition behind it."

From the outset, Flotek was built with scale in mind. That meant putting the right systems, processes and supplier relationships in place early, rather than trying to retrofit them later. Acquisitions were always part of the plan, so a single, central platform for managing customers, service delivery and billing became a foundation rather than an afterthought. Just as important was the internal mindset.

Standing out in a crowded market

In a market where technical capability is no longer enough, differentiation comes down to clarity and execution. Ball is candid about what he would do differently. "I would simplify even faster," he says. Too many MSPs, he argues, rely on complex bundles and unclear billing, which only makes services harder to adopt and harder to trust.

Flotek's aim has always been to remove that friction and make services "easy to buy, easy to understand and easy to

consume." That focus on simplicity has been refined over time as customer expectations and the wider threat landscape have evolved.

Alongside this, supplier strategy plays a critical role. Ball is clear that "a narrow, strategic vendor portfolio aligned to our long-term goals is far more powerful than multiple supply chains." It is a deliberate choice that aims to support consistency and long-term growth.

Ultimately, the difference comes down to understanding the customer. As Ball puts it, success lies in "deep understanding of customer frustrations and relentlessly closing the gap between what customers need and how MSPs traditionally deliver it."

Scaling without losing direction

For Ball, 'scale done right' is not about speed alone, but about alignment. "Scale done right starts with people, then processes, then systems and suppliers," he says. All four need to move in the same direction, with a clear understanding of the journey ahead.

Flotek's growth through acquisition reflects that ambition. The business completed 15 acquisitions in under four years, but in recent times, the pace has been deliberately moderated. Over the last 18 months, the focus has shifted towards strengthening organic growth and reducing reliance on deals to drive momentum.

That decision reflects a broader principle. Building a "fundamentally strong business at every level" matters more than headline growth. At the same time, there was a recognition that continuing at the same pace risked stretching leadership capacity and external relationships. By slowing down, the business has been able to strengthen its senior team and protect long-term value, rather than prioritising short-term expansion.

Choosing between acquisition and organic growth

Flotek's approach to growth has become more selective over time. While acquisitions remain part of the strategy, the business has built a strong organic engine alongside it. Today, that organic growth delivers around £15 to £20k in net new monthly recurring revenue, which, on an annualised basis, compares with the scale of many standalone MSP acquisitions in the UK.

When evaluating acquisitions, the focus is on fit. Regional coverage, customer profile and supplier alignment all play a key role in the decision-making process. But the balance of the model is intentional. As Ball puts it, "organic growth alone will not deliver our long-term ambitions, so acquisitions remain a core part of our strategy."

That balance is important. Relying too heavily on either acquisitions or organic growth can create vulnerability. A blended approach helps ensure resilience, giving the business stability even when market conditions shift or deal flow fluctuates.

Culture, morale and the reality of integration

For Flotek, cultural alignment is not a secondary consideration, it is the deciding factor. "Cultural alignment is non-negotiable," says Ball. That alignment begins with leadership, but it extends much further, shaping how customers are served and how the business operates day to day. In many MSPs, customer expectations often reflect the mindset of the owner, which means misalignment can quickly create friction.

While revenue, capability and geographic fit all play a role, they only matter if the cultural foundation is right. If it is not, Ball is clear that the conversation does not continue.

Experience has shown that overlooking this element leads to far greater challenges later, particularly as businesses attempt to scale and integrate.

That same focus on people carries through into how Flotek approaches integration. There is a clear acknowledgement that change inevitably brings disruption. "There is no such thing as an acquisition without disruption unless you leave the business entirely siloed," Ball explains. Instead, the emphasis is on transparency from the outset. Teams are told what to expect, including the positives and the challenges, but the direction of travel is always clear.

From there, engagement is immediate and personal. One to one conversations help build trust, while customers are given dedicated account management to maintain continuity. The transition itself is carefully structured, with service migration phased over six to nine months. Systems and processes are mapped first, before any changes are implemented. This measured approach helps protect morale while ensuring service delivery remains consistent, striking a balance between growth and stability.

Balancing local identity with a national brand

From the outset, Flotek is transparent with the owners it acquires. Brand transitions are handled gradually, with names typically retained for 12 to 18 months before being unified under the

Flotek brand. It is a deliberate approach that avoids unnecessary disruption while allowing time for customers and teams to adjust.

In practice, Ball suggests that branding is rarely the deciding factor for customers. “Customers are more resilient than many expect,” he explains. What matters most is consistency in service, responsiveness and the ability to deliver more value over time.

That does not mean the local presence disappears. Flotek continues to operate with a regional footprint, whether through local offices or hybrid working models. This helps preserve familiarity and trust, even as the business becomes more unified at a national level.

In fact, the transition can often unlock new opportunities. While some customers may initially prefer smaller independent providers, many begin to see the benefits of scale. Access to a broader range of services and capabilities often leads to strong growth following acquisition.

Building and retaining a high-performing team

Recruitment is one of the defining challenges for MSPs, but Flotek has taken a deliberate approach to stand out in a crowded market. The result is a business that now attracts consistent inbound interest, with strong application volumes coming directly through its website. According to Ball, this reflects sustained investment in employee experience and a clear effort to articulate what makes Flotek different, both in the role itself and in the wider opportunity.

A key part of that proposition is ownership. The company’s EMI equity scheme plays a significant role in attracting and retaining talent, creating a sense that people are building something together rather than simply holding a job. It fosters long-term thinking and shared commitment, which becomes increasingly important as the business scales.

When it comes to advice for other MSPs, Ball keeps it simple: “My advice to other MSPs would be to over communicate. Make people feel part of the journey, involve them in events and decisions, and actively build a sense of togetherness.”

Retention, while never perfect, has remained strong. Flotek has largely retained the people it wants to keep, recognising that some turnover is a natural part of growth. The focus is on investing in people, reinforcing culture and giving teams a clear sense of identity. Internally, that culture is known as the Purple Army, underpinned by shared values and a strong sense of purpose.

Crucially, engagement is not left to chance. When decisions affect the wider team, input is actively sought. A recent example is FloFest, where feedback led to a shift from a single annual event to more frequent regional gatherings. That willingness to listen and adapt has become a defining feature of how Flotek operates, helping to keep teams engaged as the business continues to scale.

At the core of Flotek

Flotek’s story is defined by a clear sense of direction. The business has focused on simplifying complexity and bringing communications and IT together in a more cohesive model. Growth has been pursued with structure and intent, rather than speed alone.

There is a consistent emphasis on alignment across people, processes and customers. At the same time, the business continues to adapt as it scales. In this context, growth is not just about size. It is about building a model that can sustain itself. One where culture, capability and customer experience evolve together.

MANAGED SERVICES SUMMIT

BENELUX
LONDON
NORDICS
MANCHESTER

CREATING VALUE with MANAGED SERVICES

managedservicessummit.com

MANAGED SERVICES SUMMIT BENELUX

benelux.managedservicessummit.com

10 JUNE 2026

MANAGED SERVICES SUMMIT LONDON

london.managedservicessummit.com

17 SEPTEMBER 2026

MANAGED SERVICES SUMMIT NORDICS

nordics.managedservicessummit.com

03 NOVEMBER 2026

MANAGED SERVICES SUMMIT MANCHESTER

manchester.managedservices summit.com

07 NOVEMBER 2026

Scaling with purpose: Inside Evergreen's fast-growing global expansion

In an exclusive conversation with Isobelle Coventry, this article explores the significant growth trajectory of Evergreen and the strategy underpinning its rapid expansion across the UK, Ireland, and beyond

WITH EVERGREEN surpassing $1 billion in revenue and completing more than 100 acquisitions globally, Isobelle Coventry offers an insider perspective on what is driving this momentum and why the model resonates so strongly with MSP founders. Drawing on her experience leading M&A in the region, she speaks to the personal nature of founder transitions, along with the importance of trust and legacy in every deal. She also reflects on how expectations among MSP owners are evolving in a more sophisticated market.

The article explores Evergreen's portfolio, as well as the broader consolidation trends shaping the MSP landscape. It also outlines the key factors behind the company's success and what lies ahead as it targets its next phase of growth towards $5 billion in revenue by 2030.

A relationship-led approach to M&A

Speaking on her role at Evergreen, Coventry describes a process centred on building relationships with MSP founders across the UK and Ireland. She explains that much of her time is spent understanding what founders have built, what matters most to them, and whether Evergreen represents the right long-term fit. This, she says, spans the full deal lifecycle, "from building relationships over time, determining valuation through to agreeing a deal, and supporting a founder through what is often a very personal transition."

She also highlights her role as an advisor to the wider MSP community, offering guidance on valuations and buyer expectations even where a deal with Evergreen is not pursued. Coventry notes that the opportunity appealed due to the chance to support an alternative succession model, one that avoids traditional integration or short-term outcomes and instead focuses on long-term continuity for founder-led businesses.

