BLUEVOYANT REVIEW

Managing Cyber Risk Across the Extended Vendor Ecosystem

2021

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

1,200 CIOs, CISOs and CPOs (Chief Procurement Officers) responsible for supply chain and cyber risk management were surveyed from companies with 1,000-plus employees across a range of industries including: business services, financial services, healthcare and pharmaceutical, manufacturing, utilities and energy, and defense. To gain a global perspective, the research was conducted in the following countries: U.S., Canada, Germany, The Netherlands, the United Kingdom, and Singapore.

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 cyber attacks have affected multiple industries in waves: Accellion, SolarWinds, Kaseya. 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, defense companies, utilities, healthcare systems, and governments. SolarWinds is estimated to have cost in excess of $100 billion. The importance of third-party cyber risk management has been proven to be a necessary component of an overall risk management program.

The question remains of how companies and the 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. Simply gaining visibility into the supply chain 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. The responses show a fractured landscape, with different industries and regions responding differently to the challenges posed by another year of damaging, costly cyber events.

Companied across all industries and across all of the countries surveyed in this report are investing in cybersecurity. However, some still hesitate to make third-party cyber risk a strategic priority and to coordinate and formalize their approach to cyber defense and remediation. In addition, many companies struggle to assign ownership of their third-party cyber risk program.

Adversaries can now actively scan organizations 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 program, as well as raise awareness at the senior executive and board level to help the business understand the resources needed to protect the business.

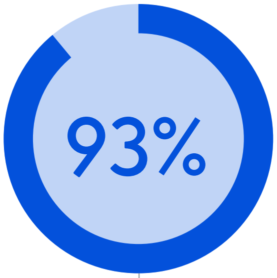
Table of Contents

BlueVoyant®

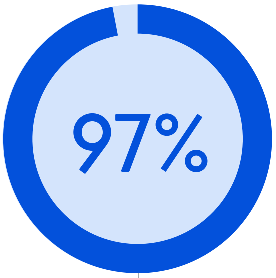
GLOBAL REPORT

At-a-Glance Findings

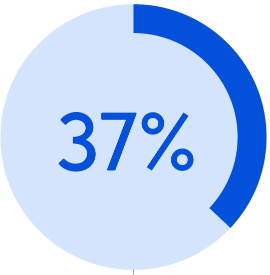
At-a-Glance Findings



93% have suffered a cybersecurity breach because of weaknesses in their supply chain/third-party vendors



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

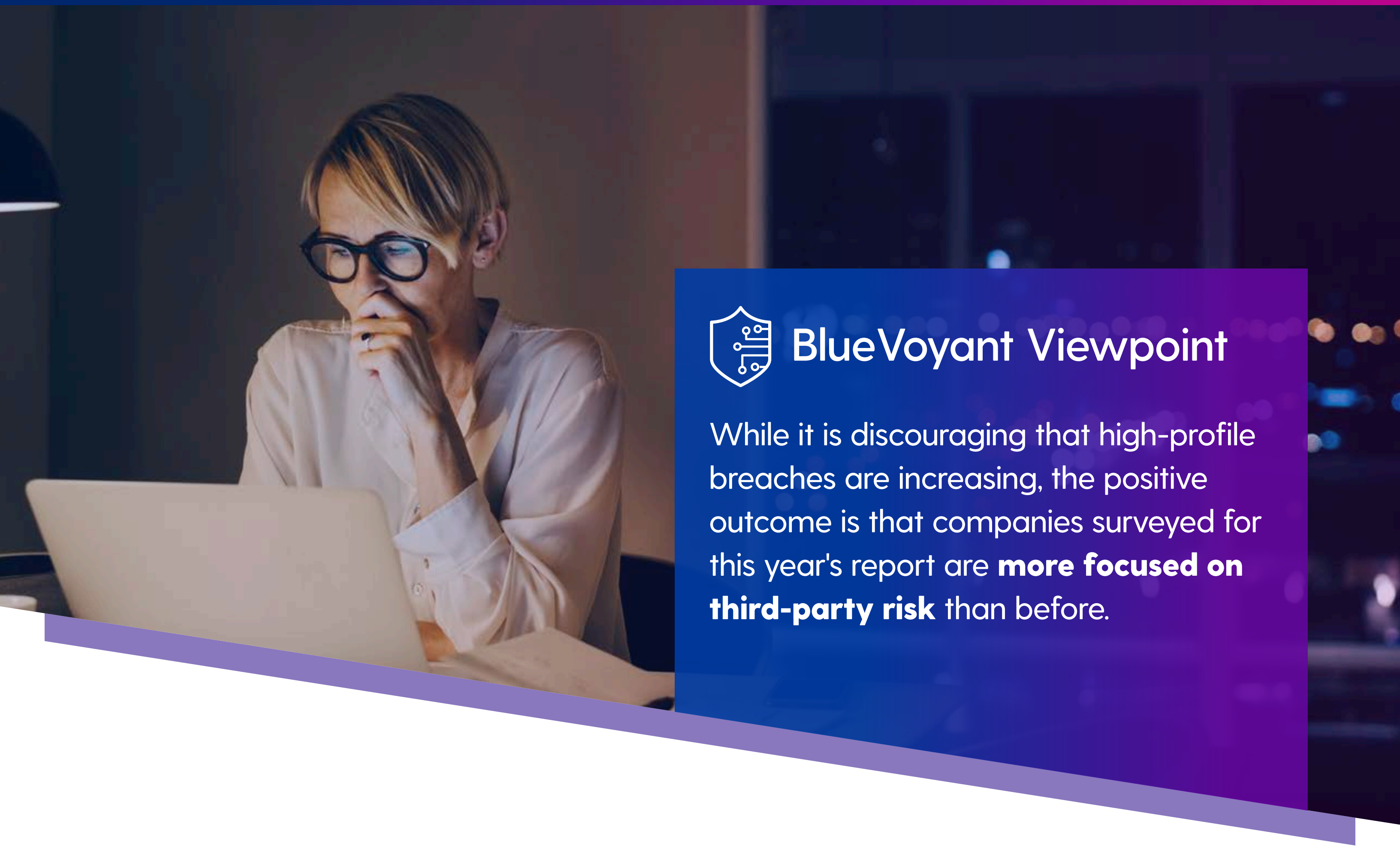


The average number of breaches experienced in the last 12 months grew from 2.7 in 2020 to 3.7 in 2021 — **a 37% year-over-year increase**

BlueVoyant®

GLOBAL REPORT

Key Survey Findings



BlueVoyant Viewpoint

While it is discouraging that high-profile breaches are increasing, the positive outcome is that companies surveyed for this year's report are **more focused on third-party risk** than before.

