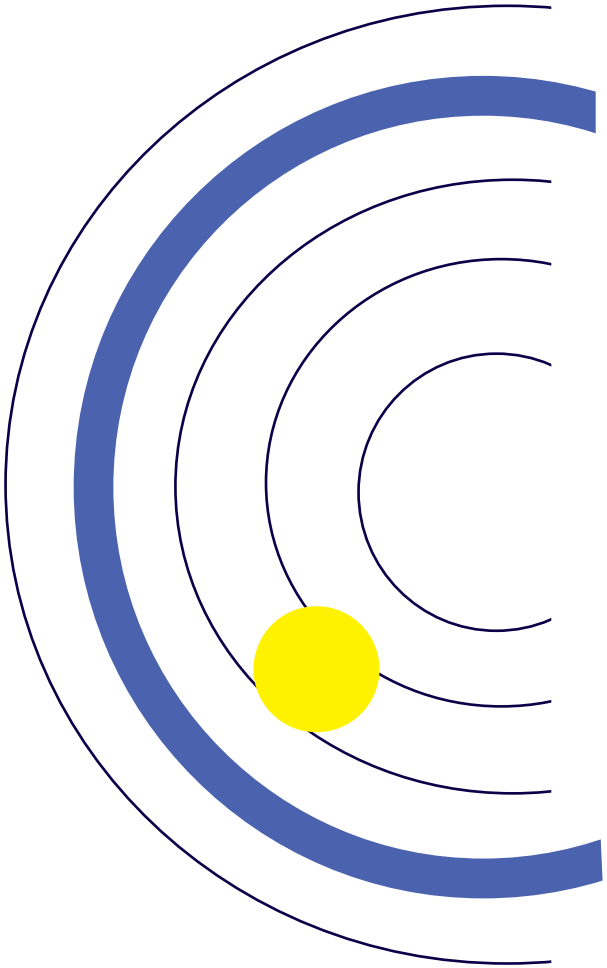
BlueVoyant

UK REPORT

GLOBAL INSIGHTS:
SUPPLY CHAIN CYBER RISK

MANAGING CYBER RISK ACROSS THE EXTENDED VENDOR ECOSYSTEM



Report Survey **Methodology**

BlueVoyant commissioned its first annual survey undertaken by independent research organisation, Opinion Matters, in June 2020. 302 UK 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. To gain a global perspective the research was conducted in the following countries: United Kingdom, USA, Switzerland, Mexico and Singapore.

Foreword

The global third-party cyber risk management landscape

By Jim Penrose, COO, BlueVoyant

Managing third-party vendor cyber risk is fast becoming the defining cybersecurity challenge of our time. As organisations have increased the number and variety of suppliers they work with in the pursuit of competitive advantage, they have simultaneously exposed their enterprise network to the vulnerabilities of those partners. Put simply, the extended ecosystem is the threat.

In a cyber threat environment where adversaries are well-resourced, sophisticated and relentless, a breach in a single one of what may be thousands of affiliated vendors can have catastrophic impact. Attacks such as NotPetya are testament to the fact that the interdependency between businesses means an attack on a vendor – who may be deemed unimportant to the primary organisation – can quickly spread with devastating consequences.

The result is that organisations face large-scale cyber risk across a heterogeneous supplier network, especially from the long-tail of vendors that would typically be below the cut-line for continuous monitoring. Understanding the scale and scope of third-party cyber risk, the impact it is having, and the way cyber risk management professionals are mitigating the issue is critical if, as an industry, we are to level up our defences and drive risk out of partner networks.

We asked more than 1500 CIOs, CISOs and CPOs across five countries, 302 were from the UK, to share their approach to managing third-party vendor cyber risk, exploring the scale of the challenge they face; the actual level of breaches originating in the supply chain; the resources they have at their disposal and the level of investment they are planning over the coming year.

The responses show a landscape where large vendor ecosystems are leading to frequent breaches and major business impact. Professionals are experiencing multiple pain points in operationalising their cyber risk management programme as they attempt to gain visibility and drive risk-reduction actions across a vast supplier base. Despite investment being on the rise, there remains a lack of clarity over where ultimate responsibility for third-party cyber risk lies. Ownership of this challenge at the senior leadership level is crucial to operationalising third-party vendor cyber risk management.

