BlueVoyant

BLUEVOYANT REVIEW

Managing Cyber Risk Across the Extended Vendor Ecosystem

2022 Benelux Report
Netherlands, Belgium, and Luxembourg

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

Twelve-hundred chief information officers (CIOs), chief information security officers (CISOs), and chief procurement officers (CPOs) responsible for supply chain and cyber risk management were surveyed from companies employing 1000-plus across a range of industries including: business services, financial services, healthcare and pharmaceutical, manufacturing, utilities and energy, and defence. To gain a global perspective, the research was conducted in the following countries: the United States, Canada, Germany, the Netherlands, the United Kingdom, and Singapore. This was followed by commissioning two further European reports whereby an additional 450 respondents were surveyed across Europe in January 2022, making an overall total of 1,650 respondents. Two-hundred seventy-seven respondents were from Benelux countries – the Netherlands, Belgium, and Luxembourg.

Foreword

In 2020, our "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 the intervening period 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 affected tens of thousands of companies.

Accelerated by the worldwide rise of ransomware activity, cyberattacks 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, according to Roll Call.

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.

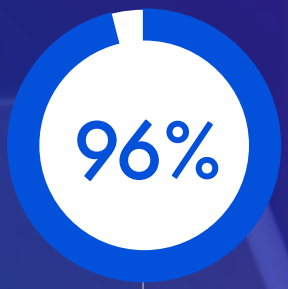
Businesses in all industries across the Netherlands, Belgium, and Luxembourg are investing in cybersecurity. However, some still fail to make cyber risk a strategic priority and to coordinate and formalise their approach to cyber defence and remediation. In addition, companies struggle to assign ownership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

Benelux 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, combined with supply chain shortages, 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 itself.

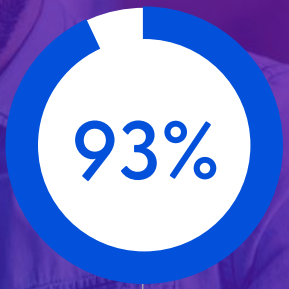
Benelux Findings

At a glance Benelux findings:



96% **have suffered a security breach because of weaknesses in their third-party vendors in the past 12 months**

3.93 **average number of breaches experienced in Benelux in the last 12 months due to weaknesses in supply chain cybersecurity**



93% have been negatively impacted by a cybersecurity breach that occurred in their supply chain

Despite high breach levels, companies in the Netherlands, Belgium, and Luxembourg show an inconsistent approach to supply chain cyber risk management. Awareness, prioritisation, and monitoring of third-party cyber risk are all low.

The Benelux findings paint a stark picture of rising breaches, low vendor visibility and limited awareness of third-party cybersecurity. **Ninety-six percent of Benelux-based firms surveyed said they suffered a direct breach because of weaknesses in third-party cybersecurity in the past year.** This is higher than the overall 93% average of other surveyed countries in 2021.

The average number of breaches originating in the supply chain is high, at 3.93 per organisation. Fifty-two percent of organisations experienced between two and five cybersecurity breaches. **A concerning 27% experienced between six and 10 breaches — far higher than the previous overall average reporting this breach frequency, which was 19% in 2021.**

Compared with counterparts in other territories, **Benelux respondents are more likely to say that third-party cyber risk is not on their radar.** The proportion saying it is not on their radar was 42%, which exceeds the overall average of 29% among surveyed countries in 2021. Only 26% said managing third-party cyber risk was a key priority for their organisation while just 9% said that they monitor all their third-party suppliers for cybersecurity risk.

The number of companies reporting supply chains with between 1,001 – 10,000 was 43%. Simultaneously, the number reporting between 501 – 1,000 vendors was 34%. **The average vendor ecosystem in Benelux now contains 3,781 third parties.**

Rising vendor numbers are exposing a lack of visibility Benelux 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 was 43%.** This is a clear indication of the complexity of the issues Benelux businesses must solve if they are to stem the tide of breaches and control organisational risk.

2021

43%

had no way of knowing if an issue arises with a third-party/ supply chain's cybersecurity.

Benelux Vendor Monitoring Frequency

However, do Benelux companies recognise vendor visibility shortcomings? **Seven out of 10 (70%) Benelux businesses only monitor their vendors quarterly or less frequently.** In terms of weekly monitoring, only 9% did so; 19.5% check monthly; while 2% or less assess on a daily basis or in real time.

In contrast, only 18% assessing suppliers do so six monthly, while 21% assess annually or less frequently.

When it comes to briefing senior teams on the outcomes of third-party cybersecurity risk monitoring, Benelux was slightly ahead of the overall average of countries surveyed last year. **Twenty percent brief senior teams monthly, compared to the previous overall average of 18% in 2021, while 12% of Benelux respondents say they brief weekly and 3% brief daily.**

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

60%

Said these breaches are likely to lead to an increase in budget for additional **internal resources** to help protect against supply chain cybersecurity issues.

33%

Said these breaches are likely to lead to an increase in budget for additional **external resources** to help protect against supply chain cybersecurity issues.