Key Findings

Companies are more focused on third-party and supply chain cyber risk and more aware of their vendor ecosystems than in 2020

Last year, a surprising 31% of companies said that supply chain and third-party cyber risk was not on their radar. This year, by comparison, only 13% of companies said that third-party cyber risk was not a priority. **In this year's survey, it is clear priorities have shifted** in response to a rapidly evolving cyber threat landscape.

The number of companies reporting a supply chain of more than 1,000 companies more than doubled from 14% in 2020 to 31% in 2021. At the same time, the number of companies reporting 500 vendors or fewer dropped from 29% to 22%. It is possible that supply chains exploded, but it is more likely **that companies became more aware of the full extent** of their vendor networks.

Vendor risk visibility and continuous monitoring remains low

The frequency of assessing third-party risk and briefing senior management dropped from the 2020 survey to the 2021 survey. **More companies in 2021 assessed their vendors less frequently.** Forty-seven percent audited or reported on vendor security no more than twice per year, compared to 32% in 2020. And the number of vendors practicing continuous monitoring also dropped, from 0.9% to 0.5%.

2021	2020
47% audited or reported on vendor security no more than **twice per year**	**32%** audited or reported on vendor security no more than **twice per year**
.5% number of vendors practicing continuous **monitoring dropped**	**.9%** number of vendors practicing continuous **monitoring dropped**

This highlights two areas of concern

This year, many of the most damaging third-party cyber attacks occurred immediately after discovering new critical vulnerabilities. For example, the January 2021 cyber attacks that exploited weaknesses in Microsoft Exchange **began within days of the exploits being discovered.** Without continuous monitoring and rapid remediation, cyber attacks similar to this can leave organizations vulnerable to significant threats for an extended period of time.

Third-party cyber risk management needs to be, and can become, a strategic priority for the business by ensuring communications around third-party cyber risk management is consistently communicated to senior management and the board.

BlueVoyant Viewpoint

Taken together, these findings are concerning and suggest that **organizational willpower alone is not enough to overcome institutional inertia.** While budgets for cybersecurity are increasing year-over-year, investments need to be tied to strategic initiatives with defined and actionable outcomes.

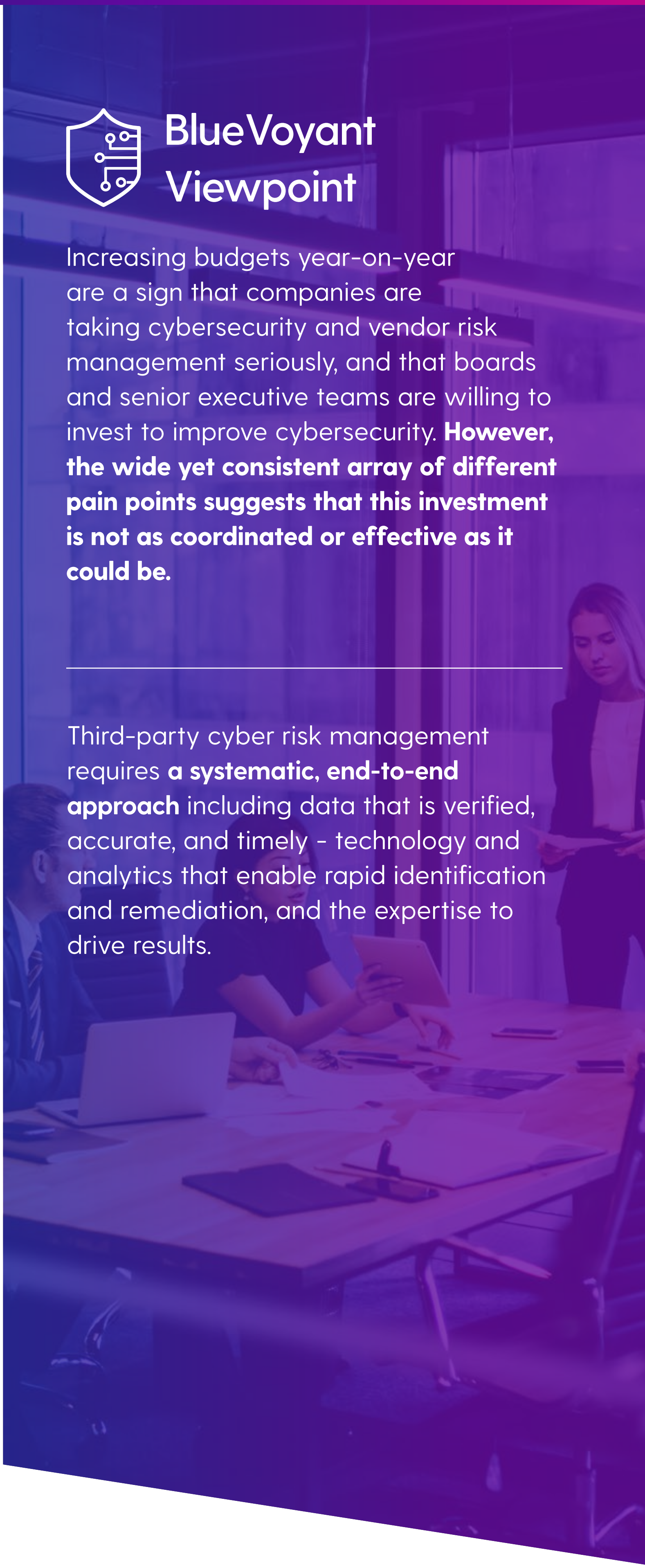
Budget for third-party cyber risk continues to rise year-on-year

Reports of budget increases matched figures from last year. Twenty-nine percent of companies reported budget increases of 26-50%; 42% reported increases of 51-100%; and 17% reported increases of 100% or more. Only 5% reported no increase, and just 4% reported a decrease.

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 an almost equal distribution of pain points** including reducing false positives, managing the volume of data, prioritizing risk, and knowing their own risk position. The fact that organizations are reporting so many similar issues indicated a high degree of commonality across different industries and region..

Many organizations are blind to cyber risk, unable to ensure that the issue is remediated

Thirty-eight percent of respondents said that they had **no way of knowing when or if an issue arises with a third party.** Forty-one percent said if they did discover an issue in their third-party ecosystem that they informed their supplier but were unable to easily verify if the issue had been resolved.



BlueVoyant Viewpoint

Increasing budgets year-on-year are a sign that companies are taking cybersecurity and vendor risk management seriously, and that boards and senior executive teams are willing to invest to improve 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.**

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.

BlueVoyant®

GLOBAL REPORT

Recommendations

Recommendations

Gain visibility into the supply chain

Supply chain ecosystems are large, multilayered, and complex. Getting 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.

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 the sine qua non of effective third-party cyber risk management. Automate analysis; expand assessment to include the "long tail" of vendors and not a limited number of critical suppliers; identify areas of non-substitutability or where risk is pooled.