01

At a **Glance** Findings

> Time and again, as organizations investigate the sources and causes of malicious cyber attacks on their infrastructures, they discover that more often than not, the attack vector is within the infrastructure owned by third-party partners. Organizations must be responsible for protecting not only their own networks and data, but also ensuring that the same protections are in place in their third-party partner systems. The risks are significant and growing, and the mandate is clear.
>
> Organizations must understand and actively engage in the protection and defense of their entire ecosystems. Understanding third-party vendor risk is critical, as is understanding who is accountable and responsible for managing these risks. This report establishes the foundation for both.

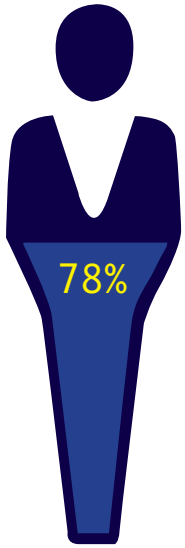
DEBORA PLUNKETT, BlueVoyant Board of Directors and former Director of Information Assurance, NSA

82%

Have suffered a breach at the hands of a third-party in the past 12 months

2.6

Average number of breaches experienced in the past 12 months



78%

of respondents said they have limited visibility around their third-party vendors

02

Key Survey Findings

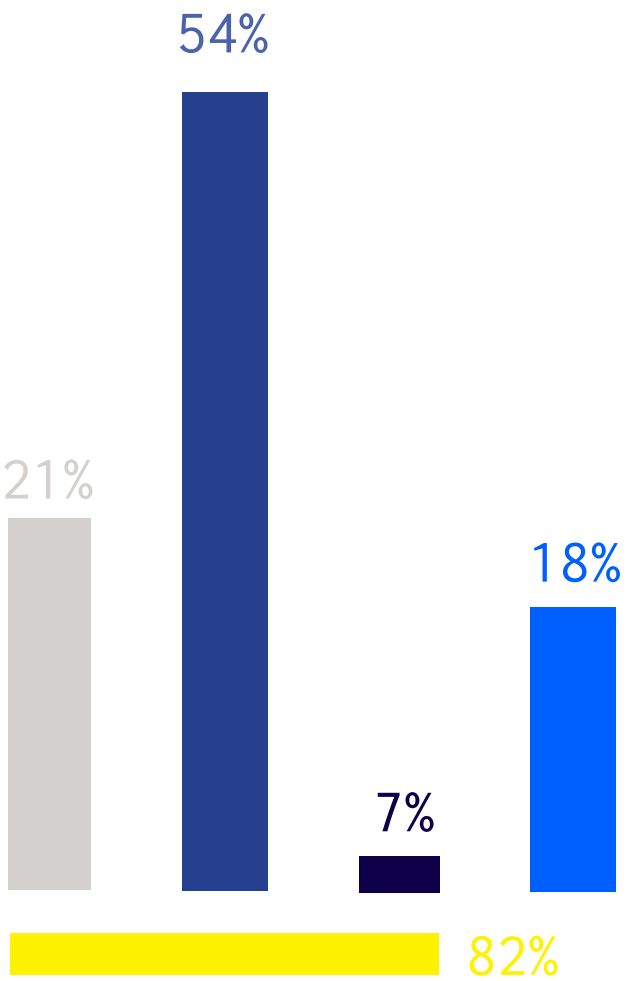
Key Survey Findings

34%
of respondents said they had no way of knowing if a risk emerged in a third-party

Vendor ecosystems are expansive and vendor-originated breaches are common

The research found that UK organisations have a lot of vendors in their supplier ecosystem, an average of 1013. These vendors are causing significant cyber risk with 82% saying they have suffered a breach in the last 12 months as a result of weakness in the supply chain. The high number of vendors and high percentage of organisations reporting breaches via the supply chain is proof that monitoring the extended supply chain is a large and growing challenge for UK organisations.

Overall, 82% have suffered one or more **breaches** in the past 12 months



Frequency of Vendor Related Breaches in the Past 12 Months

- 21% 1 breach
- 54% between 2 and 5 breaches
- 7% between 6 and 10
- 18% have not suffered a breach