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

In 2021, third-party cyberattacks were in the headlines, and as more attack details become clearer there becomes a greater need for rapid response.

Many of the most damaging third-party cyberattacks in 2021 occurred in the immediate aftermath of new vulnerabilities discovery. Without frequent – deally continuous – monitoring, cyberattacks like this can go unrecorded and unseen for weeks and months.

9%

However, only 9% of Benelux companies are assessing third-party cyber risk weekly

and the number undertaking daily, or real-time monitoring, is incredibly low at 2% and 1%, respectively. That leaves a high-risk window in which threats go undetected.

BlueVoyant Viewpoint

Third-party cyber risk can only become a strategic priority through clear and frequent briefings to the senior executive team and the board. However, these briefings and the data that informs them can **only be effective if there is an established third-party risk awareness culture within the organisation.**

With 42% of Benelux respondents saying that third-party risk is not on their radar, and 43% admitting they have no way of knowing if a cybersecurity issue arises with a vendor, BlueVoyant can help your team understand the risks or help your team raise cultural awareness around this issue.

Budget for third-party cybersecurity risk management has increased, but spending may lack strategic focus.

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

45%

of Benelux organisations said budgets were rising by between 51-100%.

16%

a further 16% reported increases of more than 100%. Only 11% reported static or falling budgets.

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.

Tellingly, Benelux firms are most concerned about the challenge of understanding how to penalise third parties when they don't respond or remediate issues. They also report concern around a lack of in-house resources to manage the program. Likewise onboarding new third parties with the speed and rigour was also cited as the third-highest challenge.

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

BlueVoyant Viewpoint

Increasing budgets year-on-year are a sign that Benelux companies are taking cybersecuriity and vendor risk management seriously. Additionally, 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.

Benelux companies utilise vendor risk management and integrated enterprise risk management programmes.

More than 36% of Benelux companies are using vendor risk management programmes and 34% rely on integrated enterprise risk management programs. Nearly 25% of Benelux organisations use on-site audits to manage third-party cyber risk. About a quarter use questionnaires, compared to an overall average of 27% among 2021 research participants.

23%

of Benelux businesses used external consultants

correlating with the findings that they rely heavily on outsourced teams; on average, organisations outsource to teams with more than 11 employees, while internal cyber risk teams are of a similar size.

While they may not lack headcount, Benelux firms are failing to reap automation benefits that can help lift the administrative burden of regular risk monitoring. Only 36.5% have vendor risk management programmes in place, compared to the overall 39% average of those countries surveyed last year.

BlueVoyant Viewpoint

The split of tools and programmes in use points to a **less mature approach among Benelux 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.

Similarly, only 34% have an integrated/enterprise risk management programme in place, while across the six countries surveyed last year the average figure was 36%, indicating Benelux firms in general lack an overall strategic approach to cyber risk management.

High-profile breaches are influencing senior decision-makers in Benelux firms.

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

60%

say they are likely to lead to budget increases for internal resources to protect against supply chain cybersecurity issues.

33%

think they will get an increased budget to invest in external resources.

As previously discussed, the reputational damage caused by breaches of this type is forcing Benelux senior leaders to pay attention — with 42% saying board scrutiny has increased as a result.

Nevertheless, Benelux firms don't need to look at the headlines to feel the impact of third-party cyber breaches. Ninety-six percent of them have suffered a direct breach due to a weakness in their supply chain, and 93% have experienced indirect negative impact when a breach has occurred within their supplier ecosystem. The rising frequency of breaches and their impact should be driving businesses to action.

BlueVoyant Viewpoint

Benelux organisations have been prioritising internal network risks, potentially because of a historic shortfall in this area. However, they 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.

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 30% of Benelux respondents, the CISO has ownership of third-party cyber risk. While 28% said it was the CIO, for 14% it is the CPO, with the remaining respondents saying other executives. This lack of clarity means there is considerable variation in the way different organisations approach the cybersecurity risk issue. 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 are 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 budget allocation, 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.

30%

of organisations think the CIO owns cyber risk

28%

of organisations say it belongs to the CISO

14%

say CPOs are responsible

Recommendations

Decide who owns third-party cyber risk

Respondents globally gave mixed answers to third-party cyber risk ownership — between CIOs, CISOs, CFOs, and 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 cyberattacks 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 swift action against newly discovered critical vulnerabilities** needs to become essential in 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 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.

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: *In January 2022 an addendum to the 2021 survey was carried out by Opinion Matters on behalf of BlueVoyant with a sample of 450 18+ CTOs/CSOs/COOs/CIOs/CISOs/CPOs responsible for supply chain & cyber risk management in Poland, Hungary, Czech Republic, Belgium, Luxembourg, and Switzerland working in companies employing 1,000-plus employees from the following industry sectors: Financial services, Healthcare & pharmaceutical, Utilities & Energy (combined: equal split), Business services and Manufacturing & Defence.*

The 2021 survey was 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 U.S., Canada, Germany, the Netherlands, U.K., and Singapore, working in companies employing 1,000-plus 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.