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.**

Improve cybersecurity education and training for vendors

For years, employee education programs have demonstrated outsized impact on organizational 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.

BlueVoyant®

GLOBAL REPORT

Vertical Market Analysis

Business Services Sector

The business services sector, including legal, accounting, and consultancy firms, is a foundational area in the economy. Firms in this sector are frequently targeted by cybercriminals and nation-state actors who have a goal of stealing critical data, deploy ransomware to disrupt the firm, and use trust relationships between the firm and the client to move upstream in an effort to compromise a higher-value target.

Business services typically reported smaller supply chains than other industries, with

27% reporting vendor numbers

in the range from 101-500. However, a small number of business services firms reported astronomical vendor numbers, suggesting that large legal, accounting, and consulting firms take care to monitor a giant vendor ecosystem:

12% reported 10,001-50,000 vendors,

almost twice the average.

Business services had among the largest in-house cybersecurity or risk teams of all sectors

61% had a team of over 10

11% had 21-25 employees

more than twice the average.

Business services were **one of the few industries** reporting daily monitoring of third-party vendor risk.

Financial services and utilities had **THE HIGHEST PERCENTAGE** of respondents experiencing budget increases of

51-100%

Financial Services Sector

The financial services sector is the most-targeted vertical market as well as the most sophisticated and well-resourced to defend against cyberattacks. Financial services firms, including investment and retail banks, investment firms, and online financial platforms, typically support sophisticated in-house teams of cybersecurity and risk professionals and have an extensive cybersecurity technology stack.

In financial services, **the percentage of respondents** with 101-500 vendors is much smaller than overall (12% vs. 22%) and the percentage in the 1,001-10,000 range is much higher (40% vs. 31%).

Negatively impacted breaches: Financial services had an **especially low percentage of 1 breach responses and an especially high percentage of 2-5 breach responses** (31% and 59% for financial services, 42% and 49% overall). A similar, but less pronounced difference affected the energy sector (37% and 54% vs. 42% and 49%).

Financial service organizations are more likely to have the **CIO taking responsibility for cyber risk** (42% vs. 30% overall).

Financial services and utilities had the **highest percentage of respondents experiencing budget increases** of 51-100%, with 50% of each reporting this level, compared with 42% of organizations overall.

Healthcare/ Pharmaceutical Services Sector

The healthcare and pharmaceutical industries had a difficult year. For years, cyber attacks on healthcare organizations has been skyrocketing, as cybercriminal gangs increasingly target hospitals and healthcare systems to steal data or to extract ransom payments. Data breaches have become commonplace, as large, integrated healthcare systems find themselves targeted for the huge quantities of sensitive patient data they handle. The proliferation of digital healthcare tools has made healthcare easier to access, but also created a wide, exposed attack surface for opportunistic cyber actors.

Then COVID-19 happened. As the race to a vaccine attracted nation-state competition, and as hundreds of millions of patients flooded telehealth and other digital healthcare platforms, healthcare and pharmaceutical firms faced an unprecedented level of attack. Nation-state groups targeted pharmaceutical companies for vaccines and ransomware gangs became so ruthless that they precipitated a national healthcare crisis in France. The healthcare supply chain, a complex web of device manufacturers, digital services, small and large healthcare systems, and data storage and processing firms, came under pressure like never before.

Responses from the healthcare sector suggest the **highest overall level of awareness,** with 80% of respondents saying that supply chain/third-party cyber risk is on their radar and 20% saying that it is not, in comparison to overall percentages of 71% and 29%.

Healthcare and pharmaceutical had the highest percentage of responses identifying **supply chain/third-party cyber risk as a key priority** (55%) compared to an overall percentage of 42%.

Healthcare had an **especially high percentage of respondents reporting between 6-10 breaches** (29% vs. 19% overall) and a correspondingly lower percentage reporting breach numbers in the 2-5 range (44% vs. 56% overall).

Healthcare respondents demonstrated the **highest commitment to board scrutiny and increased investment of all vertical sectors surveyed**, indicating the level of pressure the sector has faced from malicious cyber attacks over the past 12 months.

25%

Manufacturing has the highest percentage of respondents who are reporting annually

Manufacturing Sector

The manufacturing sector has long suffered from being, in many ways, the ideal ransomware victim. Dependent on finely-tuned automated processes, relying on just-in-time deliveries and shipments, and sensitive to disruption, manufacturing companies were early and aggressively targeted by opportunistic cybercriminals looking to extract ransoms for locked systems.

Manufacturing firms also produce, and rely on, thousands of IoT devices, which make operations more efficient but are often not designed with cybersecurity in mind. Outdated IoT and SCADA systems create a large and inviting attack surface for potential attackers.

In the past year, persistent logistics and supply chain disruptions put manufacturing in the spotlight, as the supply of critical goods was delayed or halted. Further, nation-state attackers began to notice and focus attention on critical manufacturing subsectors, such as semiconductors. This increased attacker focus on manufacturing is mirrored by increased regulatory pressure, as new legislation on IoT device manufacture and use will force higher costs on manufacturing centers and services.

Manufacturing had the lowest percentage of responses identifying **supply chain/third-party cyber risk as a key priority** at 29% versus 42% across all industries.

Large manufacturing supplier ecosystems: While the percentage of responses in the less than 100 range is low across all industries at 9%, **it is especially low in manufacturing** (4%), where the percentage of responses in the 101-500 range is also slightly lower than the overall percentage (18% vs. 22%). The percentages of responses in the 501-1,000 and 1,001-10,000 ranges are higher (36% and 39% in manufacturing vs. 30% and 31% overall).

At the other end of the spectrum, manufacturing had the highest number of respondents for whom **supply chain/third-party cyber risk is not on their radar** at 36%.

Low reporting frequency: Manufacturing has the **highest percentage of respondents who are reporting annually** at 25% compared with 18% overall, and the lowest percentage reporting on third-party cyber risk on a monthly basis at 14% versus 20% overall.