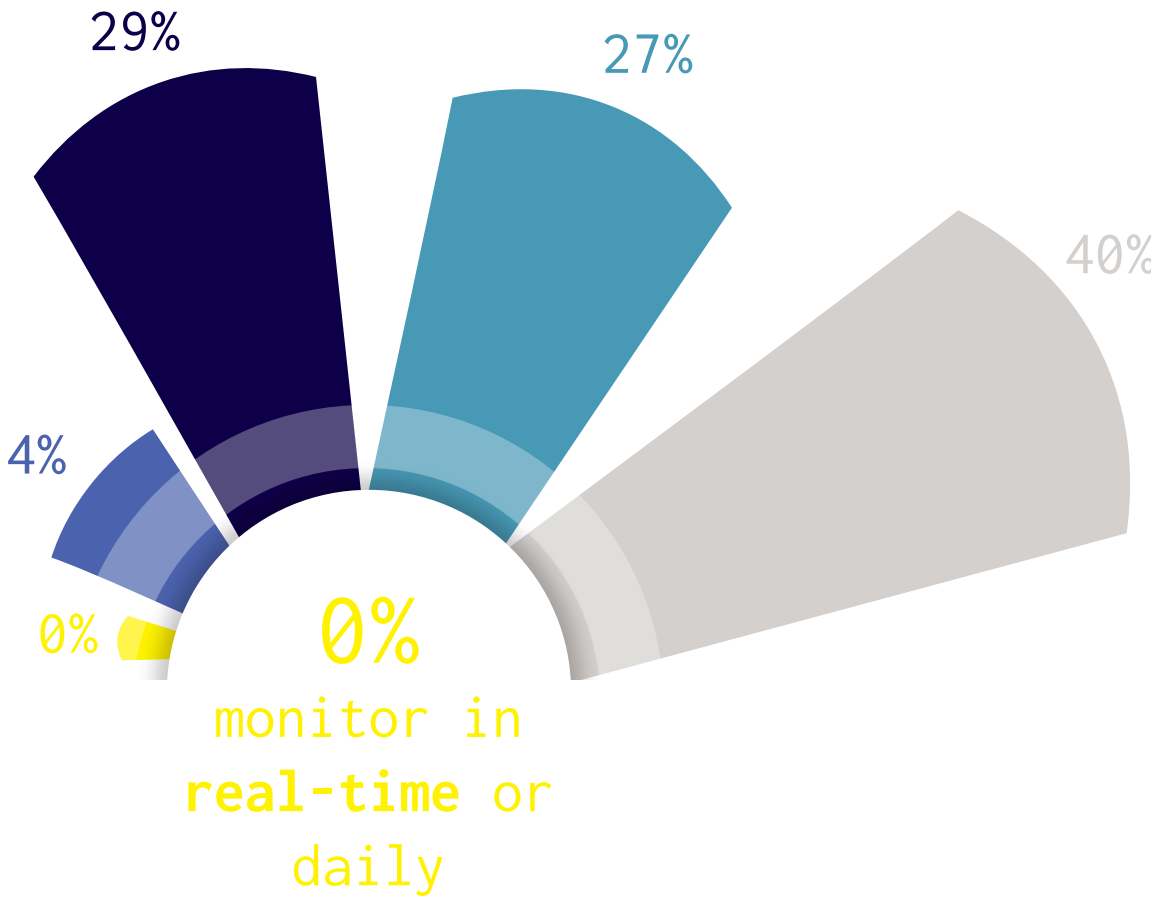
Vendor risk visibility and continuous monitoring is concerningly low

The scale of third-party vendor ecosystems is causing difficulties across the board, with evidence that limited resources are forcing organisations to compromise on the scope of their monitoring programme. Only just over one fifth (22%) said they monitor all vendors, meaning 78% do not have full visibility. 24% said they monitor only critical vendors while 20% said they monitor critical and top third-party vendors. This leaves a long-tail of vendors entirely unmonitored, with risk potentially arising from any of them on a given day.

40% only reassess and report on third-party cyber risk six monthly or less frequently, meaning they spend at least half a year with no insight into the changing risk in their supply chain. Over one quarter (29%) are re-assessing and reporting monthly. A further 27% are doing this quarterly. Just 4% re-assess and report weekly. This severely limits their ability to respond to emerging threats and can lead to serious negative findings when audits do take place, due to the extent to which threats have matured by the time they are identified.

- 0% monitor in real-time or daily
- 4% weekly
- 29% monthly
- 27% quarterly
- 40% six-monthly or less frequently

