



## EXECUTIVE INSIGHTS

# The Next Frontier in Professional Cyber Services: Operational Technology Security

### Key takeaways

1. The convergence of operational technology (OT) and information technology (IT) is heightening cyber risk across critical infrastructure sectors, bringing OT cybersecurity to the forefront of board-level priorities.
2. Governance, risk and compliance stands out as the most attractive segment, supported by mandatory spend, predictable revenue streams and high outsourcing momentum.
3. Clear differentiation hinges on sector fluency and regulatory depth, particularly in verticals with complex compliance environments.
4. Winning players combine deep OT expertise with tailored, scalable solutions that translate cyber risks into business outcomes.

### The rising need for OT cybersecurity

The convergence of operational technology (OT) and information technology (IT) has dramatically increased cybersecurity risks in critical infrastructure sectors such as energy, transportation, utilities, telecommunications and manufacturing. Once isolated from external networks, OT systems are now increasingly connected, exposing them to cyber threats — including power outages, production shutdowns, supply chain disruptions and safety hazards — that could have catastrophic consequences.

OT security refers to the protection of industrial control systems, supervisory control and data acquisition (SCADA) systems and other critical infrastructure technologies from cyber

threats. Unlike traditional IT security, which safeguards data and networks, OT security focuses on securing physical processes and machinery in the aforementioned sectors.

Several factors are accelerating the demand for OT-focused cybersecurity services, making it an attractive investment opportunity:

- **IT/OT convergence:** As industrial systems integrate with corporate IT networks and cloud solutions, they inherit the vulnerabilities of digital networks, demanding sophisticated security measures.
- **Regulatory pressure and compliance requirements:** Governments worldwide are tightening cybersecurity mandates for critical infrastructure — such as through the NIS2 Directive (EU), EASA cybersecurity standards in aviation (EU) and NIST-CSF (US) — driving mandatory investments in cybersecurity services.
- **Rising cyber threats:** The increase in geopolitical cyber threats has elevated cybersecurity as a boardroom priority. Germany's recent €500 billion infrastructure spending announcement directly amplifies the demand for OT-focused cybersecurity services, particularly in critical infrastructure sectors.
- **Cyber insurance evolution:** Insurers are enforcing higher cybersecurity standards for OT-heavy industries, requiring security assessments, incident response planning and ongoing monitoring as part of their underwriting process.
- **Talent shortage in OT security:** OT cybersecurity expertise remains scarce, pushing companies to outsource cybersecurity services, driving growth in professional and managed security service models.

This edition of L.E.K. Consulting's *Executive Insights* highlights why this space presents a high-growth opportunity for investors. It also details why cybersecurity for industrial and critical infrastructure is not just a necessity but a regulatory and operational imperative.

## Pockets of opportunity

### Segments in the professional cybersecurity services market



The cybersecurity landscape is experiencing strong growth, presenting an £8-10 billion market opportunity in professional cybersecurity services in Western Europe alone — expanding at 10%-12% per annum. OT-heavy industries such as manufacturing, energy and critical infrastructure are driving 20%-30% of this total cybersecurity spend.

To better understand where the most attractive opportunities lie, professional cybersecurity services can be segmented into distinct service lines, each addressing critical aspects of cybersecurity risk management, compliance and resilience.

Below, we break down the core professional cybersecurity service categories and their value propositions (see Figure 1).

**Figure 1**

Key segments in professional cybersecurity services

 Service line	 Description
Architecture and design	<ul style="list-style-type: none"> <li>This involves designing secure IT infrastructure, networks and applications to protect against cyber threats while ensuring scalability and resilience. Security architects develop frameworks incorporating encryption, identity and access management, secure coding practices and network segmentation.</li> </ul>
GRC	<ul style="list-style-type: none"> <li>GRC encompasses the strategic alignment of cybersecurity policies with business objectives, ensuring regulatory adherence and risk management               <ul style="list-style-type: none"> <li>- <b>Governance:</b> developing cybersecurity policies, incident response plans and governance frameworks to ensure compliance with standards (NIST, ISO, GDPR, etc.)</li> <li>- <b>Risk management:</b> assessing security posture, threat modelling, third-party risk and remediation planning to mitigate cyber threats and vulnerabilities</li> <li>- <b>Compliance:</b> preparing for audits, supporting certification processes and ensuring regulatory compliance through documentation and validation</li> </ul> </li> </ul>
Assurance/audits	<ul style="list-style-type: none"> <li>Cybersecurity assurance and audits involve systematically assessing an organisation's security controls, policies and compliance measures to identify gaps and vulnerabilities</li> <li>Auditors evaluate security postures against frameworks like SOC 2, NIST and ISO 27001, providing reports and recommendations to enhance security resilience and mitigate risks from cyber threats</li> </ul>
Pen testing	<ul style="list-style-type: none"> <li>Pen testing is a simulated cyberattack performed by ethical hackers to identify vulnerabilities in an organisation's systems, applications and networks before malicious actors exploit them</li> </ul>

