CYBER.
LONDON
Innovation through Collaboration
NOT-FOR-PROFIT CYBER CLUSTER RECOGNISED BY DSIT & SUPPORTED BY UKC3

Cyber Security Landscape in the London Market 2024

Department for
Science, Innovation
& Technology

UKC3
UK Cyber Cluster Collaboration

Cyber Security Landscape in the London Market 2024

Executive Summary

This research, conducted by Cyber London, aims to gain a comprehensive understanding of the cybersecurity landscape in London, with a particular focus on the IT vendors operating within the market. It seeks to identify the types of cyber security businesses present, including those specializing in network security, cryptography, identity management, privacy, artificial intelligence (AI), and other areas, especially those targeting small and medium-sized enterprises (SMEs).

A key objective of the research is to assess the cyber skills gap and shortage in the London market, with an emphasis on SMEs. It also seeks to evaluate SMEs' understanding of cyber security as they navigate the process of digitisation. Additionally, the research examines the role of Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) in delivering critical cyber security services to SMEs in London.

Another key objective of this research is to analyze the NCSC CIR Level 2 list to assess how many companies in London can effectively support SMEs in the event of a cyberattack.

This report presents key findings on cyber security trends, practices, and insights derived from recent surveys of SMEs and MSPs. The results highlight a broad spectrum of cyber security capabilities across organizations—while some have adopted cutting-edge tools and technologies, others remain less prepared, relying on basic measures and outdated systems. Organizations are at varying levels of maturity when it comes to delivering and managing cyber security services.

Key Objectives of the Research

- Assess the Cybersecurity Landscape, Cyber skills gap and shortage in London, specifically for SMEs and the servicing MSSPs.
- Assessment of Cybersecurity Awareness Among SMEs as they transition towards digitisation.
- Identify the role of MSPs and MSSPs in securing SMEs' digital infrastructures.
- Analyze the services offered, training, hiring practices, and certifications of MSPs/MSSPs operating in the London market.
- Review the list of companies approved under Cyber Incident Response (CIR) Scheme in London and evaluate the criteria for CIR Level 1 and CIR Level 2 to determine if more MSSPs can be included in these categories.

By focusing on these areas, this study aims to highlight both the challenges and opportunities within the cybersecurity sector in London, ultimately fostering a more resilient business environment.

Methodology

This research involved a detailed analysis of the cyber security landscape in London, focusing on SMEs and MSSPs. The methodology followed these key steps:

- **Shortlisting**: A total of 40 SMEs and 60 Managed Security Service Providers (MSSPs) were selected from various London boroughs to form the core research sample.
- **Data Collection**: Both phone interviews and desk research were conducted on all shortlisted SMEs and MSSPs. Approximately 50% of the SMEs and 40% of the MSSPs contributed through primary research, providing insights into their cyber security practices and needs.
- **Hiring Trends Review**: A review of hiring practices and job postings was conducted across four major platforms—**Glassdoor, Indeed, LinkedIn, and TotalJobs** websites—focusing on cyber security roles to identify trends and workforce gaps in the sector.

- **Cyber Incident Response (CIR) Evaluation**: A list of CIR companies in London was reviewed, focusing on the criteria for CIR Level 1 and Level 2. The list was examined in terms of company location, specific skills offered, and business size. The research assessed whether additional companies meet the required standards to be included in these categories, particularly those with capabilities to respond to advanced threats and support SMEs during incidents.

This mixed-method approach combined both primary and secondary data sources to develop a comprehensive understanding of the cyber security ecosystem in London.