How Frequently Respondents Re-assess Third-Party Vendors in the Past 12 Months

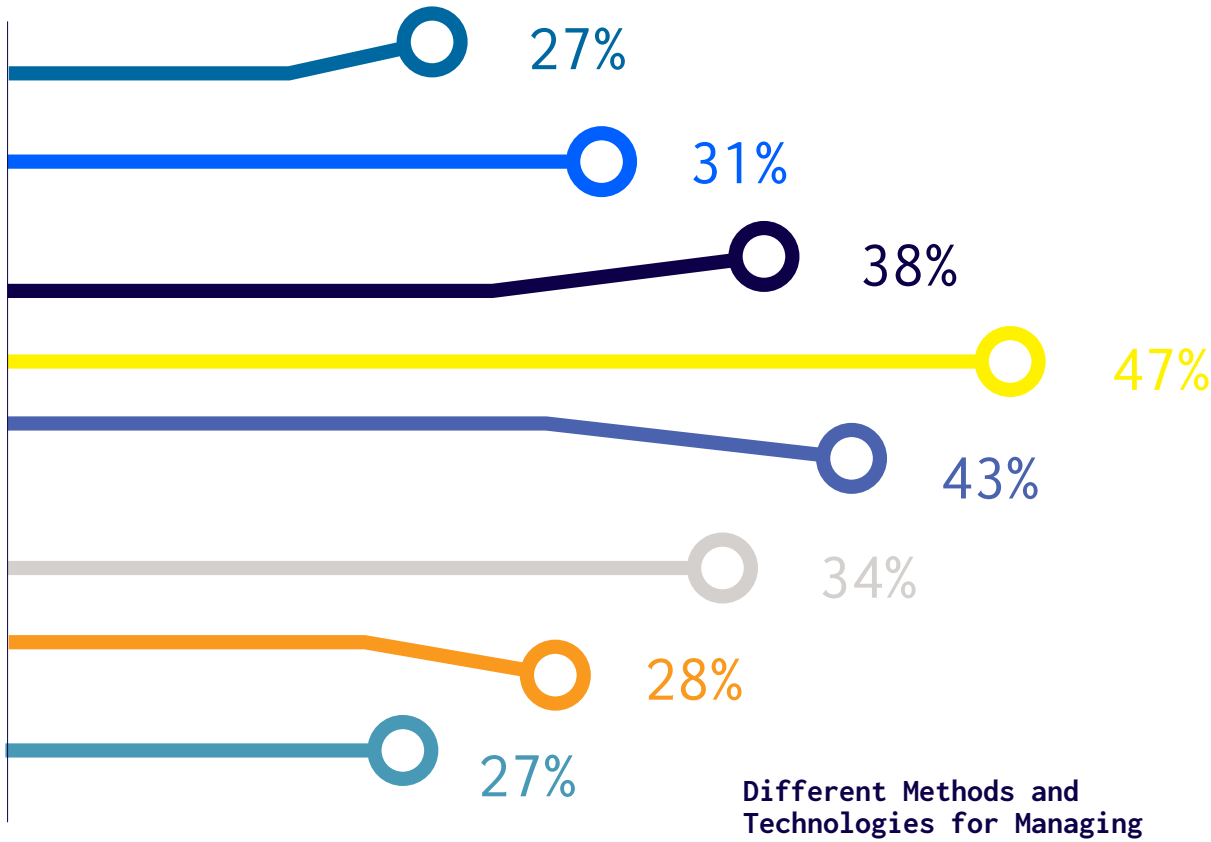


Patchwork of approaches creates operational drag

This lag in risk discovery was also evident when we asked about the tools in place to implement third-party risk management; we found a mix of approaches with no single strategy dominating. Many organisations are evolving towards a data-driven strategy, with supplier risk data and analytics in use by 47%. However static, point-in-time tactics such as on-site audits and supplier questionnaires remain common.

The multiple approaches used by organisations also presents a management challenge when it comes to working with unresponsive vendors and enforcing SLAs.

47% use **supplier risk** data and analytics



Different Methods and Technologies for Managing Third-Party Cyber Risk

- supplier risk data and analytics
- vendor risk management
- security ratings services
- external consultants
- integrated risk management
- exchanges and marketplaces
- onsite audits
- questionnaires

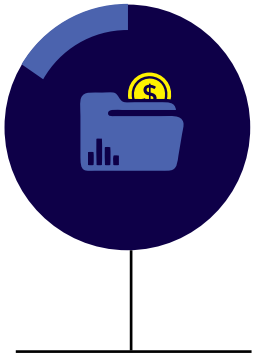
Respondents could tick more than one answer

Budgets are on the rise but multiple pain points diffuse areas for investment

Given the number of breaches originating in the supply chain, it is not surprising that organisations are ramping up investment to tackle the issue. 87% of UK respondents said their budget for third-party cyber risk management has increased compared to the past twelve months. This was the highest percentage increase out of all five countries. These budget increases will likely be partially allocated to headcount: UK respondents said they had an average of 11.7 people in their in-house teams, and those that outsourced cyber risk management typically handed it to teams of similar sizes. Resources are clearly being dedicated to managing cyber risk but are they being directed where it matters?