Source: L.E.K. research and analysis

## Key hotspots for investment

There are several factors to consider when evaluating an investment opportunity in professional cyber services (see Figure 2), including:

- **Market opportunity.** How large is the market in this segment?

- **Revenue predictability.** What is the level of reoccurring demand? Is it driven by predictable, ongoing needs of an organisation or one-off projects with higher demand volatility?
- **Outsourcing trends.** Is the segment experiencing an increasing rate of outsourcing?
- **Scope of differentiation.** Is there potential for differentiation, or is the market largely commoditised?

**Figure 2**

Attractiveness of investment opportunity in professional cybersecurity services

Service line	Relative opportunity size (current market spend)	Revenue predictability and reoccurrence	Outsourcing rate	Scope for differentiation	Attractiveness of investment opportunity
Architecture and design	High	Medium	Stable/marginal growth	High	Medium to high
GRC	High	Medium to high	Growing	Medium to high	High
Assurance/audits	Medium	High	Growing	Medium	Medium
Pen testing	Low	High	Growing	Low	Low

Note: GRC=governance, risk and compliance  
Source: L.E.K. research and analysis

### Market opportunity and demand

The largest opportunities in professional cyber services lie in governance, risk and compliance (GRC) and architecture and design. These service lines command significant market spend as organisations invest in having a secure IT infrastructure design to protect against cyber threats while ensuring scalability and resilience.

Aligning cybersecurity policies with business objectives to achieve robust risk management, mitigation and regulatory adherence is another key area of spend.

### Revenue predictability and reoccurrence

High reoccurrence is a key driver of predictable revenues in cyber services. Assurance/audits and pen testing are highly reoccurring, fuelled by regulatory audits and compliance

mandates. GRC services also exhibit strong reoccurrence, with governance projects being ad hoc (every few years), while risk management and compliance require continuous engagement. Architecture and design improvements follow a more periodic cycle, driven by large-scale infrastructure upgrades rather than ongoing needs.

Although individual organisations may increase or decrease their spending on professional cybersecurity services from year to year, overall market demand remains stable. This is because companies move through different phases of cybersecurity maturity – ramping up, optimising or scaling back – at different times, which evens out fluctuations at the broader market level.

### Outsourcing rate

Outsourcing in cybersecurity is growing across most service lines, driven by specialised talent shortages, cost efficiency and regulatory requirements. Pen testing and assurance/audits are particularly mandated for third-party validation, making them prime candidates for outsourcing. However, architecture and design upgrades experience stable levels of outsourcing, as organisations prefer to retain in-house capability over critical security architecture elements.

### Scope for differentiation

The degree of differentiation across service lines is shaped by three key factors:

- **Vertical/sector expertise.** Understanding industry-specific regulations, business operations and data flows (e.g. in the energy sector, deep familiarity with IEC protocols; in manufacturing, expertise in SCADA/PLC security and knowledge of production workflows)
- **Technical capabilities.** Certifications, subject-matter expertise, knowledge of specialised security frameworks
- **OT expertise.** Knowledge of OT systems (e.g. SCADA, PLC, DCS and RTU) as well as industrial communication protocols and networks (e.g. Modbus, DNP3 and Profinet)

The architecture and design area offers the greatest scope for differentiation, as expertise in secure system design requires a deep understanding of sector-specific IT and OT configurations, unique operational risks and industry-specific attack vectors.

GRC and assurance/audits also provide moderate differentiation, where strong regulatory expertise and technical competency in identifying critical vulnerabilities create competitive advantage.

## The winning playbook in OT cybersecurity

A vendor's right to win within OT cybersecurity is underpinned by deep technical OT expertise; vertical-specific knowledge of OT systems, regulations and the threat landscape; and highly skilled talent with sector-relevant experience.

