IT EUROPA

IT Europa's **High Growth 100 – Cybersecurity** analyses how the UK's fastest-growing MSPs have made gains in this quickly evolving but increasingly lucrative sector.

High Growth 100 in Cybersecurity

Insights that give you an edge

Contents

Introduction

This report collates detailed financial data, insights from industry leaders, and conversations with cybersecurity experts to explore the trends shaping the landscape and the strategies keeping high-growth MSPs ahead of the curve. As part of the High Growth series, the report serves as a valuable resource for companies, stakeholders, and investors looking to understand the growth dynamics in this sector. We also extend our thanks to those who agreed to be interviewed, including Littlefish, Vizst Technology, and Trustmarque. It is from their insights that the opportunities and roadblocks explored in this report have been identified and demystified.

Methodology

In this report, IT Europa conducted a comprehensive analysis of the UK's top-performing MSPs delivering profitable cybersecurity services. Our screening process began with a pool of 1,500 companies, from which we identified the most profitable based on key financial indicators. By reviewing Profit & Loss accounts, we assessed turnover growth from the latest available financial year. For companies with undisclosed turnover, we evaluated solvency ratios using Total Assets and Shareholder Funds to highlight those with the strongest financial stability. Ultimately, IT Europa ranked and distilled these insights into a list of the top 100 cybersecurity MSPs in the UK.

Market snapshot

The UK's cybersecurity sector generated revenue of £11.9 billion in 2024, up from £10.5 billion the previous year, according to data from the Department for Science, Innovation and Technology (DSIT). This surge in demand stems from UK businesses lacking cybersecurity skills with DSIT estimating that staff at approximately 637,000 businesses (44%) are unable to carry out the basic tasks laid out in the government-endorsed Cyber Essentials scheme while also not using external cybersecurity providers. Furthermore, approximately 390,000 businesses (27%) have gaps in advanced skills, such as penetration testing.

Top 100 in cybersecurity

The High Growth 100: Cybersecurity report highlights a cohort of MSPs with an impressive average annual growth rate of 39% and an average solvency ratio of 58%. Each organisation boasts a turnover north of £5m and has maximised operational efficiency, with an average of 182 employees driving exceptional results. What sets these MSPs apart is their elevation of cybersecurity as a key pillar of their growth strategy, not just a bolt-on component of a wider managed service offering. These organisations have deepened their portfolios by partnering leading security vendors, most

Meet the High Growth 100 in Cybersecurity...

1. A&O IT Group
2. Acora
3. ADA Networks
4. Adarma
5. Agile IT
6. Air IT
7. Altiatech
8. AMC-IT Solutions
9. AMJ IT
10. Ampito Group LLP
11. Annodata
12. Blue Rock IT
13. Bridewell Consulting
14. Bytes Technology Group Plc
15. C & S Parker
16. Capito
17. Centerprise International
18. Central Support Technologies (CST)
19. Central Technology
20. CF Systems
21. Claranet Group
22. Clear Thinking IT Solutions
23. CloudCoCo Group Plc
24. Concorde Technology Group
25. CSG Computer Services
26. Data Productions +B27:B47
27. Data Systems (Computers)
28. Eurotek UK
29. Excellence IT UK
30. Exmos
31. Fitzrovia IT
32. Foster's Computer Services
33. FSP Consulting Services
34. Genmar (UK)
35. Halifax Computers
36. Hixon Group
37. Holistic IT
38. Icon I.T. Services
39. Icris Managed IT Services
40. Infologic
41. Innovate
42. Interactive Data Technology (IDT)
43. IT Naturally
44. ITC Global Security
45. IT-Worx Solutions
46. Kascade (ComputerWorld Systems)
47. Kick ICT Group
48. LIMA Networks
49. Little Fish (UK)
50. Logicalis Group
51. Lyon Managed Services
52. Managed247
53. Marsden's Computer Systems
54. Mason Infotech
55. Max Cloud Services
56. Mercury Systems Engineers
57. Mirus IT Solutions
58. Modern Networks
59. Monument IT Consulting
60. MT Services Computer Systems
61. MTI Technology
62. Network (London)
63. Nimbus Blue
64. Node4
65. Nomios Uk&I
66. Ontraq
67. P2 Technologies
68. Pentesec
69. Performanta
70. Phoenix Software
71. Proact IT UK
72. Pxosys
73. QD Tech
74. Quiss Technology
75. Quorum Cyber Security
76. Razorblue Group
77. Redcentric
78. Redinet
79. Siarp
80. Sisl Infotech (UK)
81. Smallworld IT (UK)
82. Spherica Business Solutions
83. Spirit UK Managed Services
84. Systal Technology Solutions
85. Sytec - Systems and Technology
86. TechNet Easy Services
87. TheLogic
88. Tiva IT Solutions
89. Toro Risk Solutions - Global
90. Transparity Solutions
91. Trustmarque Solutions
92. Ultima Business Solutions
93. Uptech
94. Utilize
95. vIT4u
96. Vitanium Cloud
97. Vizst Technology
98. Wanstor
99. Webby Tech
100. Xpertex