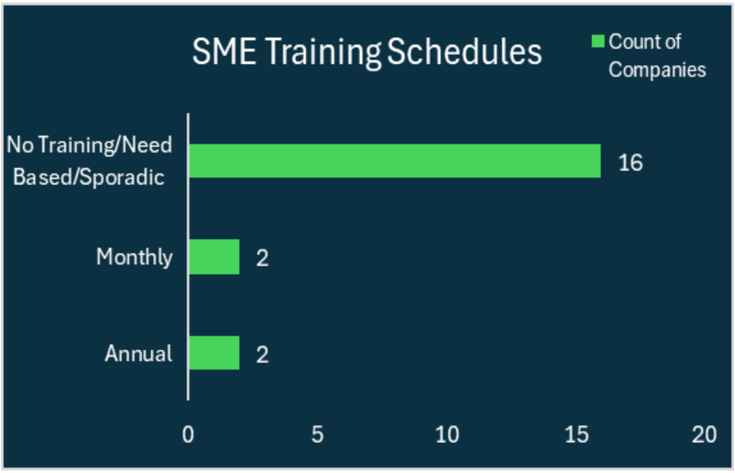
Key Findings

1. SMEs and Cyber Security

Cybersecurity Awareness vs. Prioritization

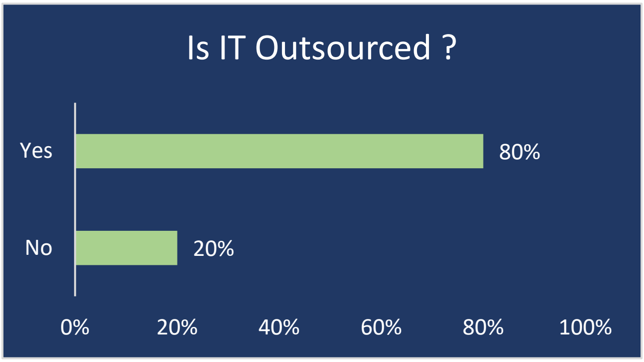
More than **90% of SMEs** recognize the importance of cybersecurity but do not prioritize it. While the majority acknowledge its significance, cybersecurity often takes a backseat in their **business** concerns. Many SMEs focus on essential protections like antivirus software and firewalls—commonly recommended by their MSSPs—while advanced measures are rarely considered unless mandated by regulations.

It was observed that, while SMEs often claim to prioritize cybersecurity, this focus does not translate into adequate financial investment in security measures or employee training. In fact, **60% of SMEs** interviewed confirmed that they had either never received cybersecurity training or had only participated in one-off



training sessions. This gap highlights a disconnect between the stated emphasis on cybersecurity and the actual steps taken to safeguard against threats.

Reliance on MSSP Recommendations



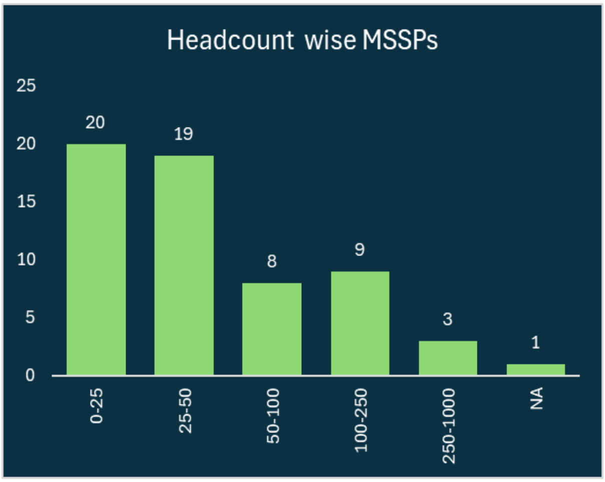
Nearly **80% of SMEs** responded that they do not have any inhouse staff and they heavily rely on their MSP/MSSP partners to recommend and implement cybersecurity measures.

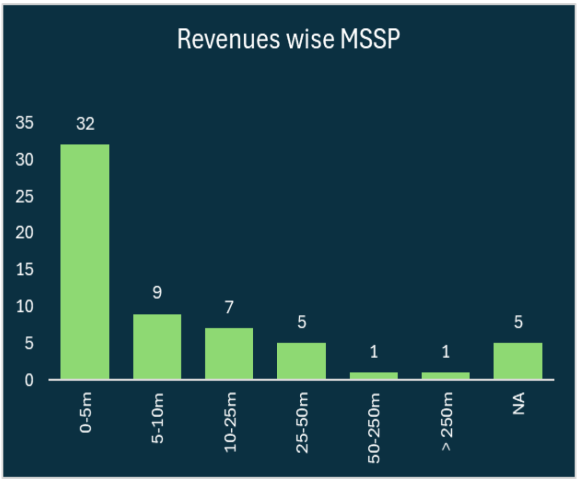
In **over 95% of cases**, these recommendations focus on basic solutions such as antivirus software and firewalls, with less emphasis on comprehensive protections against sophisticated threats.