There are signs of recognition that the problem needs to be addressed – budgets are rising - but if they are not allocated effectively in a way that gives visibility across the whole vendor ecosystem, UK companies will not be able to stem the tide of third-party cyber risk.

Other areas for investment are unclear, as we saw when we asked respondents to tell us where the top three biggest pain points lay in third-party cyber risk management. The responses highlighted the complexity and multiple challenges involved in implementing programmes and how difficult it therefore is to choose a single area to work on. The most common response was handling the challenges of dealing with unresponsive vendors (25%). Overall, given the choice of 13 possible pain points, no single issue stood out, indicating the diversity of fronts on which programmes are causing problems. This shows that there is a very long way to go before organisations can be confident that they have an effective, comprehensive third-party cyber risk management programme in place.



87%

of UK respondents said their budget for third-party cyber risk management has increased

11.7

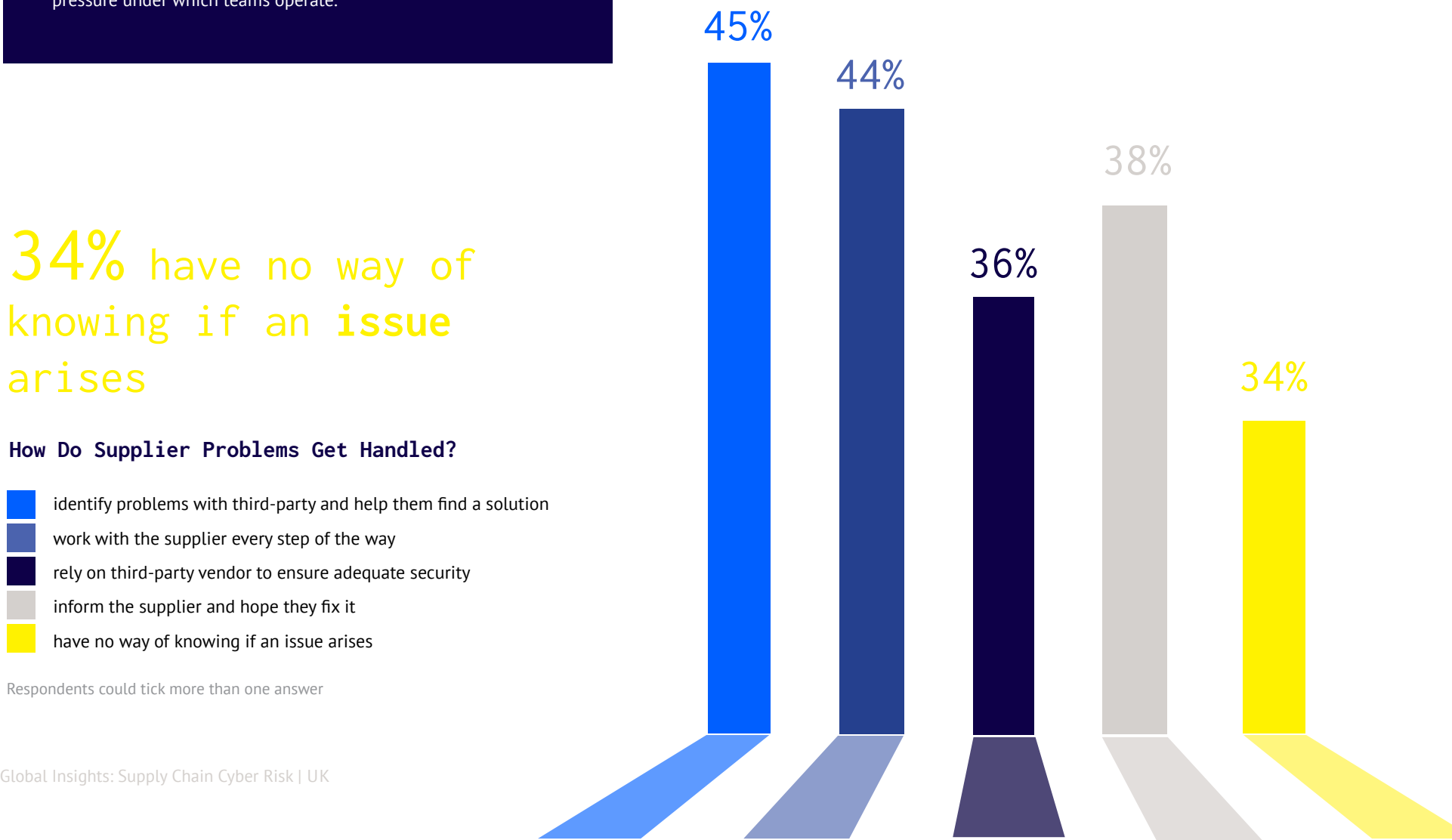
People in their own in-house teams

Over a third take a hands-off approach when they find a vendor problem

Organisations are not always upfront with suppliers when they do discover a problem. 38% inform the supplier and hope they fix the issue, while 36% rely on the supplier to ensure adequate security. This lack of control and proactivity when it comes to protecting the business is a matter of concern, but likely derives from the pressure under which teams operate.

34% have no way of knowing if an **issue** arises

How Do Supplier Problems Get Handled?



Respondents could tick more than one answer

Our research revealed much of the complexity and tension involved in third-party vendor cyber risk management. Awareness of the issue is on the rise, as vendor-originated breaches are frequent and organisations plan investment, but the scale and scope of the challenge seems to be leading many organisations to resign themselves to compromise, leaving large parts of the ecosystem unmonitored. These gaps and the patchwork use of different tactics and management tools leaves organisations struggling to work out what is important and unable to manage suppliers proactively in order to prioritise and remediate.

A business that is on the back foot when it comes to cyber risk visibility is highly vulnerable to the kinds of serious breaches that we are seeing more and more often across the cyber environment. This is especially true for the long-tail of cyber risk in the smaller vendors that have been overlooked due to constraints on the programme.