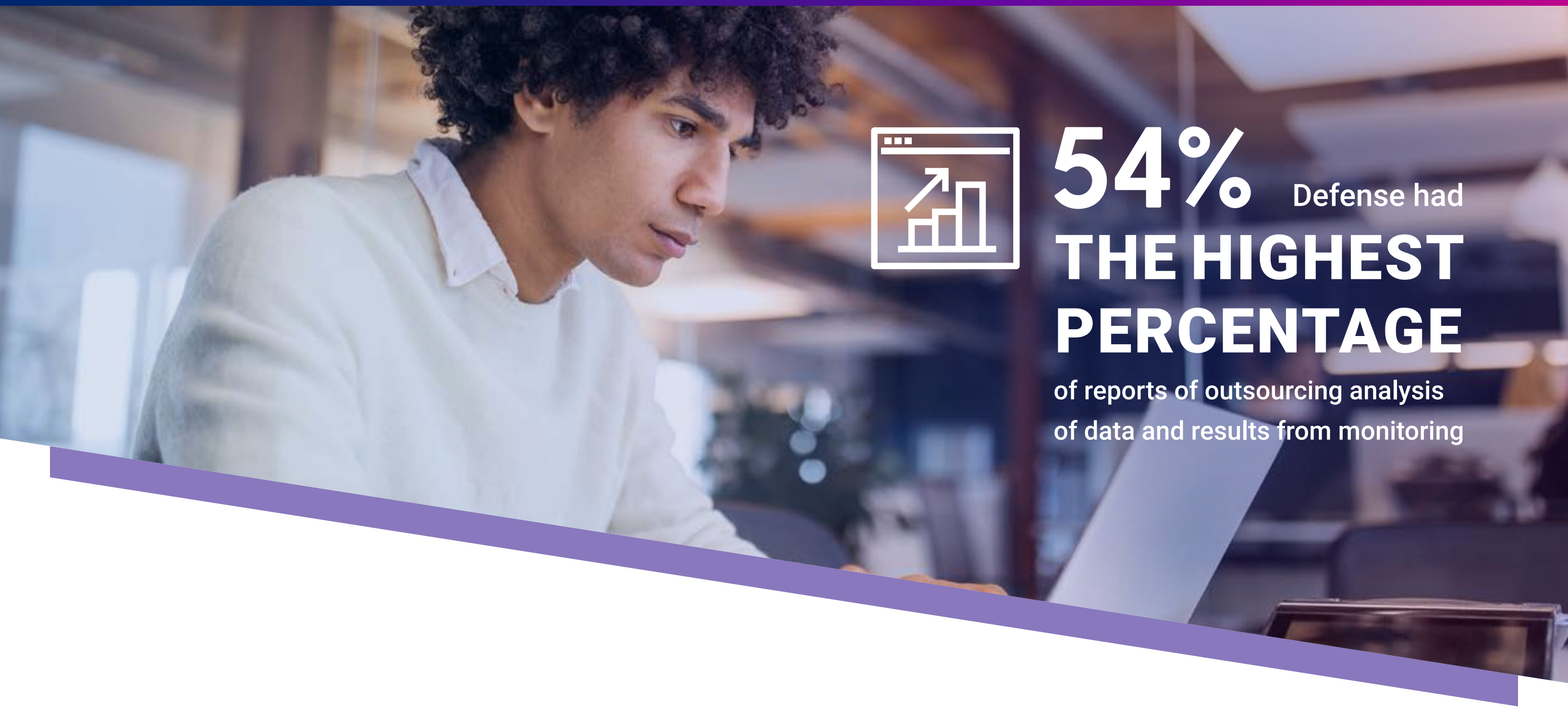
Utilities/Energy Services Sector

The utilities and energy sector have faced increasing pressure, and increasing scrutiny, from regulators as cyberattacks have shut down pipelines and disrupted power grids that are critical to day-to-day needs of the populations impacted. Cyberattacks have shifted focus to these historically less targeted organizations because ransomeware and other attack vectors against this sector creates an acute need for resolution, which may involve receiving payment to recover critical infrastructure.

Respondents from the utilities sector were **most likely to say they monitor all suppliers,** with 31% claiming to achieve this, compared with 22% overall.

Bi-annual monthly reporting was **especially high in the utilities and energy sector** (36% and 37% - the only ones above 30%, compared to 24% overall). However, it was notably low for weekly or daily.

CPOs are more likely to bear responsibility for **third-party cyber risk in the utilities and energy sector**, with 40% compared to an overall figure of 19%.


54% Defense had **THE HIGHEST PERCENTAGE** of reports of outsourcing analysis of data and results from monitoring

Defense Services Sector

Targeted for years as part of ongoing global power competition and espionage, defense firms and contractors were thrown particularly into the spotlight in 2021 thanks to several well-publicized campaigns - especially SolarWinds, but also Microsoft Exchange, Pulse Secure VPN, Kaseya ... the list goes on.

Defense firms have a complex task in securing their vendor networks. Reliance on huge supply chain networks for defense programs makes visibility difficult. A typical defense supply chain is not only large but also deeply heterogenous, including small manufacturing firms along with large and highly advanced R&D companies. The existence of extremely agile and persistent attackers, willing to move up and down the supply chain looking for weak links and novel exploits, underscores the need for continuous monitoring.

Defense had the highest percentages of respondents reporting that their **in-house team had 20-plus employees** at 13% vs. 10% overall.

Defense keeps senior teams in the loop compared to other sectors, **having the highest percentages** saying they brief senior teams weekly and daily, at 11% and 3%, respectively, compared with 8% and 1% overall.

Defense had the highest percentage of reports of **outsourcing analysis of data and results from monitoring** at 54% in defense, 47% overall.

BlueVoyant®

GLOBAL REPORT

Region-Specific Analysis

Global Insights: Supply Chain Cyber Risk Key Country Comparisons

	Who have suffered breaches	Supply chain risk is a key priority	Plan budget increases	Only re-assess six monthly or less frequently	Wouldn’t know if a risk emerged in a 3rd party
US/CA	97%	43%	89%	54%	36%
DE/NL	99%	43%	98%	58%	46%
UK	97%	27%	92%	29%	39%
SG	79%	56%	85%	46%	30%
GLOBAL	93%	42%	91%	47%	38%

US/CA: United States of America/Canada
DE/NL: Germany/Netherlands
UK: United Kingdom
SG: Singapore

28%

responded that their outsourced teams were in the 6-10 & 11-15 range.

21%

responded that their outsourced teams were in the 16-20 range.

43% of North American firms view supply chain risk as a **key priority for their company**

97% reported that they **suffered at least one breach** in the past year

89% **reported budget increases** for cybersecurity and third-party risk

31% vs. 26%

In North America, 36% reported bi-annually to a senior management team or the board vs. 26% globally.

25%

25% of North American respondents reported budget increases of more than 100%.

North America had a slightly higher percentage of respondents reporting between 6 and 10 breaches at 23% vs. 19% overall.

23% vs. 19%

Europe

Europe had the highest rate of reported malicious cyber breaches globally with 99% of respondents saying they had suffered at least one breach, and the highest percentage of respondents who said they planned budget increases for cybersecurity and supply chain risk (98%). It is clear that another year of persistent cyber attacks has led to another year of increased investment.

In Europe, a slightly higher percentage (58%) said they only audited or reported on third-party cybersecurity bi-annually or less, and almost one-third of respondents (31%) said they did not have any insight into whether or not an attack on a third-party vendor occurred.

Variations compared to other countries

In Europe, more responses **indicated smaller outsourced cyber-risk teams**:

37%

Responded that their outsourced teams were in the 6-10 range.