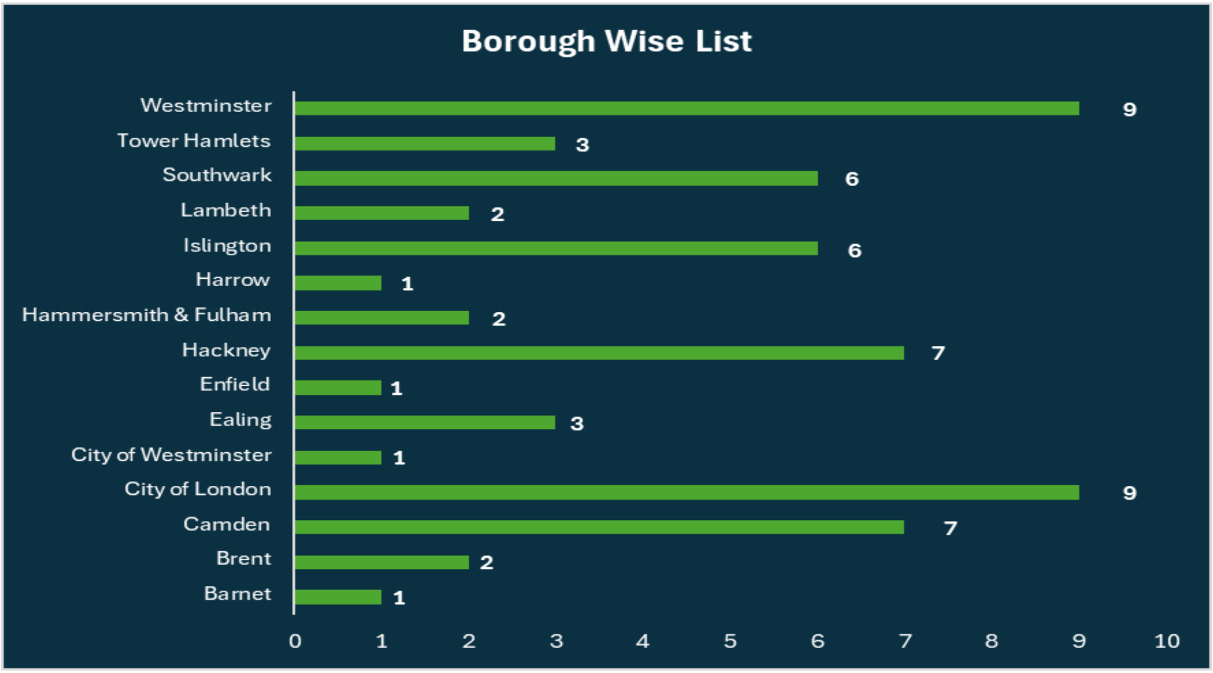
2. MSSPs in London

MSSPs are critical players in securing SMEs.As SMEs increasingly turn to MSPs and MSSPs for IT and cyber security solutions, these service providers have become key to ensuring the safety and resilience of London's small businesses. The growing reliance on MSSPs has made them central to the broader cyber security landscape in the city.

Survey participation and scope: The survey included 60 MSSPs from across the London boroughs, representing a range of sizes based on employee numbers and revenues. Of these, 23 MSSPs responded, providing the data for the primary research findings.







- **Transitioning from IT service providers to cyber security specialists:** Many small and medium-sized MSSPs are evolving from general IT support providers to cyber security specialists. However, their expertise is often limited to handling routine security issues, and they may not yet possess the skills or capacity to manage large-scale or catastrophic cyber security incidents.
- **MSSP Basic Cybersecurity Skills vs. Advanced Requirements:** Most Small and Medium MSSPs focus their skill sets on basic functions like conducting risk assessments and providing SIEM (Security Information and Event Management) services. However, these companies may lack the expertise and resources to offer more advanced support, such as