Lessons from a fast-growth journey

Reflecting on Evergreen's growth to over $1 billion in revenue and more than 100 acquisitions globally, Coventry points to a number of key lessons from the journey so far. She emphasises that these are deeply personal decisions for founders, noting that each transaction represents decades of work and trust. "At its core, this role is about stewardship. Founders are trusting us with something they've often spent decades building, and I see that as a real privilege." This perspective has shaped her approach, with a strong focus on transparency and following through on commitments.

She also highlights that long-term outcomes matter more than the deal itself, explaining that the strongest-performing businesses are those where growth is supported without losing what made them successful in the first place. Finally, she points to the value of bringing strong operators together, where businesses can learn from one another while continuing to operate independently, creating a compounding effect over time.

What's driving Evergreen's growth

According to Coventry, a key driver behind Evergreen's recent growth has been the strength of its model. Offering a long-term home where businesses remain independent, rather than being

integrated or sold on, has proven to be a compelling alternative for many founders. She notes that consistency has been critical, with trust building over time as the company continues to deliver on what it sets out to do.

As the platform has scaled, she explains that the focus has evolved. Rather than concentrating solely on preserving legacy, Evergreen is now more intentional about how it supports growth. With clearer growth levers, defined targets, and stronger alignment across the platform, the emphasis has moved toward a broader question: "We've shifted from just protecting the business legacy to also asking: how can we add more value to your business?"

She also points to the importance of collaboration across the platform. With a growing ecosystem of MSPs, Evergreen creates opportunities for shared learning through regional cohorts, leadership summits, and regular touchpoints between operators. Beyond structured forums, collaboration happens day to day, with businesses sharing insights and supporting one another across client needs. Coventry highlights the strength of the MSP community, noting a genuine willingness to collaborate, which Evergreen looks to support and amplify through its model.

What MSP founders value most

Through her work with founders navigating major transitions, Coventry points to a clear set of priorities that shape decision-making. "The biggest thing is trust. Not just in the deal, but on what happens next for their people, their customers, and their brand." She notes that this extends into a strong emphasis on legacy, with many MSP owners building something deeply rooted in their local market and wanting reassurance that identity is preserved.

Flexibility is also key. Every founder's journey is different, whether that involves continuing to lead, stepping back, or transitioning leadership over time, and Coventry highlights the importance of a model that can accommodate those paths. Alongside this, she adds that growth remains a key driver: "The best businesses don't want to stand still: they want access to ideas, talent, and capabilities that make them stronger, without losing their autonomy."

What makes a strong fit

When it comes to acquisitions, Evergreen takes a considered approach. Coventry explains that the focus is not just on scale, but on finding the right businesses to partner with. "We're looking for high-quality businesses with strong fundamentals, but also the right cultural and leadership fit." From a commercial standpoint, she adds that "recurring revenue, strong customer relationships, and exposure to positive industry tailwinds are all important." Factors such as customer retention, concentration, and organisational maturity also play a key role.

Ultimately, she notes that the strongest partnerships go beyond the numbers. The best outcomes come when there is deeper alignment, where founders see Evergreen not just as a buyer, but as a long-term home and growth partner for their business. She states that the most successful providers are positioning themselves as end-to-end technology partners, playing a more strategic role in supporting clients' wider business outcomes.

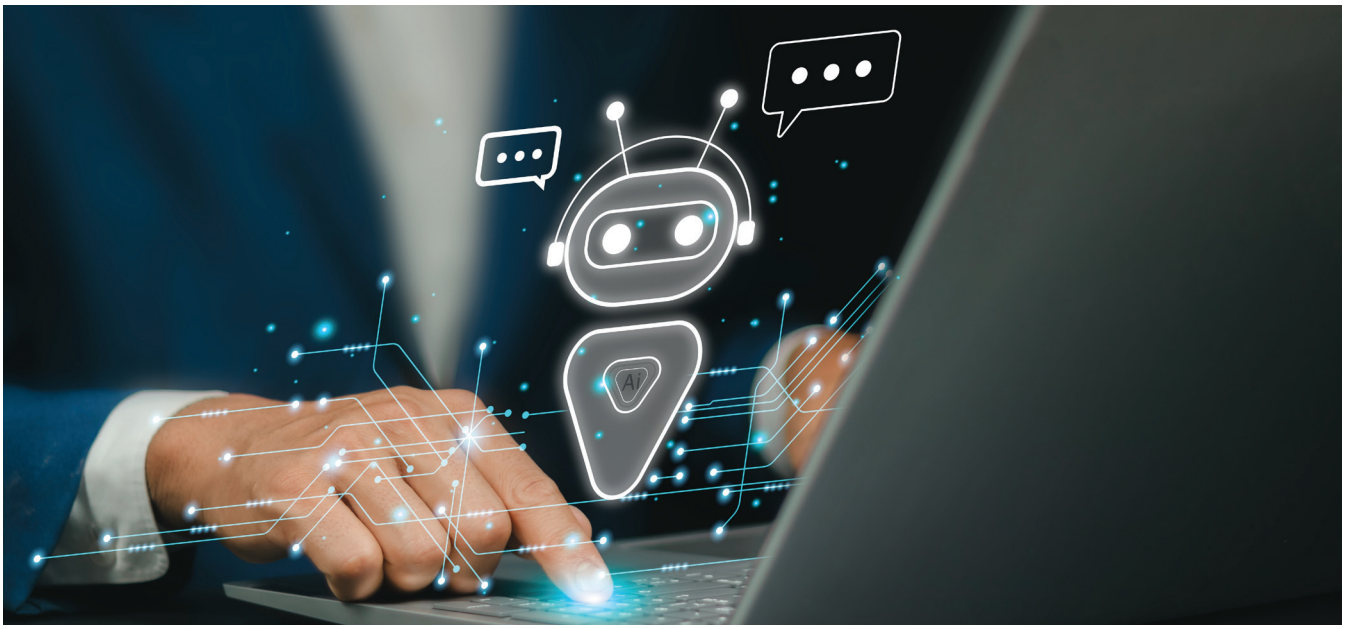
While scale can bring advantages such as access to better tools, stronger talent, and more advanced service offerings, Coventry does not see the market becoming 'winner-takes-all'. Instead, she highlights the continued strength of local MSPs that differentiate through service and relationships. As the market evolves, expectations are rising, with MSPs needing to be more proactive, more strategic, and more specialised in how they deliver value to customers.

Inside Evergreen's next phase of expansion

Looking ahead, Evergreen is entering a more ambitious phase of expansion, with plans to complete between 30 and 40 acquisitions in 2026. Speaking on this trajectory, Coventry points to a growing pool of founders seeking long-term succession options that allow their businesses to continue to thrive. She highlights a shift in how opportunities are being assessed. "Valuation always matters, but it's no longer just a headline figure. It's a compelling deal structure, buyer credibility, and what happens post-transaction." For Evergreen, this reflects a broader focus on consistency and credibility, ensuring its approach continues to resonate as it scales.

Beyond acquisitions, she outlines the key priorities shaping Evergreen's path to its $5 billion revenue target by 2030. Growth will be driven by a combination of continued M&A and strong organic expansion, supported by a deeper focus on enabling its businesses to succeed. This includes investment in areas such as talent, go-to-market execution, and adapting to industry shifts including AI and cybersecurity. International expansion will also play a role, with opportunity across the UK and Ireland alongside growth into regions such as Benelux and the Nordics.

Looking ahead, the market can expect continued expansion, but also consistency. Evergreen will continue to operate on the same principles that have driven its growth to date, including long-term, decentralised ownership and empowered business leaders, with a focus on helping each business grow in a way that remains true to its identity.



AI in action: Applying probabilistic thinking to enterprise workflows

In a recent conversation, Andy MacMillan, CEO of Alteryx, shared insights into how organisations are navigating the growing complexity of AI adoption. Alteryx focuses on helping business analysts put data to work, enabling them to connect, prepare, and operationalise data through analytics and automation.

Why most AI pilots fail to scale

WHILE AI experimentation is widespread, scaling those experiments into production remains difficult. In an exclusive interview with MSP Channel Insights, Andy MacMillan highlighted that fewer than one in four AI pilots successfully transition into real-world use.

The challenges behind this are not surprising. Trust sits at the centre. As MacMillan explained, “If we’re going to use these agents and these AI capabilities, we have to trust the answers, and people are discovering they’re probabilistic by nature, so you get different answers.” In a business context, where precision matters, this variability can quickly become a barrier rather than a benefit.