commonly Sophos and Fortinet, positioning themselves as trusted advisors in an ever-evolving digital landscape.

Key Attributes for Success

Conversations with industry leaders identified several common strategies for succeeding in cybersecurity. Strong vendor relationships, staying at the forefront of emerging trends and making the most of automation stand out amongst the common opportunities being extolled by The High Growth 100: Cybersecurity. Below is an exploration of the nuances of these themes.

Leadership Insights:
A selective vendor strategy

According to Gartner there are more than 3,200 active cybersecurity vendors, with the list constantly shifting and altering to reflect M&A and market newcomers. The hard task for MSSPs in to balance breadth of their portfolio across many vendor partners with the depth of forging strong Bendor partnerships to develop enhanced expertise and service levels. For Dorset-based Vizst Technology, which generates 40% of its recurring revenue from cybersecurity services, finding the sweet spot has involved a multi-year process of vendor consolidation. The privately owned MSP was born from The Techneds-backed three-way merger of ITSB, Quad Vision and Data Integration in late 2021. Narrowing its supplier portfolio was driven by a desire to become closer to its core partners. "Our approach has evolved over the last two years, and we have refined our vendor portfolio from a large number to a more focused group of eight vendors," said CEO Richard Betts. These include Fortinet, Palo Alto Networks, and Arctic Wolf. "This more concentrated approach has enabled us to achieve the highest accreditations and develop specialised skill sets so we can provide tailored solutions to clients," added Betts.

Over the past year, Vizst's team has completed more than 120 vendor accreditations, according to Betts. "As a cybersecurity and networking partner, this remains a key focus for us and will continue to be as we grow," Betts adds.

Richard Betts

Having less vendors enables us to concentrate our efforts on certifications, training and strategic growth plans.

The MSPs that will truly thrive in the coming years are those that strike the right balance between automation and human expertise

"Having less vendors enables us to concentrate our efforts on certifications, training, strategic growth plans, focused marketing campaigns, and pipeline and lead generation."

Trustmarque's Cyber Security Practice Director James Holton notes that this trend is common across the cybersecurity industry as partners aim to reduce the complexity in their customers technology landscapes. He said: "We are seeing MSSPs looking to do more with fewer vendors as having a clear cybersecurity strategy becomes a mandatory part of a resellers offering."

One Equity Partners-backed Trustmarque has over three decades of pedigree in solving IT problems in the public and private sector. The provider lists 14 cybersecurity partners within its own portfolio. Vizst Technology and Trustmarque's focus on tighter vendor relationships and achieving top-

of its portfolio after identifying a marked increase in criminals targeting this attack vector into organisations. OT systems, which control physical devices and processes in sectors like manufacturing, energy, and healthcare, are increasingly under siege, notes Tickle. "There's been a staggering 400% increase from 2022 in malware against OT environments.," said Tickle. "These environments, often part of critical national infrastructure, simply can't afford downtime."