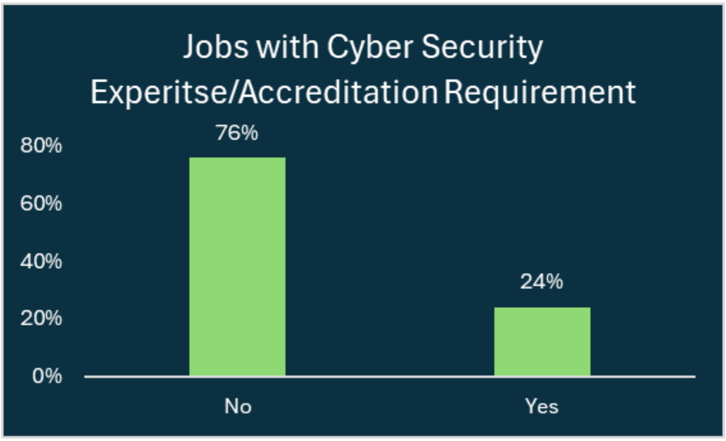
ensuring regulatory compliance with standards like PCI DSS or GDPR. Additionally, they may not be equipped to provide robust defensive measures in the event of a major cyberattack.

- **Client Choices Driven by Cost, Not Risk Understanding:** MSSPs believe that clients often choose service packages based primarily on affordability rather than fully understanding the associated risks. Additionally, **33% of interviewed MSSPs** feel that securing client sign-ups for more comprehensive packages requires significant effort and sales strategies. Clients also tend to show greater willingness to invest in security services only after experiencing a cyberattack.
- **Disclosure of cyber-attacks by MSSPs:** In the survey, **39% of MSSPs** admitted that they or their clients had experienced a cyber-attack in the last two years. Additionally, **8% of respondents** stated they were unable to disclose whether an attack had occurred, highlighting potential transparency issues or regulatory limitations regarding incident reporting.
- **Inconsistencies in Accreditation Standards Among Smaller MSSPs:** Training and certification requirements in smaller MSSPs tend to vary, with many not employing staff who possess advanced cybersecurity credentials like CISO or CISSP. These MSSPs often prioritize practical skills or general IT expertise over formal certifications, which can result in a less standardized approach to cybersecurity practices across different organizations. Our Research shows that only **17% of responding MSSPs** had or were hiring for accredited cyber specialists.

3. Cyber Security Skills Gap

- **Limited emphasis on cybersecurity expertise in hiring**: **Only 17%** of managed Security service providers (MSSPs) actively seek candidates with cybersecurity-specific expertise or accreditation when hiring for cybersecurity roles, opting instead for general IT skillsets and in-house training.

- **Focus on basic IT skills in job postings:** Analysis of hiring data from job portals reveals that approximately **76% of cybersecurity** job listings prioritize basic IT skills, indicating a gap between the advanced cybersecurity needs and the qualifications being sought by employers.

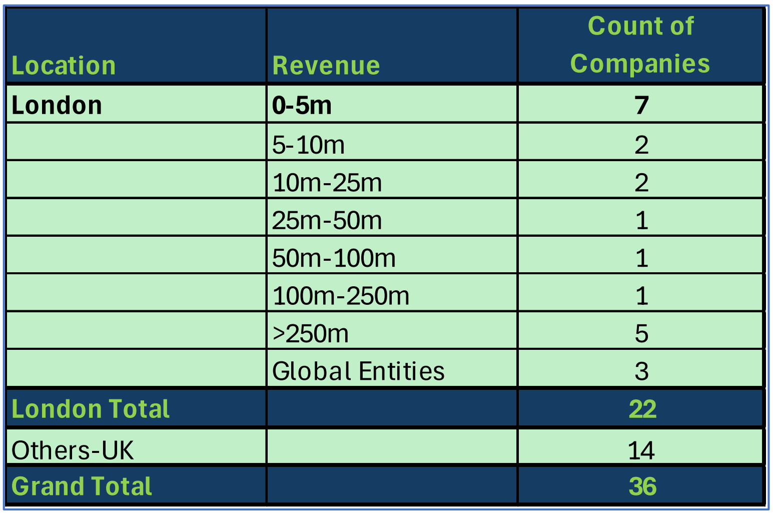


- **Impact on MSSP and Client's security posture:** Due to the absence of advanced cybersecurity expertise, employees often lack the skills to support more complex needs such as defensive security, incident management, and compliance. As a result, these organizations are less equipped to effectively support SMEs in the event of a catastrophic incident.