He added that organisations are still working through this shift, noting, “We’re really spending time trying to help companies figure out how do you establish that baseline of trust.” Without that foundation, it becomes difficult to move AI from experimentation into production in a meaningful way.

Alongside trust, data quality and workflow ownership also play a major role. Without clean, well-structured data and clearly defined ownership of processes, AI struggles to deliver consistent value. MacMillan emphasised the importance of building “the capabilities and the infrastructure that this new AI universe will depend on that gives you the right answer, tells you where it got the right answer, and creates visibility, repeatability, and auditability.”

Alteryx aims to address these challenges by helping organisations establish a trusted data foundation. By doing so, organisations can better understand how AI arrives at its outputs and build confidence in its use.

AI: when ‘probably’ works, and when it doesn’t

The report highlights a shift in responsibility for AI workflows, moving from centralised IT teams to individual lines of business. MacMillan explains that budgets shift as organisations move away from experimental pilots toward embedding AI into core business functions such as finance, sales, and marketing. This transition is accelerating adoption, as teams closest to the business are best placed to identify meaningful use cases and apply AI in ways that drive measurable outcomes.

However, this shift also reflects a deeper understanding of where AI can be safely applied. MacMillan emphasises the importance of recognising AI’s probabilistic nature, noting that “you can ask AI the same question multiple times, and you get different answers each time.” This makes it well suited to exploratory or supportive tasks, but less appropriate in scenarios that demand certainty, such as compliance. As he points out, asking whether something is GDPR compliant and receiving a “probably” is not sufficient.
By placing AI in the hands of those

who understand both the data and the business context, organisations can better balance innovation with control, empowering teams to apply AI effectively while maintaining governance and accuracy.

Extending AI into everyday decision-making

As organisations begin to move past early experimentation, the conversation is shifting towards how AI fits into day-to-day operations. The emphasis is no longer on isolated pilots. It is about embedding AI into the fabric of how work gets done.

"I think initially when AI was this big mega-trend, CEOs found some budget, they handed it to the IT team, the CIO, the engineering team, and we ended up with a bunch of these pilots," MacMillan said. This approach helped organisations explore what was possible with AI, but it did not always lead to meaningful change in how businesses operate.

"We're good at showing the art of what's possible, but what's happening now is we don't want the art of what's possible, we want to change the way the business works and find value." As a result, ownership is increasingly moving closer to the business itself. Teams are now taking a more active role in adopting AI, with a clearer focus on performance, efficiency, and measurable outcomes.

This shift also challenges traditional assumptions about how AI should be deployed. Rather than relying solely on specialist technical roles, organisations are beginning to recognise the value of empowering existing employees, especially those who already understand the business context. By enabling domain experts to work directly with data and AI systems, organisations can apply AI more effectively to real-world problems. Instead of isolated experimentation, teams are using AI to address specific operational challenges within their own functions.

MacMillan describes this as a shift towards bringing AI into structured environments where it can support, rather than disrupt, established processes. "There's a lot of places where a workflow that was orchestrated with software used to stop, and an analyst would go do the work on top. Now an agent can help that analyst do some of that work." This evolution does not remove the human from the loop. Instead, it changes the role they play within it.

The key challenge is deciding where that support is appropriate. Not every process benefits from probabilistic outputs. Some require consistency, repeatability, and strict control. Others can tolerate a degree of variability if it helps speed up insight or reduce manual effort. This distinction is becoming increasingly important as organisations mature in their use of AI.

That learning is not theoretical. It is happening in real time, as teams test, adapt, and refine how AI fits into their workflows. Over time, this builds a more nuanced understanding of where AI delivers value and where it does not.

Learning how to work with AI

As familiarity grows, organisations are developing a more practical understanding of AI's strengths and limitations. This is not just about technology. It is about behaviour, judgement, and experience.

MacMillan captures this shift clearly when he says, "We're seeing this learning curve of people realising what it's good at, what it's not good at." That learning curve is critical. It allows teams to move beyond novelty and begin applying AI in ways that are grounded in real business needs.

This is where the combination of data, context, and human expertise becomes especially powerful. When those elements come together, AI stops being a standalone tool and becomes part of how decisions are made. It supports analysis, accelerates workflows, and helps surface insights that might otherwise take longer to uncover.

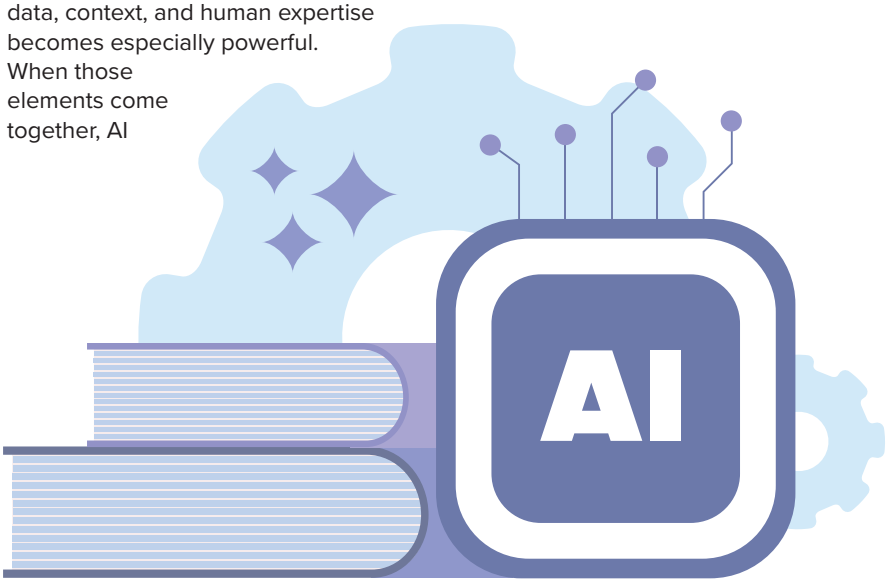
However, this only works if people feel confident in how AI is being used. Trust is not just a technical requirement. It is a practical one. Without it, adoption stalls. With it, organisations can begin to scale AI more effectively across different parts of the business.

Where the next phase begins

Looking ahead, the focus will likely remain on integration rather than invention. The question is no longer whether AI can be used. It is how it can be applied in a way that is both reliable and relevant.

MacMillan's perspective highlights this shift towards practical application. The organisations that succeed will be those that understand how to combine AI with existing processes, rather than attempting to replace them entirely. They will also be those that invest in giving their teams the tools and context needed to use AI effectively.

That means building systems that are not only intelligent, but also transparent and adaptable. It means enabling the people closest to the work to take ownership of how AI is used. And it means recognising that AI, for all its capabilities, still depends on human judgement to guide it.



From firefighting to frameworks: Helping MSPs scale with operational maturity

In an exclusive conversation with Devang Mehta of Infrassist, the focus is on how MSPs can move beyond reactive firefighting and build for sustainable growth. Mehta explains how MSPs must rethink how they define success and bring structure to their operations if they want to scale with consistency and control.

IN THE fast-moving world of managed services, it is easy to get caught in daily tickets, outages, and client demands. However, staying reactive is no longer enough. To scale sustainably, MSPs must rethink how they define success, structure their operations, and adopt technologies like AI.

In a recent conversation, Devang Mehta from Infrassist positioned the company as a growth partner for MSPs, focusing on helping them scale through structured operational and customer success support. He explained that they help MSPs to "attain operational maturity, operational efficiency, and help them achieve success." At its core, the role is about removing operational friction so MSPs can grow with clarity and control.

The hidden challenge of unstructured operations

A key challenge Mehta highlighted is the lack of structure within many MSPs. Processes are often undocumented, leaving teams reliant on informal knowledge and individual expertise. As he put it, "we see that things are not properly documented and there is no way of monitoring what the success looks like."