The challenge with OT security is that many systems operate on outdated technology, lacking the cybersecurity defences that are standard in IT systems. This makes them vulnerable, requiring a different approach to protection. Littlefish is addressing this challenge head-on, with a strategy that blends traditional IT security with specialised OT solutions, for example reimaging devices to deploy the technology as it was new. "OT is a huge opportunity, not just for MSSPs, but MSPs in general. Our growth is going to be very much focused on keeping an eye on the horizon of that OT struggle that our clients, both existing and new, are experiencing, and on what we can do to alleviate those pain points," Tickle said.

In the last year, Littlefish has experienced 42% year-on-year growth, and its team has grown to over 650 employees with approximately 45 of those making up its cyber team.

Navigating regulatory requirements

It is also critical for service providers keep up with changes within the increasingly stringent regulatory environment to which their customers must adhere. Compliance with frameworks like DORA (Digital Operational Resilience Act) and NIS2 (Network and Information Systems Directive) is essential, especially for industries like finance and healthcare. Betts noted: "We have adapted our marketing and sales strategies to help customers and prospects meet the deadlines set by these frameworks," Betts noted. "We've shifted our demand generation messaging to focus on these regulatory requirements, helping our clients navigate them successfully."

To validate the opportunity here, data from CSO Online states that 66% of companies surveyed say that compliance mandates are driving spending. According to the Competitive

tier certifications speaks to the growing importance of credibility and expertise in the cybersecurity sector.

Keeping a client focus

Betts notes that the company's vendor consolidation has strengthened its internal capabilities whilst enabling the company to take a more client-centric approach. He elaborated: "We address our customers' pain points instead of leading with a vendor or technology. By becoming a trusted technology partner, we work through their problems with them and truly understand their requirements."

Holton agreed: "Instead of pushing technology directly, we want to sit in front of more of our customers, understand their security plans and discuss how we can help over the coming years. Having those supportive vendor relationships enables us to then work with them on some more bespoke solutions for our clients."

Staying ahead of trends

Sector expertise means understanding which attack vectors cybercriminals are targeting, and this is critical to identifying where opportunities to protect clients lie. As an example, Littlefish CISO Sean Tickle shared with ITEuropa how the Nottingham-based MSSP has placed OT security at the centre

James Holton

Instead of pushing technology directly, we want to sit in front of more of our customers and understand their security plans.
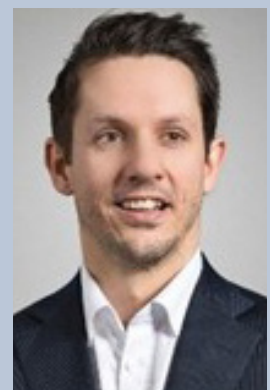
Enterprise Institute, for large firms, the cost of compliance can approach $10,000 per employee. To validate the opportunity here, data from CSO Online states that 66% of companies surveyed say that compliance mandates are driving spending. According to the Competitive Enterprise Institute, for large firms, the cost of compliance can approach $10,000 per employee.

Automation as a scale-up tool

With the right vendor partnerships in place and a product set to combat rising issues, the focus turns to improving profitability and enhancing service delivery. Littlefish's approach has been to make automation a central component of its strategy, improving service delivery and incident response. This also provides clients with confidence, helps with retention and makes scaling easier. "Automation is key for all of our services," Tickle emphasised. "Automating routine tasks like threat detection, containment, and incident response has allowed us to be quicker, leaner, faster and smarter, without increasing human resources."

Grand View Research noted that: "Technological advancements in AI, ML, and big data analytics are enhancing the effectiveness of these tools. Additionally, stringent regulatory compliance requirements and the growing adoption of IoT and cloud services are expanding the demand for robust security measures."

