



# Cybersecurity's *next winners*

Specialist Service Partners and MSPs/VARS






**OC&C**  
Strategy consultants

uncommon sense™

# Why Specialist Service Partners and Managed Service Providers (MSPs)/ Value Added Resellers (VARs) are *best placed to win*

LARGE CORPORATES AND THE MID-MARKET ARE THE HIGHEST GROWTH AREAS IN CYBER AND SPECIALIST SERVICE PARTNERS AND MSPs/VARs ARE ESPECIALLY WELL POSITIONED.

Cyber security market overview

	Cyber Complexity	Approach
 <p><b>Global Enterprises High-Complexity Industries</b></p>	<p><b>Very high complexity</b></p> <ul style="list-style-type: none"> <li>• Vast scale of highly valuable digital assets (IP, business processes)</li> <li>• Global operations</li> <li>• Often substantial sector-specific regulation</li> <li>• 100+ historical cyber incidents</li> </ul>	<ul style="list-style-type: none"> <li>• Very large in-house cyber team (100+ FTE) are core, supplemented by multiple external specialists</li> <li>• Procure direct, seek best of breed</li> <li>• All tooling highly tailored or built in-house</li> <li>• Budgets typically &gt;50m (\$/€/£)</li> </ul>
 <p><b>Large Corporates (e.g. 2k-10k FTE)</b></p>	<p><b>High complexity</b></p> <ul style="list-style-type: none"> <li>• Moderate/large scale of digital assets, increasingly of interest to bad actors</li> <li>• Multinational operations</li> <li>• Likely experience multiple historical breaches - high Board-level anxiety</li> </ul>	<ul style="list-style-type: none"> <li>• Moderate-large inhouse cyber team (10-100 FTEs) with large and growing budgets (1-25m+ \$/€/£)</li> <li>• "Picking their spots" to bring inhouse (focus typically sector dependent, and driven by leadership culture)</li> <li>• Need significant external support - both ad-hoc and managed service</li> </ul>
 <p><b>Mid-Market Business (e.g. 250-2k FTE)</b></p>	<p><b>Moderate complexity</b></p> <ul style="list-style-type: none"> <li>• Limited IP of value to bad actors</li> <li>• Few regulations/ compliance requirements historically</li> <li>• Some international considerations</li> <li>• Many with no prior track record of cyber incidents</li> </ul>	<ul style="list-style-type: none"> <li>• Limited dedicated cyber resource (&lt;10 FTE), potentially without a CISO</li> <li>• Seek to outsource most services; typically leveraging off-the-shelf solutions with limited configuration</li> <li>• May not have dedicated cyber budgets; spend competes with wider IT priorities</li> </ul>

**CYBER SECURITY IS NOTORIOUSLY HIGH-GROWTH AND ACYCLICAL SO IT RIGHTLY ATTRACTS SIGNIFICANT ATTENTION FROM INVESTORS.**

However, the space is increasingly complex and rapidly changing - the goalposts keep moving for traditional business models and while some will come under pressure, others are especially well placed to win going forward. Based on our recent work, two categories in particular stand out for the potential to generate significant returns: Specialist Service Partners and Managed Service Providers (MSPs)/Value Added Resellers (VARs).



**Growth Outlook For 3rd Party Providers**

**~10% pa**

- Ongoing growth in threat and regulations
- Increasingly complex software landscape
- Resilient (non-cyclical) budgets

**~15% pa**

- Rapid threat growth - increasingly in bad actor's "crosshairs"
- Material growth in regulation, compliance and certification requirements
- Significantly improved supplier propositions (e.g. simplicity of setup/management, lower price point)
- Historically small budgets and limited resource
- Labour shortages and wage pressure

**1**

**Winning 3rd Party Models**

**Specialist service partners**

- Domain experts in one topic area (e.g. XDR/SOC or Identity); typically picking 1-2 leading vendors to back within these areas
- Skill-set and track record drive durable differentiation and margin potential
- Significant M&A potential

**2**

**MSPs & VARs**

- Best positioned to drive upsell - have "the ear of the CTO" and largest existing ICT relationships
- Model focussed on simplicity and scalability; integration with wider ICT promises seamless integration and "one throat to choke"
- Significant M&A potential

# Specialist *Service Partners*

AS THE SOPHISTICATION OF THREATS AND SIZE OF ATTACK SURFACES HAVE INCREASED, CYBER SECURITY TOOLING HAS PROLIFERATED, SPECIALISED AND FRAGMENTED.