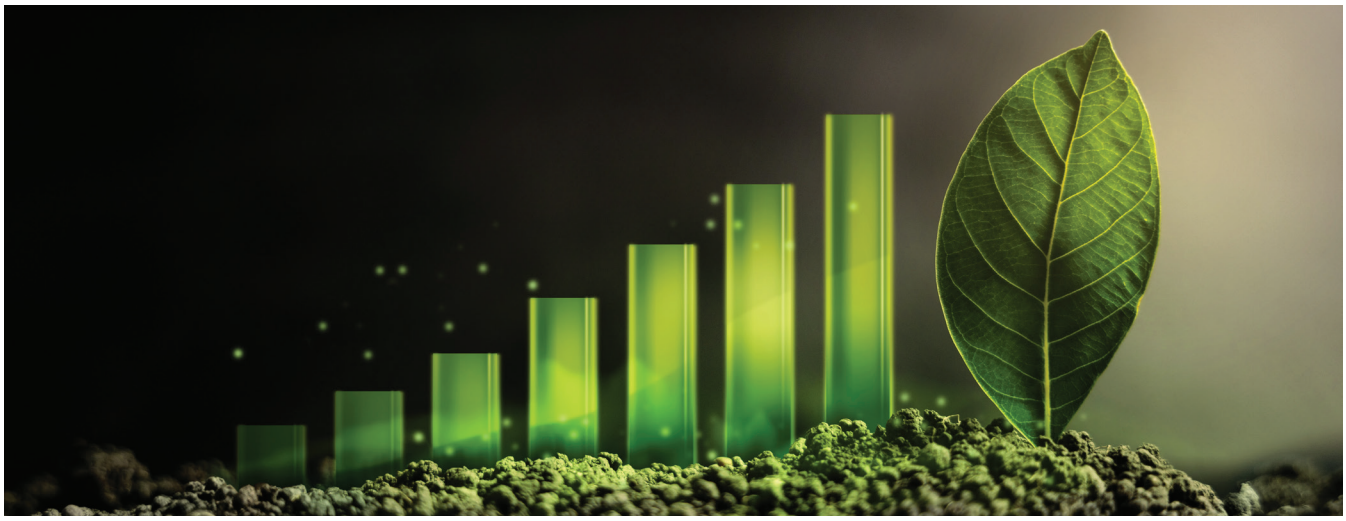
This creates inconsistency and makes it difficult to measure performance effectively. He reinforces this point by asking a fundamental question: "if you cannot define what success looks like, how will you measure the success for you?" Without clear definitions, MSPs are left reacting rather than improving. This lack of structure limits visibility, slows growth, and increases risk across operations.

Building consistency through process and structure

Designing efficient yet high-quality service delivery begins with understanding how work actually happens day to day. This includes identifying priorities, service expectations, and customer tiers early in the process. When MSPs take the time to document and standardise these elements, they begin to create a repeatable model.

Mehta emphasised that this process reveals just how critical structure is, noting that when MSPs map out their operations, they begin to understand how better definition directly improves service delivery and consistency.

This structure is essential for scalability. Without it, every new customer introduces unpredictability, making growth harder to manage. In contrast, having defined processes allows MSPs to replicate success across multiple clients, reducing complexity and improving operational control. Without that foundation, teams are forced into constant reactive mode, leading to inefficiencies and unnecessary pressure.



Transitioning from reactive to proactive customer success

For MSPs looking to move beyond a reactive model, the shift begins with intentional planning and alignment. Mehta explained how Infrassist supports this transition by working closely with MSPs to define goals and track progress over time, stating, "we sit with the MSPs, we define their quarterly goals, and then we constantly monitor with them for the first 6 months."

This structured approach aims to allow MSPs to stabilise their operations before stepping away from day-to-day involvement. Once that stability is achieved, MSP leaders can focus on higher-value activities, such as strategic planning and customer engagement. This transition is important for long-term growth, as it frees leadership from operational bottlenecks and allows them to concentrate on innovation and business development.

Not every process can be rigidly defined, and Mehta acknowledged that operational flexibility is sometimes necessary. However, he argues that having a guiding framework is essential to ensure consistency. Without one, decision-making becomes fragmented. With one, MSPs can maintain control while still adapting to different scenarios. This balance is key to delivering a consistent and reliable customer experience at scale.

How AI and automation are transforming MSP operations

AI and automation are playing an increasingly important role in enabling this transformation. Mehta highlighted how automation tools are already helping MSPs streamline repetitive tasks and improve efficiency. He explained that these technologies are designed to "reduce the repetitive task from the human," allowing teams to focus on more meaningful work. Routine activities such as user onboarding and offboarding can now be automated, significantly reducing manual workload.

One of the most impactful use cases is in helpdesk operations, where AI can categorise and route tickets automatically. Mehta pointed out that "whenever there is a human involved, there are always high chances of making errors." By removing manual intervention from these processes, MSPs can improve both speed and accuracy.

The efficiency gains are significant. Tasks that once required substantial manual effort can now be completed far more quickly. As Mehta highlighted, "a ticket which could take probably 20–25 minutes with human intervention can be done very quickly now, with AI." This not only improves response times but also enhances overall service consistency. Importantly, the goal of AI is not to replace people, but to support them. By removing repetitive tasks, engineers can focus on higher-value work that contributes more directly to business growth.

Planning ahead: the 12–24 month strategic shift

Looking ahead, Mehta emphasised the importance of strategic thinking, particularly when it comes to emerging technologies. He advised MSPs to "look at these AI tools which are coming and take the guidance of the experts on how to implement that into your business."

This is not about reacting, but about planning. He encourages leaders to "sit back and brainstorm what success looks like for you in now 12 to 24 months." This forward-looking approach allows MSPs to build structured roadmaps that align technology, processes, and business objectives.

Mehta also shared that he has seen MSPs develop long-term plans spanning several years, covering areas such as cloud adoption, certifications, and AI integration. This demonstrates that strategic planning is not limited to large organisations. It is relevant to MSPs of all sizes.

What matters most is clarity. Every MSP operates differently, with varying service models and customer agreements. Because of this, there is no universal blueprint for success. Instead, MSPs must define their own path, guided by their goals and supported by the right expertise. This ensures that growth is both intentional and sustainable.

Defining success to drive sustainable growth

Ultimately, MSPs that want to succeed must move beyond reactive operations and invest in structure, strategy, and technology. Without defining success, there is no way to measure it. Without structure, there is no way to scale it. And without planning, there is no way to achieve it.

The age of promises is over, vendors must now lead with evidence-based assurances

Why organisations need proof, not promise, when it comes to third-party security.

BY SAM KIRKMAN, DIRECTOR OF SERVICES, EMEA AT NETSPI

THE TRADITIONAL vendor–customer security relationship has long relied on contractual obligations and irregular audits. Yet in a cyber landscape defined by persistent threats and AI-accelerated attacks, these old assurances are no longer fit for purpose. Trust in a vendor's cybersecurity must be continuously validated, not periodically declared. As attacks become more complex and interconnected digital systems expand, organisations are discovering that vendor risk is their risk, and no chances can be taken.

From empty trust to proven strength

What once worked for security vendors, trust-based compliance, has now become the bare minimum, as well as an outdated approach for modern cyber strategy and data protection. Contracts and written assurances do little to protect organisations in practice, and too often, customers are left with limited insight into the real security posture of their vendors.

In the past few years, we have seen documentation, questionnaires and copious amounts of certifications which has come to overshadow demonstratable robustness. The emphasis has shifted towards ticking boxes, rather than proving strength.

Instead, we need to move from telling to showing; proof over promise.

An evidence-based model of security requires that vendors actively demonstrate that their security approach is measurably robust, measurable, and effective. Compliance does not equal resilience in today's threat landscape, instead, only a consistent and proactive approach will do.

An inherent lack of structural visibility

Of course, most vendors are not deliberately hiding vulnerabilities from customers. The issues are latency and visibility. Point in-time assessments quickly become outdated and lose relevance as systems shifts, technology advances and new code is deployed. A vendor deemed secure at the point of certification or contractual signing can carry material risks just weeks later without a consistent approach to vulnerability management.

Developing comprehensive visibility of vulnerabilities across an organisation is often challenging. Unfortunately, some vendors choose a path of wilful ignorance and blind optimism. This approach saves money for the vendor, at the expense of increasing the risk you take on as a customer.

Even when new vulnerabilities are found, customers often have little to no visibility. An ad hoc approach to third-party security has created a form of structural blindness where risk exists but remains unseen.

To address this, vendors must move towards continuously signalling operational and cyber resilience, rather than relying on static assurances.

Demonstrating in practice: penetration testing

In practical terms, this means on thing: continuous penetration testing.

For vendors performing infrequent or ad hoc tests, security teams struggle to keep up with the rapidly evolving landscape, leaving vulnerabilities unidentified and customers exposed.

By simulating real attacker behaviour, vendors not only demonstrate their commitment to a strong security framework to customers, but it also actively improves their vulnerability management and reduces the very risk of a data breach in the first place. Customers are assured with evidence; vendor's security teams can sleep easy that their weaknesses have been addressed.

For organisations managing dozens, or hundreds, of third-party relationships, this level of visibility is critical to understanding where real risk resides and improving customer relationships.

Calling all CISOs

Supply chains have become prime targets for hostile actors, where data breaches lead to a domino effect of disruption across suppliers, warehouses and manufacturers. For instance, the Jaguar Land Rover attack in September 2025 contributed to reducing real growth across the wider economy of the UK to just 0.1%.

It is critical that vendors begin to demonstrate, through evidence, that they are secure. CISOs are uniquely positioned to raise the bar and lead the charge in demanding third-party security teams are proving their robust cyber management.

