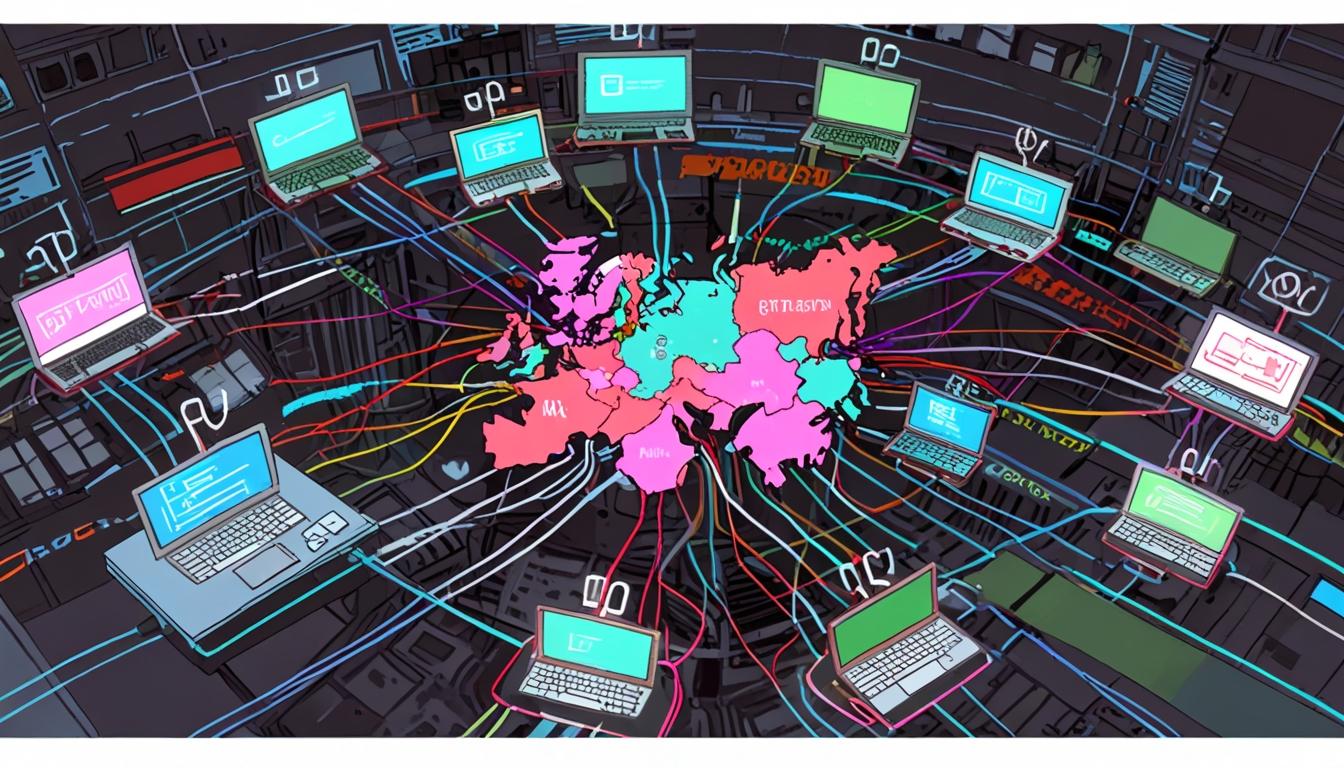
# Survey reveals UK organisations struggle with cybersecurity risks from unknown IT assets



A recent survey conducted by Trend Micro reveals significant challenges faced by UK organisations in managing cybersecurity risks linked to unknown or unmanaged IT assets. The study, which involved 100 cybersecurity leaders across the United Kingdom, highlights that 70% of organisations have experienced security incidents connected to these hidden or unmanaged assets.

Key factors contributing to the expanding attack surface include the widespread adoption of generative AI tools, continued remote working practices, and the increasing presence of Internet of Things (IoT) devices. These developments have intensified the complexity of organisational cybersecurity environments.

Concerns around unauthorised technology, referred to as Shadow IT, are prominent, with 38% of respondents citing this as a major cause of security blind spots. These blind spots arise when IT assets are not centrally overseen or even known to IT teams, creating significant vulnerabilities within organisations.

Compounding these challenges, 96% of UK cybersecurity leaders expressed worry about employees’ use of third-party AI tools, indicating that such external technology use is exacerbating attack surface complexities.

Despite these acknowledged risks and incidents, a substantial 82% of those surveyed stated that their current cybersecurity resources are adequate to tackle attack surface challenges and mitigate business risk. On average, organisations devote 29% of their cybersecurity budgets to managing attack surfaces. However, the survey points to a "clear disconnect" between this confidence and the frequency of breaches linked to unknown IT assets.