32%

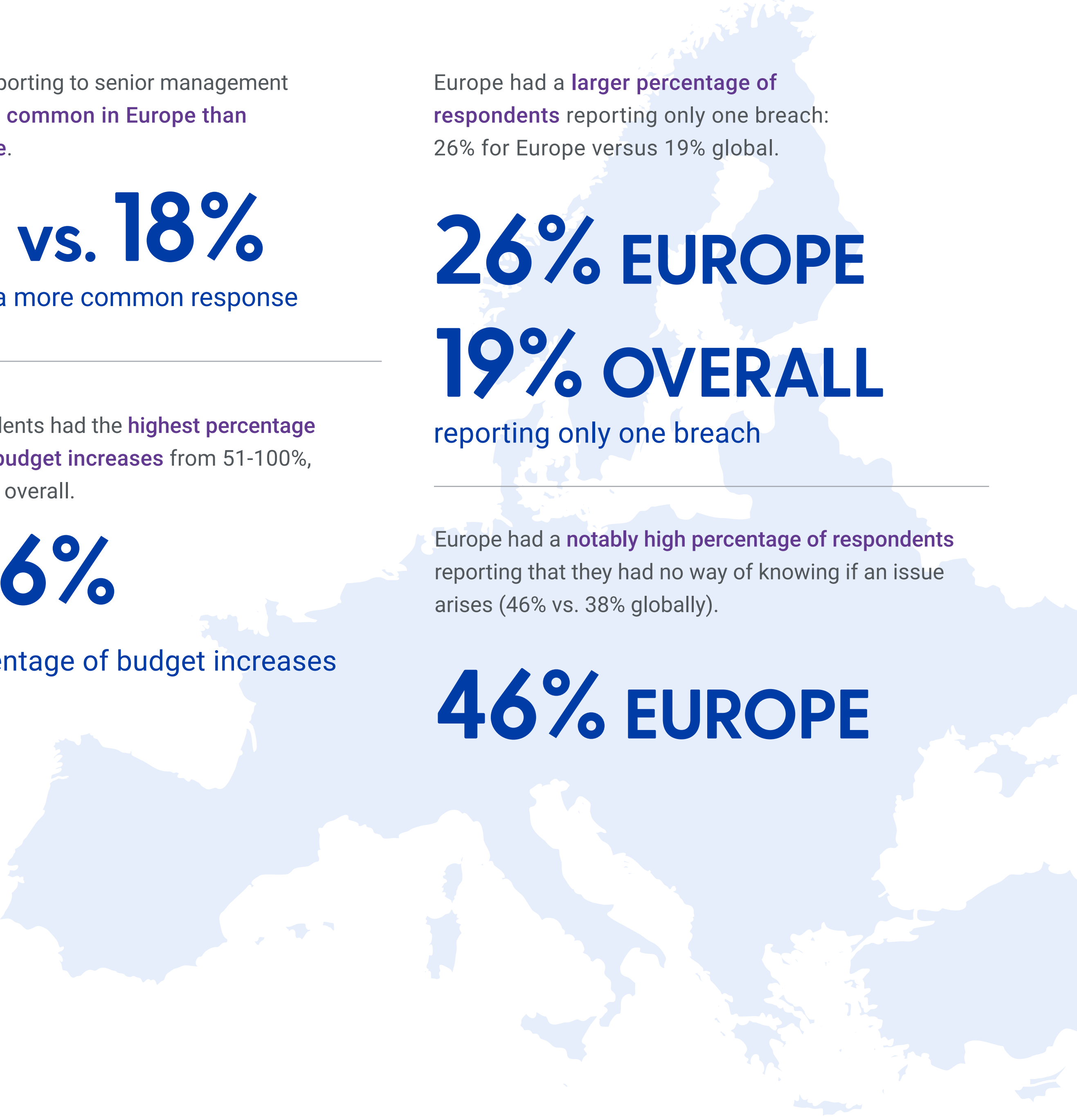
Responded that their outsourced teams were in the 11-15 range.

only 18%

Responded that their outsourced teams were in the 16-20 range.

99% of respondents said they had suffered **at least one breach**

98% are **planning budget increases** for cybersecurity and supply chain risk



Annual reporting to senior management was **more common in Europe than elsewhere**.

28% vs. 18%

reporting was a more common response

European respondents had the **highest percentage (56%) expecting budget increases** from 51-100%, compared to 42% overall.

56%

highest percentage of budget increases

Europe had a **larger percentage of respondents** reporting only one breach: 26% for Europe versus 19% global.

26% EUROPE

19% OVERALL

reporting only one breach

Europe had a **notably high percentage of respondents** reporting that they had no way of knowing if an issue arises (46% vs. 38% globally).

46% EUROPE

United Kingdom

According to most metrics, the UK is the market that is slowest to prioritize cybersecurity risk. Despite a high prevalence of cyber breaches (97%) and a large number of firms that plan to increase budgets (92%), UK firms are by far the least likely to consider cyber risk a key priority at 27% and the least likely to be aware of any risks in their supply chain at 38%.