To be clear, this is about a greater alignment between vendor and customer, not about punishing the vendors whose security might not be as strong as was hoped. Providing proof over promise represents a fundamental shift in the cybersecurity approach of both CISOs, third-parties and customer organisations.

Where CISOs are leading the charge, companies across all sectors can build up their resilience.

Proof over promise

This is a chance for CISOs to raise the bar for vendors and lead the c harge in demanding stronger proof of resilience and robust frameworks. Vendor security claims should be backed by measurable, ongoing validation, rather than ad hoc, periodic audits or unchecked promises.

With AI becoming weaponised, organisations need dynamic defence strategies. Continuous pentesting, filling in regulatory gaps and open, honest and structured communication between vendors and customers are essential to shifting from reactive defence to proactive resilience.

In modern cybersecurity, confidence is not a statement, but a sustained demonstration.

Creating pathways into tech for girls means starting early

The theme for International Women's Day this year is "Give to Gain", and for me, it perfectly captures both my journey into cybersecurity and what the technology industry must do next.

BY SAMANTHA JENNINGS, HEAD OF OPERATIONS, AVELLA

CYBERSECURITY has become one of the most critical frontlines affecting everyday life. From the resilience of the UK's critical national infrastructure to the protection of essential public services, the work we do in cyber impacts families, communities, and national stability. At Avella, where we support central government and organisations operating as Operators of Essential Service (OES) and within the UK's CNI, that responsibility is tangible.

Yet despite this, cybersecurity still does not reflect the society it protects. Gender imbalance remains a persistent issue, particularly in technical roles. If we are serious about safeguarding a diverse society, our industry must look more like it.

A non-linear route into cyber

My own path into cybersecurity wasn't traditional. I didn't study computer science or start out as a coder. I began with a love of English - stories, poetry, and the power of language to connect people. I even had poems published in local magazines at school. Alongside that, I studied Business and Finance, gaining a BTEC National Diploma that immersed me in marketing, accounting, and business law.

I also developed, at a young age, a self-imposed belief that I "wasn't good at maths", despite teachers assuring my parents that I was perfectly capable. Looking back, that was probably my first experience of imposter syndrome.

My career took me into recruitment advertising, where I built teams and proposed new operational structures to improve efficiency. At 20, I wrote a proposal to a managing director outlining the need for an administration manager role to bring consistency across three client service teams. Curiosity has always driven me to ask: "Is there a better way?"

There was even a period working abroad as a holiday entertainer, including stepping onto a stage with no prior experience, and once dressing as a Christmas elf, escorting families to Lapland. It may sound unrelated to cyber, but it taught me confidence, adaptability, and resilience. Skills I draw on daily in an industry where the threat landscape is constantly shifting.

I moved into cybersecurity through a networking conversation. Crucially, I was welcomed. The partners at Avella recognised that operational clarity, communication, and relationship-building were not peripheral skills; they were crucial to keep things together.

Cybersecurity does not only need deep technical expertise. It needs people who can translate complexity into clear language. It needs empathy, creativity, and the ability to connect policy, process, and people. In fact, some of the most effective cyber professionals I work with come from creative backgrounds. When adversaries constantly evolve, creative thinking becomes a security asset.

Why diversity for tech industries makes sense

Following events like 9/11 and the attack on the Twin Towers, there was a global

reckoning across many sectors about the importance of diversity in thinking and perspective. A realisation that security requires diverse "frames of reference" and to challenge, reason, and cross-pollinate ideas.

Threat actors do not think uniformly. They adapt, innovate, and exploit assumptions. To defend effectively, we need diverse cognitive approaches, lived experiences, and problem-solving styles. If everyone in the room has followed the same educational and professional path, we risk seeing only part of the picture.

Put simply, cyber must reflect the society it protects. And technology should reflect the societies it serves.

Early Intervention could make all the difference

One of the biggest challenges women face in this industry is underrepresentation. Walking into a room and not seeing anyone who looks like you can amplify imposter syndrome. I have felt it myself, particularly when transitioning into this highly technical, male-dominated field.

Women often hesitate to apply for roles unless they meet every listed requirement, while others may apply regardless. That confidence gap forms early, long before career decisions are consciously made.

This is why early intervention matters.

I strongly support initiatives like Festival of The Girl, a not-for-profit organisation that creates spaces where girls can try activities traditionally labelled "for boys," from coding and engineering to sport and leadership. Crucially, these experiences happen before career pressures or stereotypes fully take hold. Girls are simply encouraged to explore.

What these initiatives give is belief.

And belief changes trajectories.

What Give to Gain means in practice

For me, "Give to Gain" means giving time, visibility, and encouragement, especially to girls who may not yet see themselves in tech.

It means mentoring. It means reviewing job descriptions for unnecessary barriers. It means challenging jargon-heavy environments that unintentionally exclude. It means focusing on skills and mindsets, not just technical checklists.

Over the past year, as someone relatively new to cybersecurity, I've joined welcoming peer networks such as Women in CyberSecurity (WiCyS). The support, openness, and shared experience have been invaluable. Community matters.

Within organisations, leaders can take practical steps now:

- Audit recruitment language to remove bias and emphasise transferable skills.
- Broaden entry pathways beyond purely technical degrees.
- Create visible role models across operational, strategic, and technical functions.
- Invest in outreach with schools and community groups.
- Encourage mentorship and sponsorship programmes internally.

Letting curiosity flourish

As a leader, I believe empathy is not a soft add-on; it is a commercial imperative. In professional services, our people are our product. Enabling them to bring their best selves to work directly impacts client outcomes and, in our case, national resilience.

Equally important is curiosity. You don't need to have every answer. You need to be willing to ask the questions, even the uncomfortable ones. Curiosity has shaped every stage of my career, from advertising to cyber.

Leading to inspire

Today, my greatest inspiration is my 11-year-old daughter. I want her generation to see cybersecurity and technology more broadly as a space of possibility, not limitation.

Breaking stereotypes cannot start at university recruitment fairs. It must start in primary school classrooms, in community events, in the language we use, and in the examples we set.

If we give our time, our visibility, and our encouragement now, we gain stronger teams, better decisions, and more resilient systems tomorrow.

Cybersecurity protects the fabric of modern society, and technology underpins every facet of our day-to-day lives. It deserves and requires the full breadth of that society's talent.

That is something worth giving everything for.

Why most agentic AI projects fail, and how to avoid being one of them

As businesses get used to using generative AI, attention is quickly turning to agentic AI.

BY MARTIN TOMBS, FIELD CTO EMEA, QLIK

These systems are designed to plan tasks, interpret information and take action within defined guardrails. In theory, this moves AI from a tool that assists employees to one that helps run parts of the business.

Investment is rising fast, with McKinsey predicting that the agentic AI market will rise from roughly $5-7 billion in 2024 to over $199 billion by 2034. But many businesses are finding it harder than expected to turn early pilots into something reliable and useful at scale.

Gartner predicts that more than 40% of agentic AI projects will be cancelled by the end of 2027. Meanwhile, Qlik found that 97% of organisations have committed budget to agentic AI, but only 18% are fully deploying it.

Many see the potential, yet practical deployment still proves difficult when systems are expected to operate reliably in real business environments.

When AI starts acting inside workflows

Early generative AI tools largely acted as assistants. Employees used them to answer questions, summarise documents or draft content. If the response was slightly wrong, the impact was usually limited.

Agentic systems operate differently. They can interpret signals, recommend next steps and carry out tasks across enterprise systems. In practice, this might involve identifying unusual changes in financial performance, triggering a supply chain adjustment or initiating an operational workflow.

Once AI interacts directly with business processes, the margin for error becomes much smaller. A generative AI recommendation can be reviewed before action is taken, but an automated workflow requires far greater confidence in the information and logic behind it.

This is where many businesses discover their underlying data foundations are not ready.

Fixing the data foundations first

The most common reason agentic AI projects stall is a lack of data maturity. Agents depend on a consistent and trusted view of information across the organisation, yet many businesses still operate with fragmented data, duplicated sources and unclear ownership. In these conditions, even the strongest AI models struggle to produce outputs that teams can comfortably rely on.

Unstructured information adds another layer of complexity. Internal documents, emails and knowledge bases often contain useful context but rarely have clear ownership. That makes it difficult to verify whether the information is current, accurate or even still relevant when an AI agent draws on it.

As agents begin interacting with operational systems, these weaknesses become more visible. If the information feeding those systems is inconsistent or outdated, the reliability of the agent's outputs quickly comes into question.

Strengthening those data foundations is often the first step before agentic AI can be deployed with confidence.

Who is responsible when AI takes action

As agents take on more responsibility, governance becomes a practical issue rather than a theoretical one. Organisations need clear answers to some basic questions. Who owns the data feeding the system? Who signs off on actions an agent takes? And when should a person step in and review a decision?

