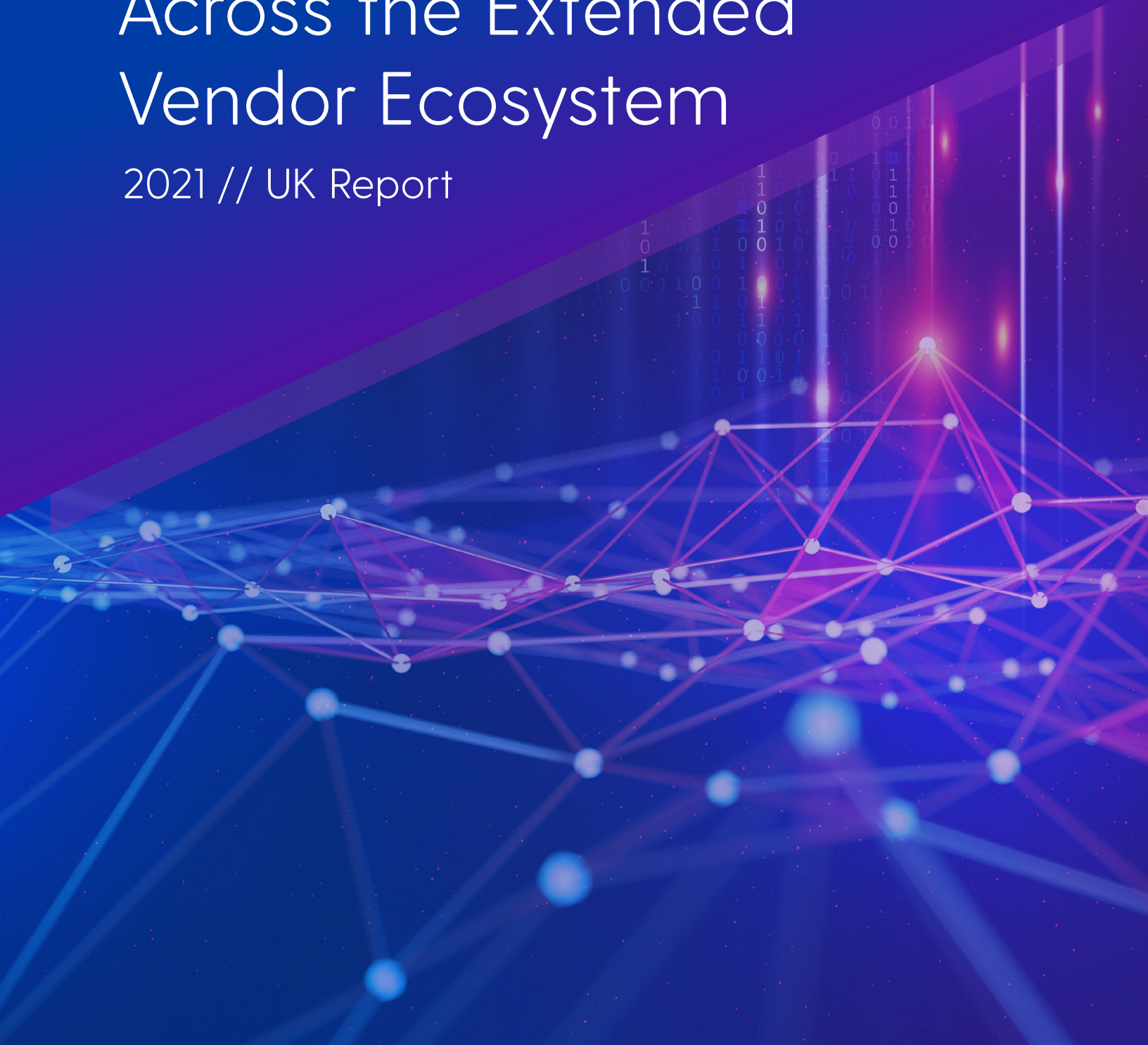



BlueVoyant|UK®

BLUEVOYANT REVIEW

# Managing Cyber Risk Across the Extended Vendor Ecosystem

2021 // UK Report





BlueVoyant commissioned its second annual survey undertaken by independent research organisation, Opinion Matters, in summer 2021.