> It is very important to review the security of your vendors before you engage them, to make sure they are capable of meeting your needs or otherwise enhancing their controls before they are onboarded. But, it is equally important to establish an approach of continuous monitoring to help assure that such control continues to be in place over the life of the engagement.

PHIL VENABLES, Board Director, Goldman Sachs and Senior Advisor (Risk and Cybersecurity)

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 organisations are experiencing frequent vendor-originated breaches. While there is recognition that more investment is needed - budgets are rising universally – with organisations 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

Until this question is answered, it is impossible to adopt a coherent and effective strategy to manage it. Take third-party cyber risk out of operational siloes and integrate it fully with the organisation's overall risk management strategy, subject to board oversight. Clearly define lines of responsibility, reporting, and budget ownership.

Improve visibility of the supply chain by operationalising the data that you already collect

so you gain better insight and maximise the value of existing resources. Automate analysis where possible to lift the burden on in-house teams and enable them to focus on the most critical risks, the exceptions that need action versus the raw cyber risk data itself.

Expand assessment, monitoring and reporting programmes

to cover the long tail of vendors, not just critical suppliers. Identify areas where aggregate risk is high in vendors outside tier 1.

Refine organisational risk tolerance and apply it to third-party cyber risk management

Prioritise and triage critical risks in the context of their impact on the organisation.

Reduce false positive alerts

and remove the "noise", so in-house teams can focus on analysing key risks. Enable your in-house teams to be exception handlers dealing with the most important issues day-to-day versus the analysis of raw cyber risk data which is very time consuming and requires special skills.

Drive supplier risk-reduction activity

by building constructive support for suppliers into your third-party cyber risk management programme. 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.

Full Survey Findings

03

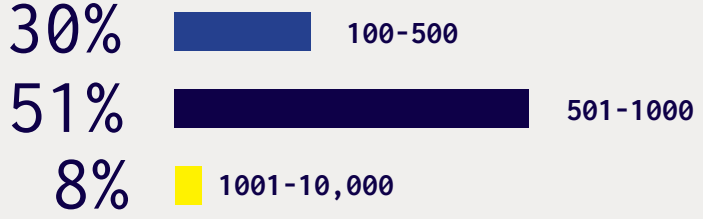
How many vendors/suppliers do you currently work with?

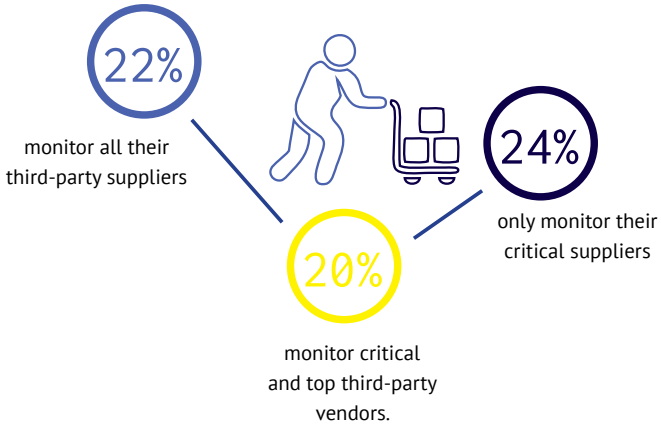
UK respondents work with a mean number of vendors of 1013. Typically, bigger companies work with more vendors.