The 2020 survey carried out by Opinion Matters on behalf of BlueVoyant with a sample of 1505 18+ CIOs/CISOs/CPOs responsible for supply chain & cyber risk management working in companies employing 1,000-plus employees in the U.S., U.K., Switzerland, Mexico and Singapore. Opinion Matters abides by and employs members of the Market Research Society, which is based on the ESOMAR principles.

About BlueVoyant

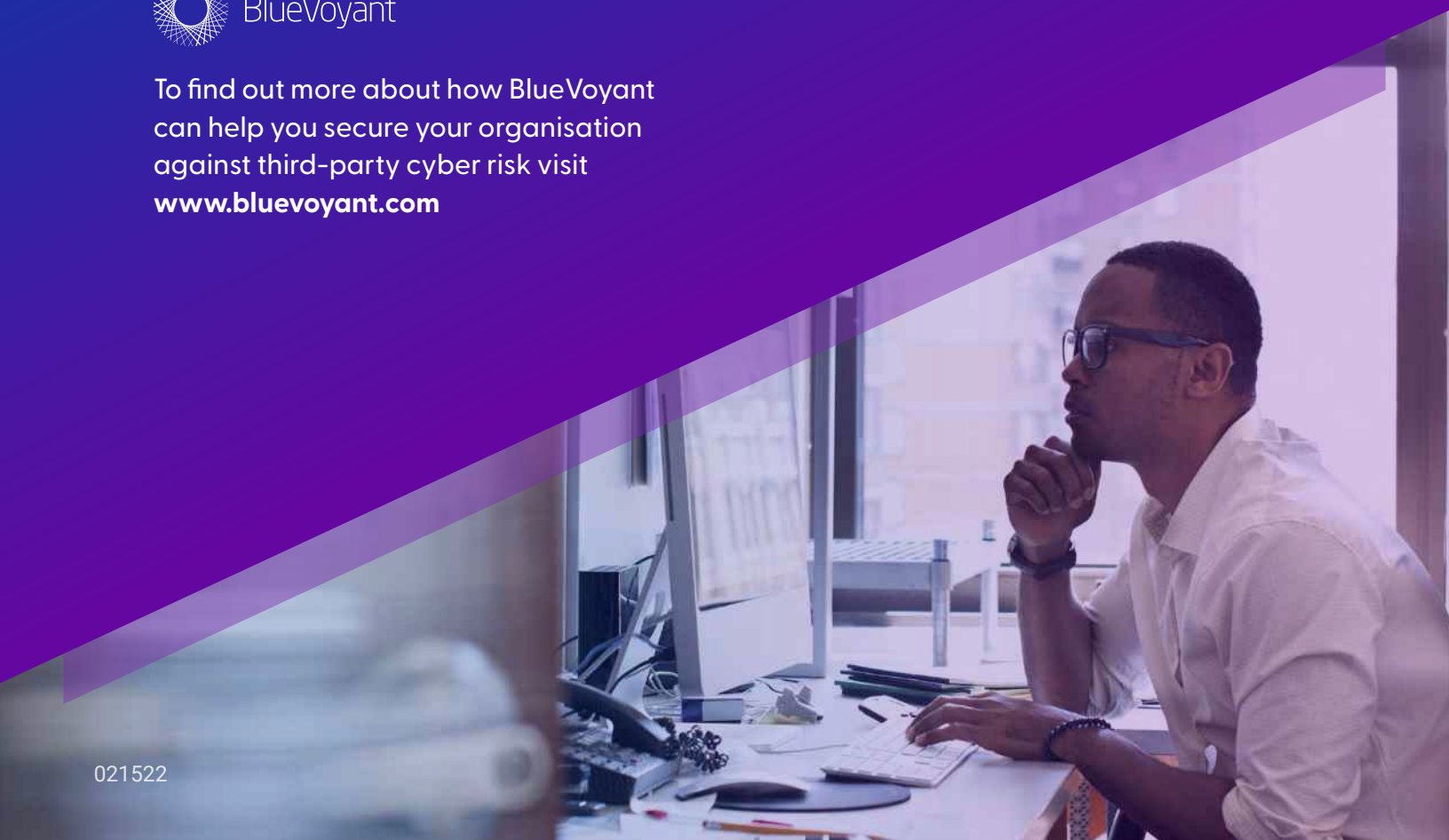
At BlueVoyant, we recognize that effective cybersecurity requires active prevention and defense across both your organisation and supply chain. Our proprietary data, analytics, and technology, coupled with deep expertise, work as a force multiplier to secure your full ecosystem.

Accuracy. Actionability. Timeliness. Scalability.

Founded in 2017 by former Fortune 500 and former government cyber officials, BlueVoyant is headquartered in New York City and has personnel in Washington, D.C., Maryland, San Francisco, Israel, Philippines, Canada, U.K., Spain, Australia, Hungary, Czech Republic, Romania, Slovakia, Netherlands, Belgium, Germany, Sweden, Denmark, El Salvador, Colombia, Mexico, and Panama. Visit www.bluevoyant.com.

BlueVoyant®

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



021522