1200 CIOs, CISOs and CPOs (Chief Procurement Officers) responsible for supply chain and cyber risk management were surveyed from companies employing 1000+ across a range of industries including: business services, financial services, healthcare & pharmaceutical, manufacturing, utilities and energy, and defence. To gain a global perspective, the research was conducted in the following countries: USA, Canada, Germany, The Netherlands, the United Kingdom, and Singapore. 300 respondents were from the UK.

## Foreword

Last year, our 2020 Global Insights Report stated that “managing third-party vendor cyber risk is fast becoming the defining cybersecurity challenge of our time.” The cybersecurity landscape in 2021 has proven that statement.

Third-party cyberattacks have affected multiple industries in waves: Accellion, SolarWinds, and Kaseya, to name just three. In some cases, a single breach in one vendor network or program affected tens of thousands of companies.

Accelerated by the worldwide rise of ransomware activity, cyber attacks on third-party vendors led to intrusions into major banks, defence companies, utilities, healthcare systems, and governments. SolarWinds is estimated to have cost in excess of \$100 billion.

Third-party cyber risk management has been proven to be an essential component of an overall risk management programme.

The question remains how companies and the wider industries in which they operate respond to the challenge of ensuring that their supply chain is secure. The solution is complex, but achievable. Vendor supply chains are often interlinked, resulting in overlap and complicated dependencies. They are multi-layered, meaning that sensitive information might be stored or processed by third- and even fourth-party providers. And they are often opaque: simply gaining visibility into a complete vendor ecosystem can be difficult and costly, even before attempting to secure it.

This year, the survey not only explores the scale of the challenge but also the amount and severity of supply chain breaches. It also tracks the way that different companies, industries, and regions are responding to a year of cyber crisis.

Businesses in all industries across the UK are investing in cybersecurity. However, some still fail to make cyber risk a strategic priority and to coordinate and formalise their approach to cyber defence and remediation. In addition, companies struggle to assign ownership of their third-party cyber risk programme.

UK companies have not only been affected by the general escalation in cyber threat activities, they have also faced additional challenges. With supply chains stretched to breaking point by the pandemic, and extra pressure exerted by the ongoing effects of Brexit, many firms have had to diversify suppliers to build resilience. Businesses must take care when onboarding new vendors that they are not introducing unknown cyber risk into their ecosystem.

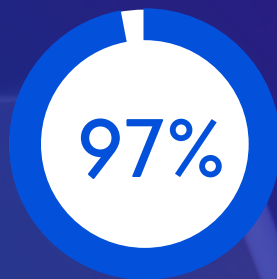
Adversaries can now actively scan organisations across the globe to identify attack vectors that can enable significant adverse cybersecurity events, including damaging data exfiltration and crippling ransomware attacks. Companies need to commit to incorporating continuous monitoring and remediation into their third-party cyber risk programme, as well as raise awareness at the senior executive and board level to help the business understand the resources needed to protect the business.





# UK Findings

At a glance UK findings:



97% have suffered a cybersecurity breach because of weaknesses in their supply chain/third party vendors in the past 12 months



3.57 average number of breaches experienced in the UK in the last 12 months due to weaknesses in supply chain cybersecurity



97% have been negatively impacted by a cybersecurity breach that occurred in their supply chain

**Despite high breach levels, companies in the UK show an inconsistent approach to supply chain cyber risk management. Awareness and prioritisation of third-party cyber risk is low.**



The UK findings paint a stark picture of rising breaches, low vendor visibility and limited awareness of third-party cybersecurity. **97% of UK-based firms surveyed said they suffered a direct breach because of weaknesses in third-party cybersecurity in the past year.** This represents an increase of 9% on 2020 and is higher than the overall average of 93%.



The number of breaches originating in supply chain weaknesses has also risen, from an average of 2.64 in 2020 to 3.57 in 2021. **59% of organisations experienced between two and five negatively impacted cybersecurity breaches - higher than the overall average of 49%.**



Compared with counterparts in other territories, **UK respondents are more likely to say that supply chain and third-party cyber risk is not on their radar.** The proportion saying it is not on their radar has risen from 28% in 2020 to 38% this year and significantly exceeds the overall average of 29%. Only 27% said managing third-party cyber risk was a key priority for their organisation.