Clear accountability helps teams trust the system implemented and reduces the risk of mistakes. It also makes it possible to understand how decisions were reached, which matters when AI outputs affect revenue, compliance or business planning.

Regulation can help provide structure here. Europe's AI rules, including the EU AI Act, aim to set expectations around transparency, accountability and risk early in the development of AI systems. While regulation is sometimes seen as slowing innovation, clearer rules can make it easier for organisations to use AI responsibly.

Getting AI tools to work together

Another challenge emerging with agentic AI is the growing number of assistants operating across a business. Most organisations are not relying on a single model or platform. Different teams often use different AI tools depending on their needs, from analytics platforms to internal systems and external assistants.

For agents to work effectively in that environment, they need secure ways to access trusted data and interact with other systems. Without that connection, agents operate in isolation and their usefulness quickly becomes limited.

This is where shared standards are starting to play a role. Technologies such as Model Context Protocol (MCP) allow AI assistants to connect with enterprise platforms while keeping access controls and governance in place. Instead of building custom integrations for every tool, organisations can expose data and analytics through consistent interfaces that different assistants can use.

As more AI tools enter the workplace, making sure they can work together and access reliable data will become increasingly important. Organisations that plan for this early will find it much easier to scale agentic systems across the business.

Building agentic AI that works

Agentic AI has the potential to completely change how organisations operate for the better. But success depends on prepare the systems underneath first, putting the right data, accountability and controls in place before scaling beyond pilots.

Why transformation fails: The missing link between technology, people and culture

Digital transformation continues to dominate boardroom agendas. According to Gartner, 87 per cent of business leaders prioritise digital transformation initiatives

BY LORENZO ROMANO, CEO OF GCX MANAGED SERVICES

DELOITTE estimates that as much as $1.25 trillion in enterprise value hinges on their success. Yet despite this focus and investment, many programmes stall, overrun or lose momentum before achieving any measurable results.

In reality, contrary to popular belief, most failures are not due to defective technology. More commonly, transformation efforts struggle because organisations treat their people and culture as secondary concerns rather than as essential elements of the design process.

Technology alone does not transform organisations

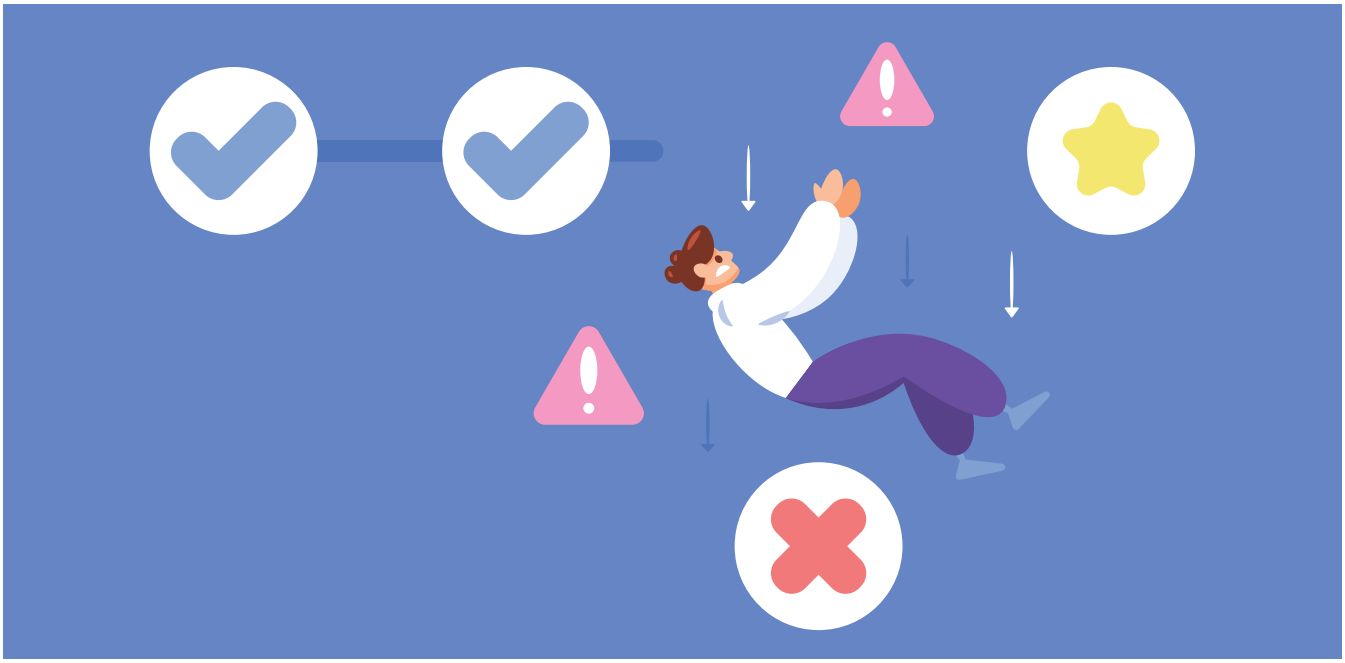
It is easy to view transformation as a technical challenge. After all, modern architectures promise agility, scalability and resilience. Vendors highlight performance metrics and integration capabilities, while project teams develop detailed roadmaps focused on deployment milestones.

But transformation is not just about infrastructure. It also requires changes in behaviour, accountability and mindset. When these shifts are not deliberately designed and supported, even the most advanced solutions can struggle to gain traction.

Enterprise networking serves as a useful example. Transitioning to Secure Access Service Edge (SASE) represents a significant architectural shift. By merging network and security into a unified, cloud-delivered framework, SASE promises simplified management, consistent policy enforcement, and an improved experience for distributed workforces. On paper, the case for SASE is compelling, but in practice, adoption can be more complex due to organisational friction rather than technological limitations.

Bridging the cultural divide

Historically, network and security functions have operated with different priorities and success metrics. Network teams focus on uptime, latency and connectivity performance, while security teams prioritise risk reduction, compliance and incident prevention. Although both functions



support business continuity, their perspectives often differ, and these differences become more pronounced in converged architectures like SASE.

Overlapping responsibilities and blurred decision-making authority can quickly create tension between the two teams. For instance, a security control that introduces minor latency may be necessary for compliance, but network teams may view it as a problem. Budget discussions can become territorial, and legacy governance structures may no longer be effective. Each of these challenges is cultural rather than technical, highlighting the need for deliberate alignment between network and security functions.

Why ownership and incentives matter

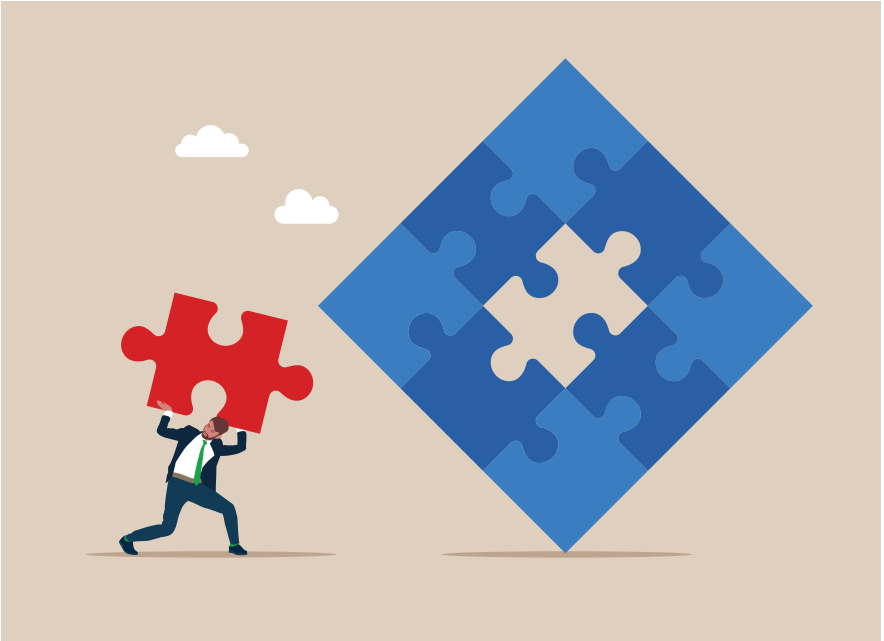
Ambiguity around ownership is a major source of friction. In converged environments like SASE, it can be unclear whether accountability for a platform lies with network teams, security or a newly established function. Without clear lines of responsibility, decision-making slows, and accountability becomes diffuse.

Incentives further complicate this issue. If teams are still evaluated against outdated metrics, collaboration suffers. Individuals tend to prioritise what they are rewarded for, and misaligned incentives can turn organisational transformation into a negotiation between departments rather than a coordinated effort.