Analysis of survey responses suggests this disconnect may be attributed to varying degrees of proactivity within security teams. Over a quarter (28%) of respondents admitted their organisations respond to cybersecurity issues primarily on a reactive basis. Only 43% reported actively employing attack surface management tools.

In terms of risk management strategies, periodic audits remain common practice, with 52% of UK security leaders conducting such reviews or relying on external assessments. Conversely, fewer than half (48%) regularly update and patch their software and systems. The study warns that a reactive approach and infrequent auditing increase the likelihood that organisations will be disadvantaged if compromised through unmanaged IT assets.

Supply chain security also features prominently in the findings. More than half (56%) of respondents now regularly assess third-party vendors for security vulnerabilities and incorporate security checks into onboarding processes. This reflects a heightened awareness of supply chain risks following major cyber incidents in recent years.

The survey also indicates strong adoption of penetration testing and vulnerability assessments, with 89% of cybersecurity leaders reporting monthly testing and 38% conducting these assessments weekly. Such measures are intended to strengthen defences against risks posed by third-party suppliers.

Bharat Mistry, Field CTO at Trend Micro, commented on the findings, saying, "The enterprise AI genie is out of the bottle and IT security leaders need to get a grasp on the implications. Attack surfaces are expanding through both authorised and unauthorised uses of IT. A proactive strategy leveraging techniques that anticipate and limit cyber threats before they cause damage is the only answer. Our study shows real progress that's being made in managing growth in attack surfaces via third-party suppliers, but also food for thought on where our industry can go further to establish truly proactive defences that tackle new AI-based threats as well as attack surface blind spots that act as an entry point for attackers."

The research was carried out by Sapo Research as part of a global study encompassing more than 2,200 respondents across 21 countries, with the UK cohort consisting of 100 cybersecurity professionals. The study aims to shed light on how organisations are navigating the increasing complexities of their cybersecurity environments, including dealing with the rise of Shadow AI and other evolving threats in the attack landscape.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.axios.com/2025/02/04/shadow-ai-cybersecurity-enterprise-software-deepseek> - This article discusses the rise of unauthorized AI tools, known as 'shadow AI,' and the challenges they pose to company IT teams, particularly concerning data privacy and security. It highlights the risks associated with employees inputting corporate data into unapproved AI models, corroborating the article's mention of concerns around unauthorized technology and the impact of generative AI tools on cybersecurity.
2. <https://www.axios.com/newsletters/axios-codebook-38f09de0-e257-11ef-8ac2-05372d4f3eec> - This newsletter covers key cybersecurity topics, including the rise of 'shadow AI' and its impact on corporate networks. It emphasizes the need for better governance of AI use to mitigate security risks, aligning with the article's discussion on the complexities introduced by generative AI tools and unauthorized technology.
3. <https://securitybrief.co.uk/story/shadow-it-threatens-corporate-cybersecurity-new-study-reveals> - This study by Kaspersky reveals that 77% of companies had suffered from cyber incidents over the past two years, with 11% directly caused by the unauthorized use of shadow IT. It underscores the risks associated with shadow IT, supporting the article's mention of 38% of respondents citing unauthorized technology as a major cause of security blind spots.
4. <https://www.intelligentcio.com/eu/2024/09/19/only-one-third-of-organisations-run-round-the-clock-cybersecurity/> - Trend Micro's research indicates that only 31% of organizations have sufficient staffing for 24/7/365 cybersecurity coverage. This highlights the challenges organizations face in managing cybersecurity risks, corroborating the article's point about the disconnect between confidence in resources and the frequency of breaches linked to unknown IT assets.
5. <https://www.gov.uk/government/publications/research-on-the-cyber-security-of-ai/ai-cyber-security-survey-main-report> - This government survey reveals that nearly half of organizations using AI technologies have no specific cybersecurity practices in place for AI. It highlights the lack of preparedness in managing AI-related cybersecurity risks, aligning with the article's discussion on the complexities introduced by generative AI tools and the need for proactive strategies.
6. <https://securitysenses.com/posts/why-shadow-it-prevails-uk-smes> - This article discusses the prevalence of shadow IT among UK SMEs and the associated security risks. It emphasizes the challenges IT admins face in gaining control and visibility over their IT environment due to shadow IT, supporting the article's mention of 38% of respondents citing unauthorized technology as a major cause of security blind spots.
7. <https://news.google.com/rss/articles/CBMilAFBVV95cUxOcVJHSFc1N3FMV2R4bEljX01idUlIajgwNjI5cmdWT2lIMy0zMkNaNkd1Ul8zYUlfa0h3bEJwZFZOTTZON1lPT1RHYkpYTldPLXMyMFF6dE0xVUxZd0ljelN3Z3ktMmlQd3BLZVpaVFFRNXFLUGdEMEZhMjdNek1mSDMzWThMdlVsTGlnZjQwNjZObmNV?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data