- **Deep, technical OT expertise.** Deep technical knowledge of OT systems, as well as industrial communication protocols and networks, is essential for cybersecurity vendors to identify and understand the security vulnerabilities in their clients' IT/OT stack and to effectively advise on how best to harden their security posture through improved security architecture, practices, vulnerability assessments and workflows.
- **Vertical-specific knowledge of OT systems, regulations and the threat landscape.** Different sectors often have unique OT environments and associated challenges and threat vectors (e.g. risk associated with real-time system availability in aviation or ransomware threats in hospital operations). Having a deep understanding of such industry-specific applications and configurations of OT environments, operational risks and threat vectors — as well as cybersecurity frameworks and regulations — is crucial for vendors to deliver high-quality professional cybersecurity services.
- **Highly skilled talent with sector-relevant experience.** Vendors must assemble teams with deep expertise in specific industries such as aviation, telecommunications and utilities. This enables them to win and deliver high-quality work that aligns their cybersecurity solutions and services to sector-specific risks, regulations and operational realities — subsequently establishing credibility and trust in the OT cybersecurity services space.

## Conclusion

The OT professional cybersecurity services market presents a compelling investment opportunity, driven by:

- Strong long-term demand drivers, including IT/OT convergence, evolving cyber threats, stricter cyber insurance standards, regulatory mandates and a critical talent shortage in OT security
- Low competition from traditional IT security providers, positioning OT security as a niche but highly lucrative market
- Strong differentiation opportunities and high barriers to entry

Within OT security's professional services segment, the GRC service line stands out as a key investment opportunity, offering sizeable market spend, predictable reoccurring revenues, rising outsourcing trends and ample scope for differentiation.

## How L.E.K. can help

We help investors evaluate asset readiness, commercial positioning and compliance scalability in OT security. Whether your organisation needs diligence, value creation planning or sector landscaping, we bring industry depth and transaction rigour.

"As OT systems become the front line of cybersecurity threats, the winners will be those that can blend deep domain expertise with tailored, scalable services. The next wave of value creation lies in enabling trust and resilience across critical industries."

— Romain Maitret, Technology Partner

## About the Authors



### Romain Maitret, Partner | [r.maitret@lek.com](mailto:r.maitret@lek.com)

Romain Maitret is a Partner in L.E.K. Consulting's London office. With more than 10 years of consulting experience, he specialises in the technology sector, providing strategic advice to clients in fields including B2B software, infrastructure technology and IT services. Romain's experience encompasses a wide range of strategic issues, including market entry and strategic positioning, business plan development and marketing. He has also led a broad range of commercial due diligence projects (buy- and sell-side) for corporate and private equity clients.



### Harsha Madannavar, Partner | [h.madannavar@lek.com](mailto:h.madannavar@lek.com)

Harsha Madannavar is a Partner in L.E.K. Consulting's Technology Infrastructure practice globally (software, data, services and silicon systems), advising US and global corporates, private equity and hedge funds on a range of shareholder value issues including growth strategy, business model transformation, technology disruptions, product development, pricing and M&A. He is a member of the firm's global Board of Directors and also serves on the Board's Audit and Risk committees.



### Kashif Khan, Engagement Manager | [md.khan@lek.com](mailto:md.khan@lek.com)

Kashif Khan is an Engagement Manager in L.E.K. Consulting's London office and a member of the firm's Software and Technology Infrastructure practice. He has nearly a decade of experience advising private equity funds and technology businesses on commercial due diligence, growth strategy, and value creation across the technology sector, including enterprise software, infrastructure software and IT services.

## About L.E.K. Consulting

We're L.E.K. Consulting, a global strategy consultancy working with business leaders to seize competitive advantage and amplify growth. Our insights are catalysts that reshape the trajectory of our clients' businesses, uncovering opportunities and empowering them to master their moments of truth. Since 1983, our worldwide practice — spanning the Americas, Asia-Pacific and Europe — has guided leaders across all industries, from global corporations to emerging entrepreneurial businesses and private equity investors. Looking for more? Visit [lek.com](https://lek.com).

L.E.K. Consulting is a registered trademark of L.E.K. Consulting. All other products and brands mentioned in this document are properties of their respective owners. © 2025 L.E.K. Consulting