Resistance to change exacerbates these challenges. This usually arises from fear and confusion: uncertainty about evolving roles, which skills will remain relevant, and what new competencies will be required. Leaders who address these concerns transparently, align governance with incentives, and build trust in the change itself will see hesitation diminish.

Making the case for change

A clear, credible case for transformation is essential. Technical advantages alone do not motivate engagement. Teams need to understand how new architectures support broader business objectives, whether enabling secure hybrid work, accelerating cloud adoption, or improving visibility across distributed environments.



Framing these outcomes as enterprise priorities, rather than simply departmental victories, builds trust. Change management must start at the outset by mapping current skills to future requirements, identifying training needs, and involving cross-functional leaders in shaping the roadmap. This approach communicates that transformation is a collaborative journey, not a top-down mandate.

Designing for collaboration

Enterprise networks are shaped as much by human interaction as by technology. Factors such as how incidents are escalated, how risks are prioritised, and how trade-offs are negotiated all influence whether a transformation succeeds or stalls.

Designing collaboration means establishing shared metrics, redefining governance, and aligning incentives across traditionally siloed teams.

Resilience is both technical and cultural: a well-designed platform will underperform without clarity, trust, and cohesion among those operating it. Conversely, organisations that cultivate cross-functional collaboration can often derive greater value from the same technology.

Modern frameworks such as SASE offer real opportunities to simplify operations and enhance security, but their long-term effectiveness depends on cultural alignment. Transformation is most successful when organisations invest in their people as deliberately as they invest in their technology.

The missing link

As spending on transformation initiatives continues to rise, the differentiator will no longer be the sophistication of tools, but rather the alignment of people, incentives and culture around shared objectives.

The future of enterprise modernisation will be defined less by features and more by trust – between teams, between leadership and frontline specialists, and between strategy and execution.

This is also where long-term strategic partners can make a decisive difference. External partners who embed themselves within the organisation provide continuity through inevitable periods of change, preserving critical expertise, reinforcing best practices and keeping programmes moving forward even as internal structures or leadership evolve.

Businesses that approach transformation with equal attention to behaviour, collaboration, and shared accountability as they do to technology will adopt modern architectures more effectively and build the resilience needed to sustain them. Ultimately, long-term transformation success depends on cultural alignment as much as technical capability.

Building cyber resilience through backup consolidation

As cyber threats accelerate, organisations are re-evaluating the weakest parts of their IT estates, with backup environments increasingly coming under scrutiny.

BY SCOTT ASHENDEN, HEAD OF SECURITY AND INFRASTRUCTURE AT TEAM MATRIX

SYSTEMS that once met operational needs often struggle to keep pace with hybrid infrastructure, cloud adoption, and the sophisticated ransomware tactics now targeting backup repositories directly. For organisations operating across multiple sites or with inherited technology stacks, fragmentation can create gaps that attackers exploit.

This was the challenge facing Team Matrix, a UK recruitment platform operating across Milton Keynes and Basingstoke. As its environment grew more complex, the company's small infrastructure team, responsible for supporting hundreds of staff and workloads across Azure and AWS, had to pursue a more unified approach to data protection. What began as a straightforward backup setup gradually grew into two competing strategies, and a potential barrier to cyber resilience.

When growth creates invisible risks

Matrix expanded into its second site through acquisition, inheriting a backup model markedly different from its existing one. The Milton Keynes site relied on an external MSP for backups, while Basingstoke used Azure Backup managed internally. Both approaches worked in isolation, but combined they created familiar challenges, including inconsistent retention policies, limited visibility across sites, increased pressure on a small IT team, disjointed audit trails and a higher likelihood of backup compromise during ransomware attacks.

This fragmentation was a significant issue because ransomware today is designed to disable recovery before encrypting production systems. Without unified visibility or consistent protection methods, organisations struggle to verify the integrity of backup data or guarantee reliable recovery. For Matrix, the risks were becoming clear as uneven protection, excessive manual oversight, and uncertainty over recovery speed emerged.

Moving toward a unified and resilient backup strategy

To correct the imbalance, Matrix chose to consolidate both sites into a single backup and recovery platform built on Rubrik's technology and supported by Assured Data Protection. The objective went beyond simplifying management and focused on strengthening the organisation's ability to withstand fast-moving ransomware attacks. Key requirements included immutable backups, automated workflows for compliance, a consistent recovery experience, and the ability to operate confidently with a small IT team. Unifying the backup environment provided exactly that. Deployment was rapid, with backups operational within

hours, immediately closing visibility and consistency gaps between the two locations.

What a unified model delivered

Once consolidated, Matrix gained a resilience-focused foundation that addressed the core weaknesses of its previous setup. Centralised visibility allowed all backup jobs, retention policies, and recovery points to be managed in one place, enabling faster validation and continuous monitoring.

With a single platform underpinning both sites, the company gained a consistent, tested path to restore critical systems quickly in the event of an incident. Scott Ashenden, Head of Security and Infrastructure at Matrix, noted that the shift offered "real peace of mind," especially as backups were running within hours of onboarding.

The market forces driving backup consolidation

Matrix's experience reflects a growing pattern among mid-sized organisations. Marked by a shift away from mixed, inherited backup systems toward unified resilience platforms. Several trends are driving this change. Ransomware has evolved to actively target backups, with attackers aiming to corrupt or destroy recovery data early in an intrusion. Fragmented systems create more entry points and fewer controls, making it easier for attackers to compromise backup integrity. At the same time, the rise of hybrid cloud means data now spans on-premises infrastructure, Azure, AWS, and SaaS platforms. Location-specific tools struggle to provide consistent protection across these environments, creating blind spots that unified platforms are better equipped to eliminate.

By consolidating its environment, Matrix was able to address all these trends at once, creating a simpler, more secure, and more resilient foundation for its data protection strategy.

Why consolidation strengthens overall cyber defence

For Matrix, reducing complexity was important, but strengthening the organisation's resilience was the real outcome. Guaranteed recoverability became a defining benefit, as the combination of immutable and unified backups significantly reduced business risk and ensured data could be restored even in the face of ransomware attacks.

The organisation also gained more consistent audit trails, making it far easier to demonstrate compliance and produce evidence during assessments. Incident readiness improved as well; with a centralised platform underpinning both sites, the company could accelerate response and recovery efforts and rely on a predictable, tested path to restoration.

As Matrix continues to grow, its protection can now scale without introducing new silos, tools, or operational burdens. The consolidation also gave the internal team confidence to focus on longer-term strategic projects, knowing that core data protection and resilience requirements were reliably managed.

Preparing for the next wave of cyber threats

The lesson from Matrix is simple. Operational growth without consolidation can weaken cyber resilience, especially as attackers target backup repositories directly. By unifying data protection under a single, resilient platform, organisations can eliminate blind spots and build the foundation for stronger, faster recovery. As cyber incidents become more disruptive and regulators demand greater assurance, the ability to recover cleanly and confidently will define resilience. Organisations that modernise their backup strategy today will be better equipped to navigate whatever comes next.

Cyber insurance is an MSP growth tool: Most of the channel is still treating it as a cost

Most MSPs think about cyber insurance as something they have to buy. A compliance requirement. A line item on the renewal list. Something the accountant asks about once a year and then files away until next time.

BY RYAN WINDT, HEAD OF GROWTH MARKETING AT SEEDPOD CYBER

THE MSPs growing fastest right now are thinking about it differently. They are using cyber insurance as a client conversation tool, a proposal differentiator, a contract protection mechanism, and in many cases a direct revenue line. The difference in outcome between those two postures is not marginal. It is structural.

This piece is for MSPs who already understand they need their own coverage and want to understand how to turn the insurance conversation into a business advantage.

The market has shifted under the channel's feet

A few years ago, an MSP raising cyber insurance in a client meeting was unusual. Today it is becoming expected. Small and mid-sized business clients are being asked about coverage by their accountants, their banks, their boards, and their largest customers. Supply chain security requirements, SOC 2 audits, and vendor onboarding questionnaires now routinely ask whether a business carries standalone cyber liability insurance.

That shift creates a clear opening for MSPs who are ready for it and a real vulnerability for those who are not. The MSP that arrives at a prospect meeting already fluent in what cyber insurance covers, what it costs, and what security controls are required to qualify for it is in a fundamentally different position than the one that hands that conversation off to a broker and moves on.

The question is no longer whether cyber insurance is part of your client conversations. It is whether you are the one leading those conversations or getting left out of them.

Three models for generating revenue from client coverage

MSPs generate revenue from client cyber insurance through three distinct approaches, each suited to a different level of investment and involvement.