The number of companies reporting supply chains with more than 1000 companies rose dramatically from 8% in 2020 to 43% in 2021. Simultaneously, the number reporting 500 vendors or fewer dropped from 40% to 29%. It is possible that supply chains exploded – particularly in the UK - but it is also likely that companies became more aware of the full extent of their vendor networks. **The average vendor ecosystem in the UK now contains 3715 third parties, a rise from 1013 in 2020.**



In the UK, organisations have **had to adapt their supply chain, onboarding new vendors due to the ongoing impact of leaving the EU.** This, added to the need to build resilience by reducing dependence on individual vendors prompted by the pandemic, would also explain growing vendor numbers.



Rising vendor numbers are exposing the increasing lack of visibility UK companies have over their suppliers' cybersecurity posture. **The percentage admitting that they have no way of knowing if an issue arises with a third party has risen from 34% in 2020 to 39% in 2021.** This is a clear indication of the complexity of the challenge UK businesses must solve if they are to stem the tide of breaches and control organisational risk.

# Changes in UK vendor monitoring frequency

In a sign that they are recognising vendor visibility shortcomings, UK companies fared better than counterparts in other territories when it comes to how frequently they re-assess their vendors.

 **4% to 12%**

The percentage monitoring weekly trebled from just 4% in 2020, to 12% in 2021, while 35% now assess monthly.

 **32% to 18%**

In contrast, the percentage assessing suppliers only six monthly almost halved, from 32% to 18%.

When it comes to briefing senior teams on the outcomes of third-party cybersecurity risk monitoring, the UK is also ahead of other regions. **27% brief senior teams monthly, compared to the overall average of 18%, while 14% of UK respondents say they brief weekly.**


There is also evidence that high-profile breaches are influencing corporate boards to deliver more robust oversight in UK businesses. **54% of respondents said breaches such as SolarWinds and Accellion had increased scrutiny and oversight from their board.**

 High-profile breaches are **INFLUENCING CORPORATE BOARDS** to deliver more robust oversight in UK businesses.

1. Questions were asked differently between 2020 and 2021. 2020 asked 'How frequently do you re-assess/audit your third party/supplier cyber risk and brief the senior management team on the findings from those audits?', whereas 2021 asked 'How frequently do you re-assess your third-party/supplier cyber security risk?'

2. Sample – 54% of the 1131 respondents who selected 'Yes' or 'Prefer not to say' to 'Have you had any cyber security breaches because of weaknesses in your supply chain/third party cyber security risk in the past 12 months? If so, how many?' (Q9)





# Speed is critical to identify and respond to third-party cyber risk

Third-party cyber attacks are headline news in **2021**, and the need for rapid response is evidenced as the detail of each attack becomes clear.

Many of the most damaging third-party cyber attacks this year occurred in the immediate aftermath of the discovery of new vulnerabilities. The January 2021 cyber attacks that exploited weaknesses in Microsoft Exchange, for example, began within days of the exploits being discovered. Without frequent – ideally continuous – monitoring, cyber attacks like this can go unrecorded and unseen for weeks and months. However, while



# 12%

of UK companies are assessing third-party cyber risk weekly, the number undertaking daily, or real-time monitoring has dropped to zero.

That leaves a high-risk window in which threats go undetected.



## BlueVoyant Viewpoint

Cyber and third-party risk can only become a strategic priority through clear and frequent briefings to the senior executive team and the Board. By that measure, the UK is performing better than some other territories. However, these briefings and the data that informs them can only be effective if there is an established culture of third-party risk awareness in the organisation. With **38% of UK respondents saying that supply chain/third-party risk is not on their radar and 39% admitting they have no way of knowing if a cybersecurity issue arises** with a vendor, the culture change needed to underpin effective third-party risk management is unlikely to take place.



# Budget for third-party risk management continues to rise, but spending may lack strategic focus.

Third-party risk management budgets are rising considerably within UK organisations.

 **27% 2020**

In 2020 27% of UK organisations said budgets were rising by between 51-100%.

 **47% 2021**

In 2021 an impressive 47% are reporting rises of that magnitude.