In-house teams are increasingly relying on specialist support across the design and build phases of core cybersecurity solutions, and to a lesser extent, for ongoing support. Key areas of focus include XDR/SOC and Identity (IAM, CIAM, PAM, IGA), but many other areas exist. Specialist service providers are very well positioned given:

---

1.

---

Strong domain expertise with tangible track records at blue-chip clients is scarce - and this is critical in an industry where cyber risk minimization is the primary objective. Quality wins and Specialist Service Partners can often position themselves as leaders.

2.

---

As Enterprise and Large Corporate cyber teams mature, they increasingly seek best-of-breed and more specialist service provision for critical applications. Independent firms typically have the closeness and agility that broadline or offshore providers lack.

3.

---

Software vendors, such as Microsoft, CrowdStrike and Okta are increasingly relying on channel and service providers for client success instead of in-house professional services. They particularly favour independents, especially those exclusive to their platform/s which can drive high volume, high-value pipeline.



# MSPs & VARs

THESE BUSINESSES TARGET THE HIGHEST GROWTH SEGMENTS - MID-MARKET AND LARGE CORPORATES - WHERE ADOPTION GROWTH IS RAPID, AND CLIENTS NEED THE MOST SUPPORT.

Critically, due to their limited in-house capabilities, these customers tend to have greater dependence on their partners and willingness to adopt a recurring managed service model - highly attractive revenue quality dynamics. MSPs & VARs are increasingly well positioned to win here given:

- 1** They already typically have the largest share of outsourced IT spend and have “the ear” of the CTO - an advantaged position to identify needs early and be able to bundle and integrate best with wider IT services.
- 2** Supply-side technological improvements allow for “mass-market” adoption of technologies (e.g., Microsoft’s rapid rise in SIEM with Sentinel). These are standardised enough that MSPs can take on the propositions with scale.
- 3** Cyber remains closely tied to, and embedded within, wider IT services and transformations, such as Cloud and data strategy. As a result, being able to provide integrated solutions is critical.
- 4** They have well-honed high-scale and low-cost delivery models.



IT IS IMPORTANT TO NOTE THAT FOR BOTH THESE GROUPS, M&A IS A VERY ATTRACTIVE MEANS TO ACCELERATE GROWTH. SERVICE PROVISION REMAINS RELATIVELY FRAGMENTED, AND M&A CAN DRIVE NEW GEOGRAPHIC AND/OR SERVICE LINE OFFERINGS WITH SIGNIFICANT REVENUE (E.G., PRODUCT CROSS-SELLING) AND COST (E.G., GO-TO-MARKET) SYNERGIES.

Notably, this list does not include the MSSP and software categories. While substantial opportunities remain in these areas, structural challenges exist. MSSPs are facing considerable pressure from MSPs. Software vendors can face rapid category and technology lifecycles, presenting a material downside risk.

For investors, significant pockets of opportunity remain in these areas, but it's crucial to approach with caution.

Understanding the product (think category trends and key vendors) and channel (think use of it, and role within it) are critical considerations.

---



*While substantial opportunities remain in these areas, structural challenges exist. MSSP's are facing considerable pressures from MSPs. Understanding the product and channel are critical considerations.*

IF YOU ARE LOOKING AT ANY OF THESE AREAS, OR REFRESHING YOUR VIEWS ON THE WIDER CYBER ECOSYSTEM, OUR EXPERTS ARE ON HAND TO DISCUSS FURTHER.



**Chris Woodland**  
PARTNER



**Ewan Parry**  
PARTNER



**Mark Blackwell**  
PARTNER



**Oleg Tschernizki**  
PARTNER



**Steve Cantin**  
PARTNER



**Phil Craig**  
ASSOCIATE PARTNER

## OFFICES

Belo Horizonte<sup>1</sup>

Boston

Hong Kong

London

Melbourne

Milan

Munich

New York

Paris

Rotterdam

São Paulo<sup>1</sup>

Shanghai

Sydney

Warsaw

uncommon sense™

occstrategy.com



Certified



1. The B Corp certification does not extend to our alliance with Advisia OC&C Strategy Consultants in Brazil.