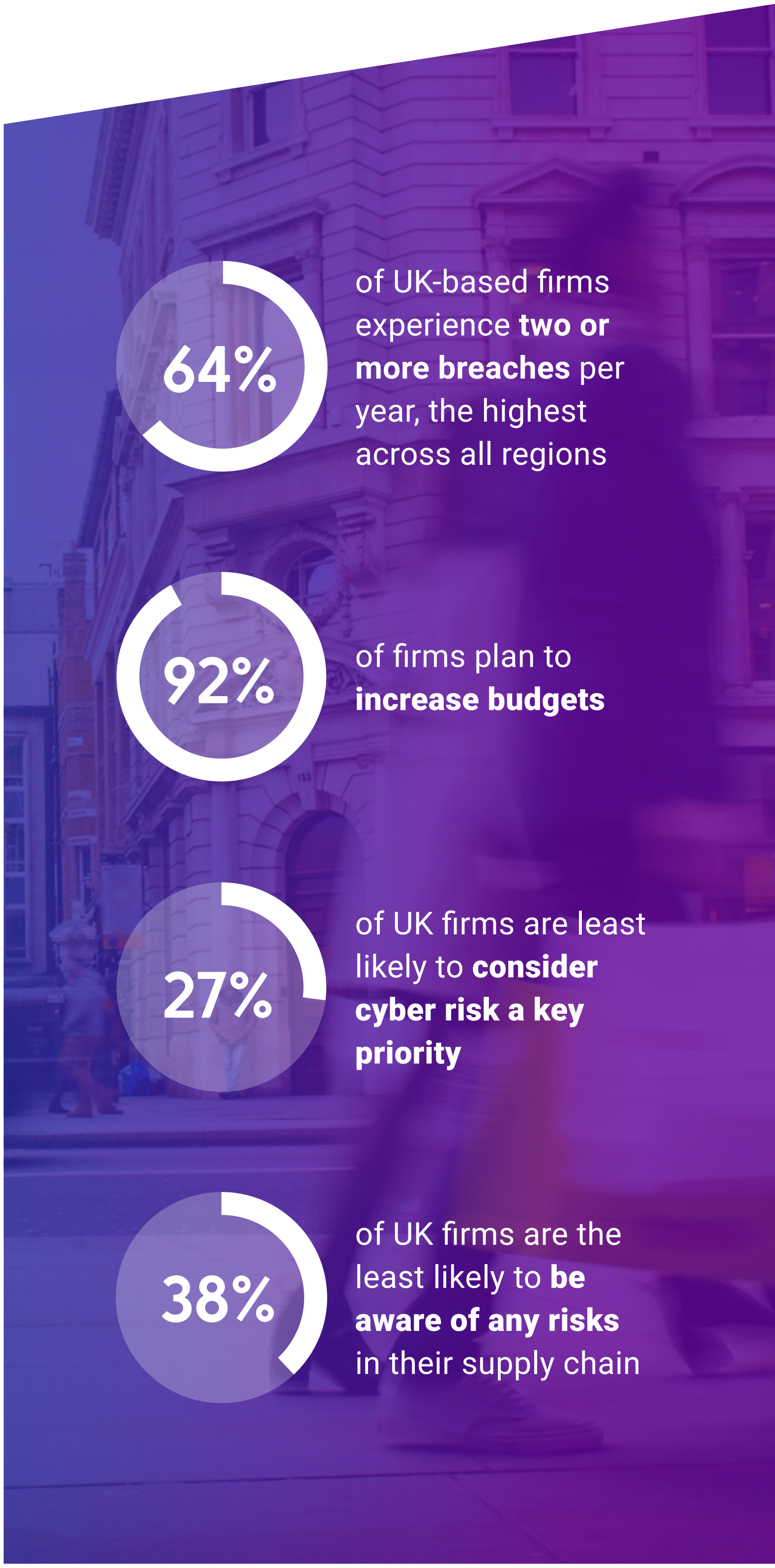
Surprisingly, UK firms report more frequently on supply chain risk, indicating a positive tendency toward regular supply chain auditing that could be more effective if it takes in a more expansive and rigorous awareness of third-party cyber risk.

Variations compared to other countries

The UK had by far the largest percentage of respondents who replied that supply chain/third-party cyber risk was not on their radar - 38% (compared to 22% in North America, 23% in Singapore, and 31% in Europe).

38%

answered that supply chain/third-party cyber risk was not on their radar



64% of UK-based firms experience **two or more breaches** per year, the highest across all regions

92% of firms plan to **increase budgets**

27% of UK firms are least likely to **consider cyber risk a key priority**

38% of UK firms are the least likely to **be aware of any risks** in their supply chain

Use of vendor risk management programs in the UK was **lower than average** (32% vs. 39%).

32% vs. 39%

use of vendor risk management programs

Monthly reporting to senior management was a much more common response in the UK (35%), where annual (10%) and bi-annual reporting (18%) were much less common.

35% UK

reporting was a MORE common response

10% ANNUAL

18% BI-MONTHLY

reporting was LESS common response

Singapore

By nearly every metric, Singaporean respondents prioritized third-party vendor risk the most were the most highly aware of cyber risks and their vendor systems, and the most committed to a structured, strategic approach to securing their networks.

This approach has paid dividends, as fewer businesses in Singapore suffered a breach than in any other region (only 79%, compared to North America at 97%, UK 97%, and Europe at 99%). Most Singaporean firms considered supply chain cybersecurity risk a key priority (56%) and less than a quarter said supply chain risk is not on their radar (23%).

Most Singaporean businesses remain committed to increased budgets (85%) and many do not audit or report to senior management on third-party cyber risk frequently. Forty-six percent say they report every six months or less.

Variations compared to other countries

Overall, 42% answered "supply chain/third-party cybersecurity risk is a key priority for my company," while 56% of Singaporean respondents answered "supply chain/third -party cybersecurity risk is a **key priority for my company."**