While it is encouraging that companies are investing in third-party risk management, the degree to which those investments are coordinated is unclear. **Companies report a wide distribution of pain points including reducing false positives, managing the volume of data, prioritising risk, and knowing their own risk position.**

UK businesses are more concerned than other regions about the challenge of meeting regulatory requirements and ensuring internal stakeholders understand the role played by third parties in the firm's



**BlueVoyant  
Viewpoint**

Increasing budgets year-on-year are a sign that UK companies are taking cybersecurity and vendor risk management seriously, and that boards and senior executive teams are willing to invest in better cybersecurity. However, the wide yet consistent array of different pain points suggests that this investment is not as coordinated or effective as it could be. This underscores a lack of strategy when approaching risk.

**Third-party cyber risk management requires a systematic, end-to-end approach** including data that is verified, accurate, and timely – technology and analytics that enable rapid identification and remediation, and the expertise to drive results.

cybersecurity posture. Tellingly, UK firms are also more likely to report difficulties onboarding new suppliers with the speed and rigour required, something that may have emerged as companies struggled with their supply chains in the past year.

The fact that UK organisations are reporting so many issues, and so many similar issues, suggests that larger budgets are not yet sufficiently resulting in risk reduction.





# UK companies rely on point in time solutions

Compared to international counterparts, UK organisations are more likely to use point-in-time solutions to manage third-party cyber risk.



## 33%

use questionnaires, compared to an overall average of



## 27%

among research participants.

UK businesses are also more likely to make use of **external consultants, with 36% incorporating them** into their programme. This correlates with the finding that UK companies have larger outsourced teams than those from other regions.

While they may not lack for headcount, UK firms are failing to reap the benefits of automation that can help lift the administrative burden of regular risk monitoring. Only **32% have vendor risk management programmes in place**, compared to the **overall average of 39%**.

Similarly, only **29% have an integrated/enterprise risk management program** in place, while overall this figure is 36%, **indicating that UK firms in general lack an overall strategic approach to cyber risk management.**



## BlueVoyant Viewpoint

The split of tools and programmes in use points to a **less mature approach** among UK companies. Point-in-time solutions don't offer the real-time, continuous intelligence needed to mount a successful third-party risk management programme. This means that even if companies are reporting regularly, the data they are delivering is not complete enough to rely on for key decision-making.





# High-profile breaches are influencing senior decision-makers in UK firms

Regular reports of devastating cyber breaches emanating from third party suppliers are having a sobering effect on UK businesses. However, the prevailing view seems to be that investment should be kept within the business:



## 59%

around three in five (59%) say they are likely to lead to budget increases for internal resources to protect against supply chain cybersecurity issues while only



## 35%

think they will get an increased budget to invest in external resources<sup>3</sup>

As previously discussed, the reputational damage caused by breaches of this type is also focusing the minds of senior leaders – in the UK more than elsewhere – with **54% saying board scrutiny has increased** as a result.



## BlueVoyant Viewpoint

The greater focus on internal investment could be recognition of a historical shortfall. However, UK organisations should not underestimate the value of external intelligence and threat management solutions when considering strategic approaches to the challenge. Procuring the advanced skills needed for intelligence analysis and remediation can be beyond in-house budgets, but accessible and affordable through managed security services.

Nevertheless, UK firms don't need to look at the headlines to feel the impact of third-party cyber breaches. **97% have suffered a direct breach** due to a weakness in their supply chain, and the same percentage have experienced indirect negative impact when a breach has occurred within their supplier ecosystem – figures that have increased considerably over the past year. **The rising frequency of breaches and their impact should be driving businesses to action.**

3. Sample – 54% of the 1131 respondents who selected 'Yes' or 'Prefer not to say' to 'Have you had any cyber security breaches because of weaknesses in your supply chain/third party cyber security risk in the past 12 months? If so, how many?' (Q9)





# Third-party

cyber risk must be taken out of operational silos and integrated fully with the organisation's overall risk management strategy with clearly defined lines of responsibility, reporting, and budget ownership.

## Tension remains over ownership of third-party cyber risk

For **29% of UK respondents the CIO has ownership of third-party cyber risk**. For **25% it is the CISO**, and for **19% it is the CPO**. This lack of clarity means there is considerable variation in the way different organisations approach the issue of cybersecurity risk. A CPO-led strategy will differ from that of a CIO or CISO and lead to difficulties establishing a standardised structure around risk management programmes.

Further, in a sector where community and knowledge-sharing is central to building a stronger defensive approach, it can be hard for professionals to 'find' each other and share insights if expectations over their role and remit differ widely.