The sector with the highest average number of vendors/suppliers was energy – 1783 - followed by utilities - 1335.

In terms of job role, the CIO is working with the largest number of suppliers and had the highest mean average of 1131.

30% of the respondents said they work with 100-500 vendors, while over half (51%) reported that they work with 501-1000 vendors. 8% work with anywhere between 1,001 – 10,000 vendors.





Which of the following statements applies to your company's handling of cybersecurity risk and third-party suppliers? [tick all that apply]

48% of respondents said that handling of cybersecurity risk and third-party suppliers is on their radar. However, 28% said it was not on their radar. 28% of respondents said it is a key priority while 24% said it was somewhat a priority and 14% said it was not a priority at all.

22% of respondents said they monitor all their third-party suppliers, meaning 78% have limited visibility. 24% admitted they only monitor their critical suppliers and 20% said they monitor critical and top third-party vendors.

Utilities (74%) and the business services (73%) sectors were most likely to say third-party cybersecurity risk was on their radar. While the financial services sector (59%) was the highest in saying that it was not on their radar.

Out of the three, CIOs were most likely to say third-party cyber risk is a key priority (43%) and CISOs scored the highest percentage in saying it is not on their radar.

Which different methods and types of technologies do you use to manage third-party/supply chain risk?

The most commonly selected response was supplier risk data and analytics (47%) followed by the use of vendor risk management (43%) and in third place 38% of UK respondents said they use security ratings services.

The utilities sector scored highest in using questionnaires (44%) and onsite audits (34%) and exchanges and marketplaces (46%) and security ratings (52%). In fact, utilities appears to be using more tools in general than other sectors. While the financial services sector (43%) and manufacturing (44%) scored highest in using integrated risk management. The healthcare & pharmaceutical sector are most likely to be using supplier risk data and analytics (62%).

The CIOs scored highest on using onsite audits (30%) and questionnaires (35%) while CISOs scored highest on using security rating services (42%).

27%

Over a quarter of UK respondents (27%) still use onsite audits and 28% still rely on questionnaires.

What is the size of your cyber risk team, in-house and outsourced, that manages your supply chain/third-party risk?

The average in-house team size is 11.6. This rises to 13 in both the manufacturing and utilities sector.
The average outsourced team size is 11.9. This rises to 14.4 in the utilities sector.

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?

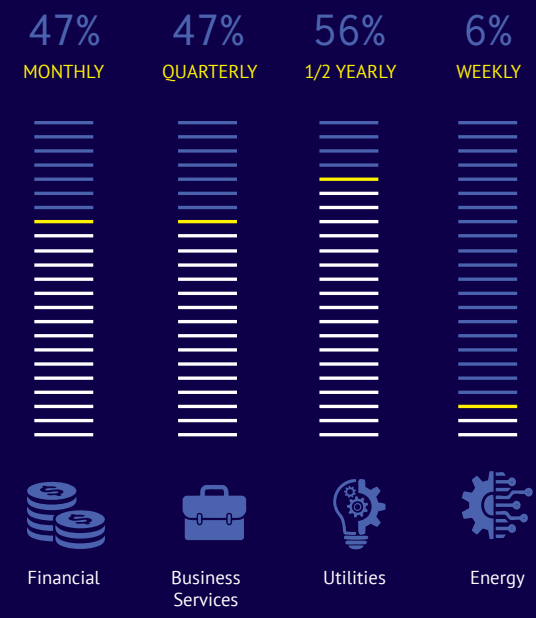
Just under one third (29%) of UK respondents are re-assessing and reporting monthly. A further 27% are re-assessing quarterly and 40% are operating an either annual or six-monthly cycle. Just 4% re-assess and report on risk weekly.

Financial Services (47%) are more likely to be re-assessing/reporting monthly than other sectors. Business services scored highest on reporting quarterly (47%). Manufacturing (42%) and utilities (56%) favour six monthly re-assessing and reporting.

CISOs scored highest out of the three to be re-assessing third-party cyber risk monthly (47%), while CIOs and CPOs were more likely to be doing this six-monthly.

How frequently do you audit?