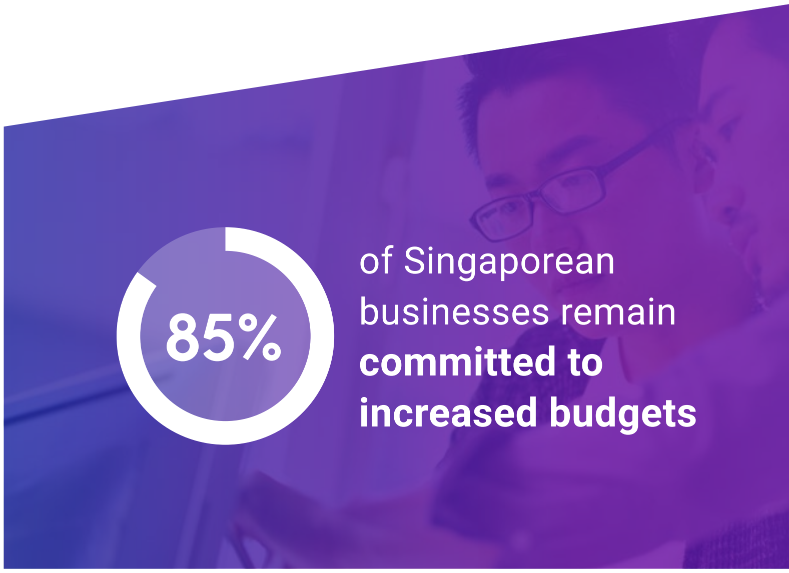
42% overall

answered supply chain/third-party risk is a key priority for my company

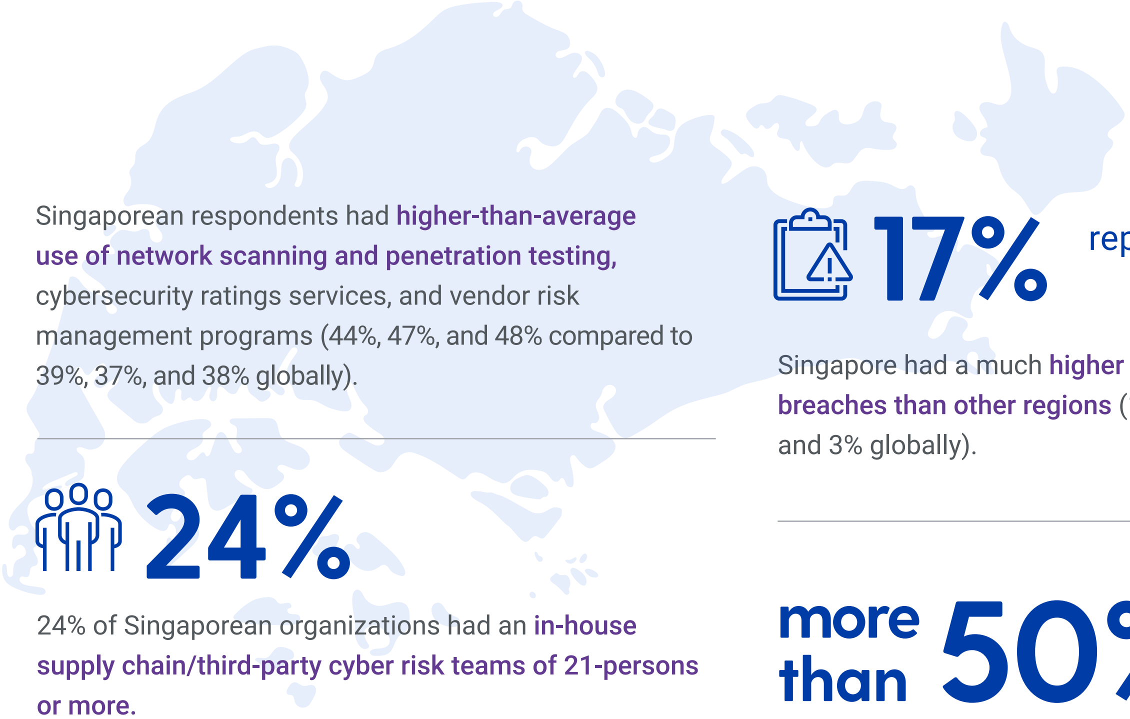
Singapore **showed superior results in regard to monitoring their third-party ecosystem,** with the highest percentage of respondents monitoring all suppliers at 35%. Twenty-five percent monitor critical and top suppliers, 20% only monitor critical, 12% monitor many but not all, and 7% don't monitor any.

35%

highest percentage of respondents monitoring all suppliers



of Singaporean businesses remain **committed to increased budgets**



Singaporean respondents had **higher-than-average use of network scanning and penetration testing,** cybersecurity ratings services, and vendor risk management programs (44%, 47%, and 48% compared to 39%, 37%, and 38% globally).

24%

24% of Singaporean organizations had an **in-house supply chain/third-party cyber risk teams of 21-persons or more.**

25% or less

budget increases

Smaller budget increases seem somewhat **more common in Singapore** - 8% of respondents reported budget increases of 25% or less (in comparison to 3% overall) and 35% reported increases of 26-50% (in comparison to 29% overall).

17% reporting no breaches

Singapore had a much **higher percentage reporting no breaches than other regions** (17% compared to between 1% and 3% globally).

more than 50%

answered that they work with the supplier/third-party every step of the way until the issue is resolved.

Final Thoughts

An aggressive and complex cyber threat landscape, evidenced by some high-profile breach incidents, has clearly prompted a shift in priorities among the 1,200 cybersecurity professionals we surveyed. Companies are more focused on third-party and supply chain cybersecurity risk, and more aware of their vendor ecosystems than in 2020. Despite this, the number of breaches originating in third parties has increased.

As this report shows, the number of companies reporting supply chains of more than 1,000 companies more than doubled from 2020, from **14% overall to 38%**. At the same time, the number of companies reporting 500 vendors or fewer dropped from **40% to 32%**. It seems organizations are beginning to recognize the true scale and interconnected nature of their supply chain.

In this expanded risk environment, cyber risk management **professionals are reporting difficulties across the board**, demonstrating the complexity they face in trying to improve performance. It is encouraging that budget is being committed to tackling the problem but traditional tools and approaches are not effective against sophisticated threat vectors.

14% to 38%

the number of companies reporting supply chains of more than 1,000 companies **more than doubled from 2020**

40% to 32%

the number of companies reporting supply chains of 500 vendors or fewer **dropped from 2020**

The challenge is compounded by the current heterogeneous nature of the tools and strategies organizations have in place to implement third-party risk management. The survey found a mix of approaches with no single approach dominating. Many organizations are evolving toward a data-driven strategy, with supplier risk data and analytics in use by nearly half of respondents.

47%

of organizations think the CIO owns cyber risk

38%

of organizations say it belongs to the CISO

11%

say Chief Procurement Officers are responsible

Executive ownership is also a gray area.

This division over who ultimately owns cyber risk can cause issues around allocation of budget, resources and ultimately an organization'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 organization's overall risk management strategy with clearly defined lines of responsibility, reporting, and budget ownership.

Rapid continuous monitoring and remediation oversight of suppliers is an important addition to existing supplier questionnaire and audit procedures in order to effectively defend against the increased capabilities of adversaries.

To find out more about how BlueVoyant can help you secure your organization against third-party cyber risk visit www.bluevoyant.com

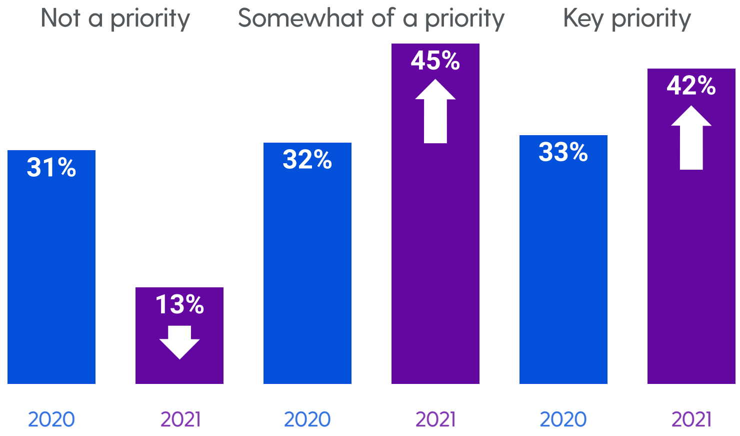
BlueVoyant®

GLOBAL REPORT

Data Appendix

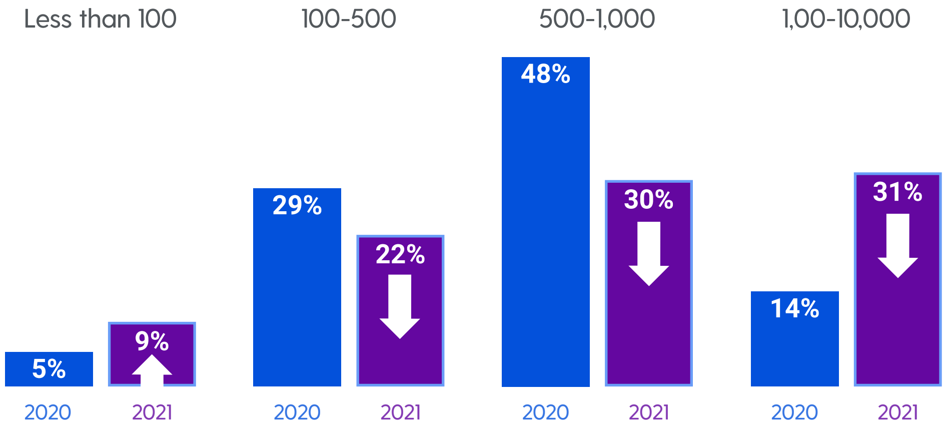
Companies are more focused on risk

Q: Which of the following statements applies to your company's handling of cyber risk and third-party suppliers?