This division over who ultimately owns cyber risk can cause issues around allocation of budget, resources and ultimately an organisation's ability to remediate issues when they arise. Overall, the research findings indicate a situation where the large scale of vendor ecosystems and the fast-changing threat environment is defeating attempts to effectively manage third-party cyber risk. **Third-party cyber risk must be taken out of operational silos and integrated fully with the organisation's overall risk management strategy with clearly defined lines of responsibility, reporting, and budget ownership.**



# 29%

of organisations think the CIO owns cyber risk



# 25%

of organisations say it belongs to the CISO



# 19%

say Chief Procurement Officers are responsible





# Recommendations

Our research shows that there are large concentrations of unknown third-party cyber risk across supply chains and vendors worldwide. Currently the treatment is not proportional to the scale of the risk faced and organizations are experiencing frequent vendor-originated breaches. While there is recognition that more investment is needed – budgets are rising universally – with organizations reporting multiple pain points, the critical question is where funds should be directed to make a tangible impact to reduce third-party cyber risk.



## Decide who owns third-party cyber risk

Respondents globally gave mixed answers to third-party cyber risk ownership – between CIOs, CISOs, CFOs, even CPOs. Until third-party cyber risk is a clearly defined mandate at the executive level, **it is difficult to effectively coordinate resources and define clear strategies.**



## Integrate continuous supply chain monitoring with appropriate reporting to the board and senior executives

Too many cyber attacks in 2021 occurred after patches were released, after vulnerabilities were disclosed, or after vendor monitoring systems would have revealed suspicious activity. Auditing or assessing your supply chain every few weeks or months is not sufficient to stay ahead of agile, persistent attackers. **Continuous monitoring and quick action against newly discovered critical vulnerabilities** needs to become essential to effective third-party cyber risk management. This includes automation of analysis; expanding assessment to include the “long tail” of vendors and not a limited number of critical suppliers; and identifying areas of non-substitutability or where risk is pooled.



## Gain visibility into the supply chain

Supply chain ecosystems are large, multi-layered, and complex. Obtaining complete visibility into the supply chain is hard. It is necessary, however, to **fully understand third-party vendors beyond the first tier or most critical suppliers.** Drive supplier risk-reduction activity by building constructive support for suppliers into your third-party cyber risk management program. Alert the vendor when new risks emerge and provide practical steps for them to follow to solve the problem. Support the vendor through to resolution.



## Improve cybersecurity education and training for vendors

For years, employee education programmes have demonstrated outsized impact on organisational cybersecurity. The same is true for vendor education. **Too often, vendors are unaware of their cyber risk,** and so do not implement appropriate asset management, cybersecurity training, or cybersecurity protocols.

**Methodology:** 2021 survey carried out by Opinion Matters on behalf of BlueVoyant with a sample of 1,200 18+ CTOs/CSOs/COOs/CIOs/ CISOs/CPOs responsible for supply chain & cyber risk management in the US, Canada, Germany, The Netherlands, UK and Singapore, working in companies employing 1,000+ employees guaranteeing at least 50 respondents per industry sector per country in the following: Financial services, Healthcare & pharmaceutical, Utilities & Energy (combined: equal split), Business services (i.e. professional services/ legal and so forth), Manufacturing, Defence. 300 respondents were from the UK.

2020 survey carried out by Opinion Matters on behalf of BlueVoyant with a sample of 302 18+ CIOs/CISOs/CPOs responsible for supply chain & cyber risk management working in companies employing 1,000+ employees in the UK. Opinion Matters abides by and employs members of the Market Research Society which is based on the ESOMAR principles.



## About BlueVoyant

At BlueVoyant, we recognize that effective cyber security requires active prevention and defense across both your organization and supply chain. Our proprietary data, analytics and technology, coupled with deep expertise, works as a force multiplier to secure your full ecosystem.

Accuracy. Actionability. Timeliness. Scalability.

Founded in 2017 by former Fortune 500 executives and former government cyber officials, BlueVoyant is headquartered in New York City and has offices in Maryland, Tel Aviv, San Francisco, Manila, Toronto, London, Latin America and Budapest. Visit [www.bluevoyant.com](http://www.bluevoyant.com)



BlueVoyant|UK®

To find out more about how BlueVoyant can help you secure your organisation against third-party cyber risk visit [\*\*www.bluevoyant.com\*\*](http://www.bluevoyant.com)