Striking a balance between human and automation

It's important to recognise the limitations of automation and the benefits of leveraging human expertise. MSPs like Littlefish and Trustmarque are investing not only in automation but also in retaining skilled cybersecurity analysts, recognising the power in harmonising human and technology touchpoints. For Littlefish, balancing automation with human skill is integral to their growth strategy. While automation can streamline processes and enhance service delivery, Littlefish's CISO, Sean Tickle, emphasises that the real value comes from its people: "Analysts are not

cheap; they're not cheap to train, they're not cheap to keep. You can't just replace their knowledge and expertise with automation. At the end of the day, it's our analysts who are at the heart of every cybersecurity effort, understanding the nuances of threats and responding accordingly."

"Even if you train fresh talent, within six months to a year, they've got recruiters knocking at their door offering them 40, 50k because that's just the market right now," added Tickle. "So, for us, it's not just about finding talent, it's about keeping them, and that's why we put a huge focus on career development and making sure we treat our security analysts and professionals even better."

James Holton, Cyber Security Practice Director at Trustmarque, echoed Tickle's sentiments about the central role of people in their cyber operations, highlighting plans to expand the team to ensure ongoing success. "We plan to grow. In fact, we've just hired four new people in our cyber team. So, we should be upwards towards 45 by the end of this year," he said. "We really want to crack the 50 mark and then we plan to keep growing at about 20%." Looking ahead, Holton hopes Trustmarque's cyber team will be 100 strong by the end of 2026.

The conclusion here is clear: the MSPs that will truly thrive in the coming years are those that strike the right balance between automation and human expertise. This includes nurturing skills to ensure team progression within the shifting cyber security landscape to both meet new threats and help with staff retention.

Easing skills shortages

2024 government research shows positive signs for the skills shortages that have been plaguing the post-covid cybersecurity market. According to data, the number of students enrolled in cybersecurity courses has increased by 14% and the number of students graduating in a cybersecurity course has also increased by 34%. In 2022/23 there were 580 new starts on cybersecurity apprenticeships in England, an increase of 18%.

Our Thoughts: Success hangs in the balance

The cybersecurity landscape is evolving rapidly, and MSPs like Littlefish, Vizst Technology, and Trustmarque are at the forefront of this transformation. What we have learnt from talking to leaders at these organisations and others that prefer not to be named is that success hinges on finding balances. A balance between breadth and depth in vendor relationships is key to ensuring that you can address client needs whilst offering a bespoke and unconfusing solution.

The best way to do this is to pick a core group of vendors, become experts in their offering and then go to market with a client-led approach. This strategy will also help MSPs find

Sean Tickle

Automating routine tasks has allowed us to be quicker, leaner, faster and smarter, without increasing human resources.

According to the Competitive Enterprise Institute, for large firms, the cost of compliance can approach $10,000 per employee

the balance between traditional IT security with specialised solutions when identifying new attack vectors. This will allow companies to be quick at addressing new market opportunities. It clear that there is no one true path to gain and sustain high growth with the cyber security space. However, a combination of focusing on client need, automation and nurturing talent are essential elements that

leaders exhibit. For technology centric MSPs, there is a danger that the systems and processes become too central to success and people power gets forgotten. In this spirit, it is worth remembering what Albert Einstein 'reportedly' commented: "Computers are incredibly fast, accurate, and stupid. Human beings are incredibly slow, inaccurate, and brilliant. Together they are powerful beyond imagination." ∎

About the author

Greg Denholm is an experienced writer in the IT and Telecoms channels, creating thought-leadership content for Comms Dealer and IT Europa. Greg is also the Editor of Fibreprovider.net, a leading publication in the UK altnet and ISP space.

About IT Europa

IT Europa is the leading provider of news, analysis, events and marketing services for the European IT vendor and channel partner community. Backed up by our team of journalists, data analysts and tele-marketers, IT Europa is an authoritative and cost-effective platform to reach 80,000+ director-level contacts.