4. Cyber Incident Response

The National Cyber Security Centre (NCSC) plays a key role in safeguarding the UK's critical information and infrastructure against cyber threats. As part of its mission, the NCSC operates the Cyber Incident Response (CIR) scheme, which helps organizations find trusted partners to assist in recovering from cyberattacks. CIR members are rigorously assessed companies that specialize in handling incidents such as ransomware, phishing, and denial-of-service attacks. The certified CIR ensure that victims of cybercrime receive expert support for incident investigation and recover.

The NCSC CIR Level 2 data reveals that, while London contains over **65% of the certified companies**, **only 7 MSSPs** fall within the £0-5 million revenue range. This limited pool of small providers poses a challenge for SMEs in London seeking assistance during a cyberattack. Given the potential for widespread incidents, the small number of MSSPs may leave London's SMEs vulnerable, as they could struggle to secure the necessary cybersecurity support during critical situations. Consequently, the concentration of small MSSPs may not adequately meet the demands of the larger SME community during cyber crises.



Location	Revenue	Count of Companies
London	**0-5m**	**7**
	5-10m	2
	10m-25m	2
	25m-50m	1
	50m-100m	1
	100m-250m	1
	>250m	5
	Global Entities	3
London Total		**22**
Others-UK		14
Grand Total		**36**

With over **3,000 registered MSSPs** in London, there is significant potential for more providers to expand their services and pursue inclusion in the NCSC CIR list. By enhancing their cybersecurity capabilities and aligning with NCSC standards, these MSSPs can better serve the growing needs of local SMEs. This proactive approach would not only strengthen the cybersecurity landscape but also ensure that London businesses have access to reliable incident response resources in times of crisis.

Conclusion

This research highlights the growing awareness of cyber security among London's SMEs, though it remains a secondary concern compared to other business priorities. MSPs and MSSPs are playing a pivotal role in supporting SMEs' cyber security efforts, but many smaller service providers are still in the process of building the necessary expertise to handle more complex security challenges.

The Research shows a significant skills gap within the cybersecurity sector, as many MSSPs are predominantly hiring general IT experts or network engineers rather than accredited cybersecurity specialists. This trend suggests that demand for certified cybersecurity professionals remains limited, despite the increasing complexity of cyber threats. As a result, these companies often lack the specialized expertise necessary to provide comprehensive cybersecurity services. This reliance on general IT staff, who may not have the in-depth knowledge required to address advanced security challenges, ultimately hinders the ability of MSSPs to offer robust and effective cybersecurity solutions. Consequently, it may also slow their progress in developing a mature, specialized cybersecurity practice, impacting their ability to meet the growing demands of SMEs for more sophisticated protection against cyber threats.

Further investment in training and upskilling within the MSP/MSSP community will be essential to ensuring that SMEs are adequately protected against increasingly sophisticated cyber threats. This would also ensure a wider inclusion of MSSPs in the highly coveted and needed CIR scheme.

Recommendations

- **MSSP Development:** MSPs and MSSPs must be encouraged to invest in advanced cyber security training and certification to better protect SMEs from complex cyber threats.

- **Addressing the Skills Gap:** Targeted initiatives to attract and train more cyber security professionals, especially in areas such as incident response and cyber resilience, would help reduce the skills shortage in London.

- **Expansion of CIR Level 2 List:** It is highly recommended that more Managed Security Service Providers (MSSPs) in London enhance their capabilities to meet the standards required for CIR Level 2 certification. Currently, only seven companies hold this certification in London, presenting a strategic opportunity for other MSSPs to elevate their incident response skills. Achieving CIR Level 2 certification would not only enhance the overall cybersecurity landscape but also strengthen businesses' defences against widespread cyberattacks. This would create a win-win scenario, as certified MSSPs can tap into new business opportunities while bolstering London’s resilience to cyber threats.

- **SME Education & Awareness:** Further awareness and education campaigns targeting SMEs could help shift cyber security higher on their list of business priorities.

- Notes:
  Sources for Revenue and Employee counts
  - Companies House - GOV.UK (www.gov.uk)
  - https://www.zoominfo.com/
  - https://growjo.com/
- List Of SMEs/MSSPs
  - https://rocketreach.co/
  - https://themanifest.com/
  - https://www.goodfirms.co/it-services/cyber-security/london