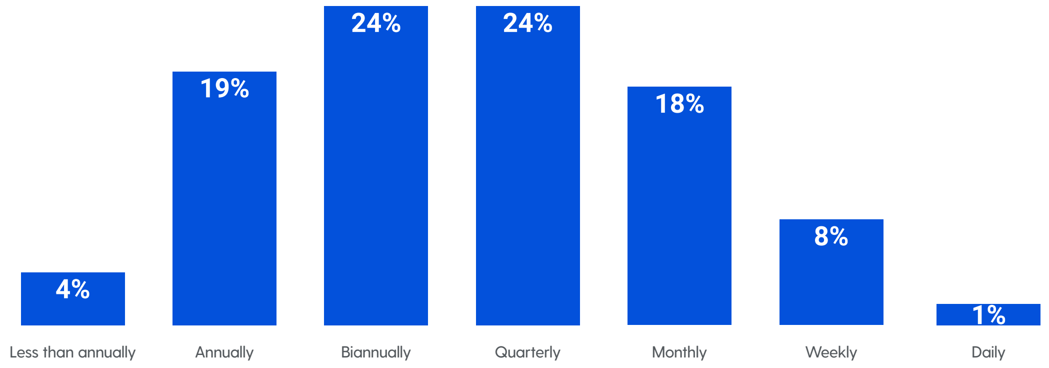
More companies report larger supply chains

Q: How many vendors do you work with?

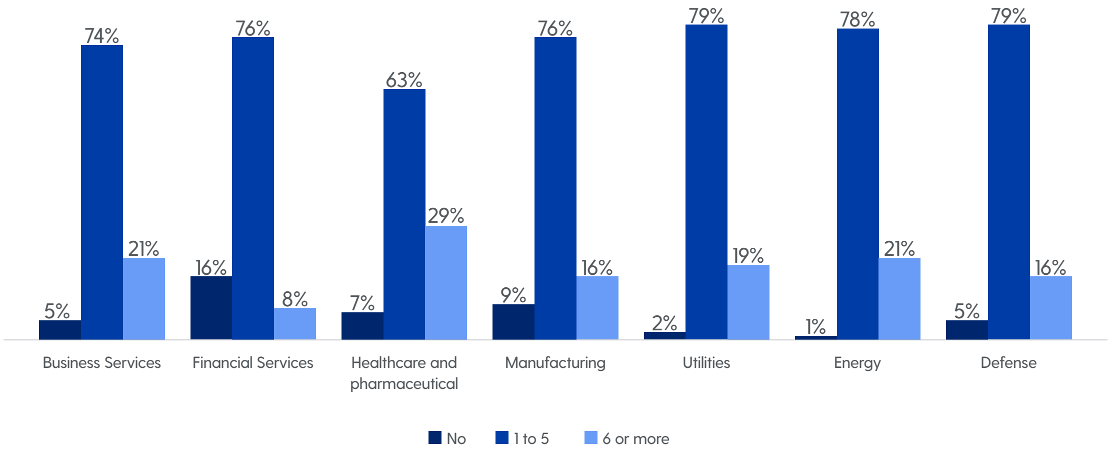


Vendor risk reporting is variable

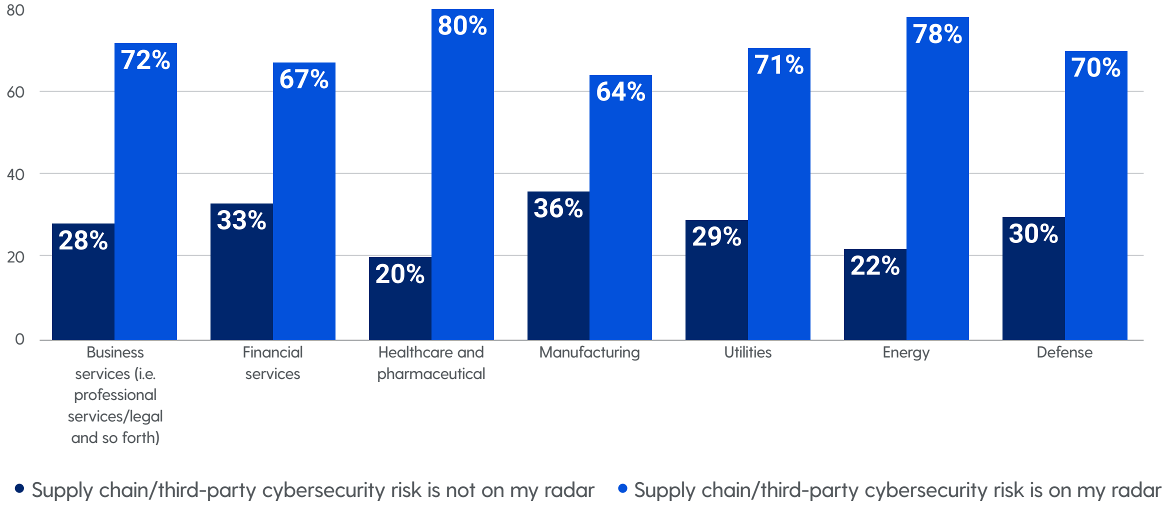
Q: How often is the senior management team briefed on third-party cybersecurity risk?



Q: Have you had any cybersecurity breaches because of weaknesses in your supply chain/third-party cybersecurity risk in the last 12 months? If so, how many?



Q: Which of the following statements apply to your company's handling of cybersecurity risk and third-party suppliers?



Budgets continue to rise

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

	2020	2021	
Yes, increased by up to 25%	3%	3%	91%
Yes, increased by 26-50%	28%	29% (+1%)	
Yes, increased by 51-100%	42%	42%	
Yes, increased by more than 100%	17%	17%	
No, it has stayed the same	5%	5%	8%
Yes, decreased	4%	3% (-1%)	

About BlueVoyant

At BlueVoyant, we recognize that effective cybersecurity 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

BlueVoyant®

To learn more about BlueVoyant, please visit our website at **www.bluevoyant.com** or email us at **contact@bluevoyant.com**