Vertical markets that scored highest in each category



Has your budget for supply chain/ third-party cyber risk management changed compared to the past 12 months, and if so, how?

Money is being allocated to third-party cyber risk showing how it is rising up the corporate agenda. 87% of UK respondents said their budget had increased. Only 6% said their budget had stayed the same. 49% have seen increases of between 26-50% and 28% have seen increases of between 51-100%. The average budget increase was 45%.

Financial services has seen the biggest percentage increase, by 58% on average. Astonishingly 16% of those in healthcare & pharmaceutical sector have increased their budgets by more than 100%.

CPOs have seen the highest average budget increase, by 58% on average.

64%

of healthcare & pharmaceutical respondents said that the CISO owns cyber risk.

Have you had any cybersecurity breaches because of weaknesses in your supply chain/third-party cyber risk in the past 12 months and if so how many?

82% of UK respondents have suffered a breach because of supply chain/third-party cybersecurity weakness in the last 12 months. 54% have had between 2 and 5 breaches. 7% have had between 6 and 10. The average number of breaches for UK respondents was 2.6.

Utilities suffered most breaches with an average of 3.7. Manufacturing has the lowest average at 1.4.

CISOs report more breaches (3.2) than CIOs (3) and CPOs (1.6). 64% of CISOs surveyed have had between 2 and 5 cybersecurity breaches.

Who owns cyber risk within your organisation? For example, when the CEO is asking the question who is answering it?

Just under half of respondents (47%) said the CIO owns cyber risk, while 38% said the CISO and just 11% said the CPO.

64% of healthcare & pharmaceutical respondents said that the CISO owns cyber risk.

Interestingly, if you're a CIO you're more likely to say it's the CIO who has responsibility (78%) while 71% of CISOs say it is they who have responsibility! 29% of CPOs say cyber risk is their responsibility.

If you find a problem with regard to your third-party/supply chain cyber security how do you go about remediation?

45% of respondents said that when they identify problems with their third party, they work with them to help find a solution. (This rises to more than 60% in the energy sector). 44% work with the supplier every step of way until the issue is rectified. However, 38% inform the supplier and hope they fix it while 36% rely on the third-party supplier to ensure adequate security.

Over one third, 34%, admitted to having no way of knowing if any issues arise with third-party cybersecurity. This rises to 60% in the utilities sector who say they have no way of knowing.

What are the biggest challenges/pain points when managing your third-party cyber risk/supply chain risk?

Out of 13 different pain points listed there were many that were causing problems, indicating that these issues were coming from multiple fronts.

The top three were:
Dealing with unresponsive third-party suppliers/vendors when there is a problem (25%), working with suppliers to improve their security performance (22%) and enforcing SLAs with all our third-party suppliers and getting them to comply (21%).

About BlueVoyant

BlueVoyant is an expert-driven cybersecurity services company whose mission is to proactively defend organisations of all sizes against today's constant, sophisticated attackers and advanced threats. Led by CEO Jim Rosenthal, BlueVoyant's highly skilled team includes former government cyber officials with extensive frontline experience in responding to advanced cyber threats on behalf of the National Security Agency, Federal Bureau of Investigation, Unit 8200 and GCHQ, together with private sector experts. BlueVoyant services utilise large real-time datasets with industry leading analytics and technologies.

Founded in 2017 by Fortune 500 executives and former Government cyber officials and headquartered in New York City, BlueVoyant has offices in Maryland, Tel Aviv, San Francisco, London and Latin America.

About DVV Solutions

DVV Solutions was established in 1999, and has become one of the UK's leading providers in the design, implementation, and management of Third Party Risk Management (TPRM) solutions and services. Our suite of consultative and managed services improve every organisation's ability to manage the increasing numbers and complexity of risks and regulatory requirements from outsourced operating models backed by leading risk intelligence and automation platforms including BlueVoyant's CRx suite.

As a Shared Assessments Program member and registered Assessment Firm we utilise industry recognised best practices and methodologies, including Standardised Information Gathering (SIG) questionnaires, Third Party Privacy Tools, and the Vendor Risk Management Maturity Model (VRMMM) to deliver robust and scalable programs of third-party risk assurance and supplier due diligence.

BlueVoyant®

BlueVoyant UK
Nova North
11 Bressenden Place
Westminster, London, SW1E 5BY

Email: contact@bluevoyant.com
www.bluevoyant.com

DVV solutions

DVV Solutions
Grosvenor House
St. Thomas's Place
Stockport, Cheshire, SK1 3TZ

Email: enquiries@dvvs.co.uk
www.dvvs.co.uk