Referral partnerships are the lowest-friction entry point. You refer clients to a cyber insurance specialist, earn a referral fee for each placed policy, and maintain visibility into what your clients are buying. No licensing is required in most states, and the

overhead is minimal. The trade-off is limited influence over the product and a lower revenue ceiling.

Embedded quoting with a specialist partner is a step up. You run a structured insurability review with each client, collect the relevant application information, and submit it to an insurance partner who handles the underwriting and placement. You earn compensation on placed policies. You are positioned as the advisor who made the introduction. This model works particularly well at QBR time, when you are already reviewing the security stack and the conversation flows naturally.

Full agency licensing is the high-investment, high-return model. Some larger MSPs pursue their own insurance agency license and write coverage directly, capturing full commission and owning the client relationship end to end. It requires investment in licensing, E&O coverage for the insurance activity itself, and process infrastructure. It makes sense at scale. It is premature for most MSPs under $10M in managed services revenue.

The right model depends on bandwidth and how embedded you want the insurance conversation to be in your service delivery. Starting with referral or embedded quoting is the right call for most of the channel.

The insurability review: the highest-value thing you are not doing at QBRs

The most effective integration point for cyber insurance in an MSP business is the insurability review. This is a structured conversation, run annually and ideally tied to the regular QBR cycle, that walks the client through four questions.

Do you have cyber insurance, and is it adequate? Many small business clients have a cyber endorsement attached to a BOP or a general liability policy. Those endorsements are almost always inadequate. Coverage limits are low, exclusions are broad, and incident response support is minimal or non-existent. Helping a client understand what they have versus what they actually need is a high-value advisory service. It is not a sales pitch.

Are your current controls enough to qualify for good terms? Cyber insurance underwriting has tightened significantly over the past three years. Clients who cannot document MFA, EDR, and tested backups are either getting declined, paying substantially higher premiums, or buying policies with exclusions that would gut a real claim. As their MSP, you are the most qualified person in the room to answer this question, and you have the tools to document it.

What gaps exist, and what is the cost of closing them? This is where the insurance conversation becomes a technology conversation. If a client needs immutable backups and managed detection and response to qualify for the coverage their largest partner is now requiring them to carry, that is a service proposal rooted in third-party authority, not just your recommendation. Close rates on proposals tied to insurance requirements are consistently higher than proposals tied to general security recommendations.

What would a breach actually cost your business? Most small business clients have never run this math. Walk them through a realistic scenario: ransomware hits on a Thursday morning, systems are down for five to ten business days, forensic investigation is required, legal counsel is engaged, notifications go out. Put dollar amounts on each component. Show them what their current coverage would pay. Show them the gap. This is not fear-based selling. It is helping a client make an informed decision about risk transfer, which is exactly what a trusted advisor does.

When a client does not have cyber insurance and suffers a breach, their recovery options are narrow. Forensic investigation, legal counsel, notification costs, and downtime losses are all out-of-pocket.

The liability angle: why client coverage protects you too

This is the part of the conversation most MSPs skip, and it is the part that creates the most exposure.

When a client does not have cyber insurance and suffers a breach, their recovery options are narrow. Forensic investigation, legal counsel, notification costs, and downtime losses are all out-of-pocket. The clients in that position are the most likely to look for someone else to absorb a portion of those costs. The MSP with administrative access to their environment is the most visible candidate.

When a client has their own cyber insurance, the dynamic is completely different. Their insurer brings in a breach coach, a forensic firm, and legal counsel. The financial exposure is managed through a professional claims process. The client has a contractual relationship with their insurer to pursue, not an emotional one with you to blame.

Adding a cyber insurance requirement to your Master Service Agreement does not fully insulate an MSP from liability. But it meaningfully reduces the exposure and signals to underwriters evaluating your own submission that you run a professional operation. A growing number of cyber insurers are now treating MSP-required client coverage as a positive underwriting factor when evaluating MSP applications.

A minimum standard worth including in every MSA: clients must maintain standalone cyber liability insurance with limits appropriate to their revenue and data exposure; they must provide a certificate of insurance upon request; and they must notify you within a defined window if coverage lapses. Most clients will comply without pushback once the requirement is framed as a risk management standard rather than a contract formality.

Insurance requirements as a tool for getting security upgrades approved

One of the most persistent frustrations in the managed services channel is the client who acknowledges a security gap but will not approve the budget to close it. The insurance angle often breaks that logjam in a way that internal recommendations alone cannot.

When an underwriter requires a control as a condition of coverage or a lower premium, that requirement carries authority that an MSP recommendation does not. Clients respond differently to "your insurer is requiring MFA on all admin accounts" than they do to "we have been recommending MFA on all admin accounts for two years."

MSPs can use this deliberately. Running clients through a standard insurance readiness checklist before their renewal period, documenting the gaps, and showing what closing each gap would mean for their premium and eligibility shifts the conversation from selling a security tool to helping the client protect an asset they already value: their coverage.

This dynamic plays out most clearly with four controls.

Immutable backups are now an explicit underwriting requirement at most carriers, not a general recommendation. Clients running backup solutions that could be encrypted or deleted in a ransomware event are either ineligible for coverage or paying for a policy that will not perform at claim time. If your backup stack meets the standard, that is a differentiator. If it does not, that is a proposal.

Managed detection and response sits in a different underwriting tier than traditional endpoint protection. A client running legacy antivirus is viewed differently than one with EDR and 24/7 monitoring. If you offer MDR, the insurance incentive creates a financial case for the upgrade that security value alone rarely closes.

Documented phishing simulation is increasingly a requirement, not a recommendation. If you run phishing simulations and can export records of participation and outcomes, that is a deliverable you can include in a client's renewal documentation file.

Privileged access management is a harder sell to small clients on security merit alone. It becomes an easier conversation when a client's largest customer is requiring them to carry a $3M cyber policy and the underwriter is asking about PAM on the application.

Why this makes clients stickier

The business case for the insurance-integrated model is not just revenue. It is retention.

Clients who have had a cyber insurance conversation with their MSP, who understand their coverage, and who have the controls in place to qualify for good terms are meaningfully harder to churn than clients who are treated as purely technology accounts. The insurance relationship creates annual touchpoints that are advisory in nature, not reactive. Renewal time becomes a security review. Gaps in coverage become proposals for services that have clear business value.

And if an incident does occur, a client who went through a proper claims process with adequate coverage comes out the other side in a better position than one who did not. The outcome is better. The relationship is stronger. Referrals follow from clients who feel protected, not from clients who feel abandoned.

The MSPs doing this well are not selling insurance. They are selling confidence. That is a more durable competitive position than price, toolset, or response time.

Where to start

The lowest-effort entry point is the insurability review applied to your existing client base. Pick five accounts. Pull up a standard cyber insurance application. Walk through the questions with each client. Document what you find.

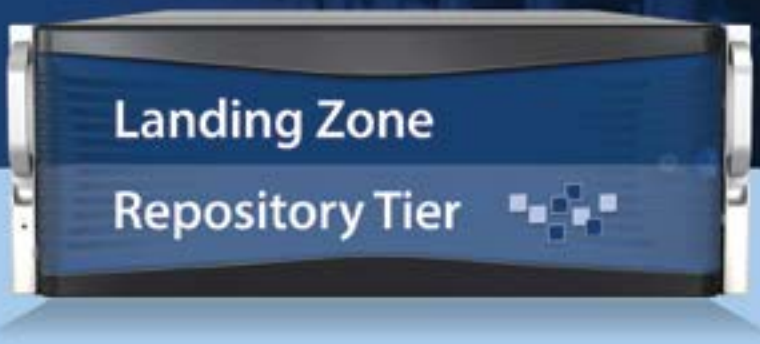
The process will surface gaps you can close, coverage you can improve, and conversations you have been leaving on the table. It will also give you direct evidence of what underwriters are asking for in 2026, which makes every subsequent conversation more credible.

From there, identify a cyber insurance partner who understands the managed services channel specifically: the aggregation risk profile, the Tech E&O coordination questions, and the client coverage dynamics that are unique to MSPs. The generic market does not serve this segment well. The right partner makes the model work. The wrong one makes it harder than it needs to be.

Clients who have had a cyber insurance conversation with their MSP, who understand their coverage, and who have the controls in place to qualify for good terms are meaningfully harder to churn than clients who are treated as purely technology accounts. The insurance relationship creates annual touchpoints that are advisory in nature, not reactive

EXAGRID
Tiered Backup Storage

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

MSP CHANNEL AWARDS
2025 WINNER

- BACKUP & DR INNOVATION OF THE YEAR
- STORAGE HARDWARE INNOVATION OF THE YEAR
- STORAGE VENDOR OF THE YEAR

Thank you so much to all who voted, and congratulations to our fellow MSP Channel Awards 2025 winners!

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

LEARN MORE >