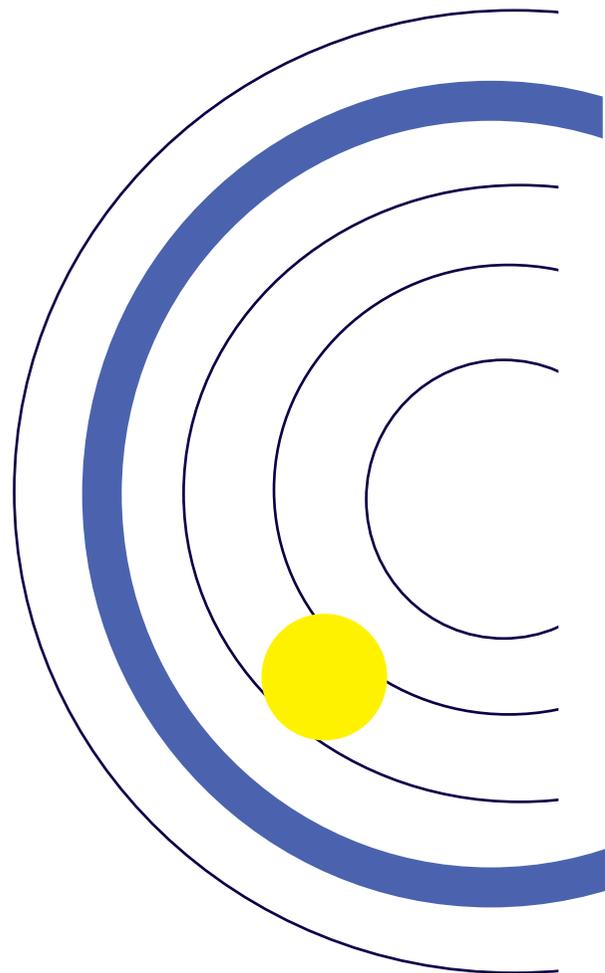


GLOBAL INSIGHTS: SUPPLY CHAIN CYBER RISK



**MANAGING CYBER RISK
ACROSS THE EXTENDED
VENDOR ECOSYSTEM**

- Methodology
- Foreword
- At a Glance
- Key Findings
- Recommendations
- Full Survey
- Contact Us



Report Survey Methodology

BlueVoyant commissioned its first annual survey undertaken by independent research organization, Opinion Matters, in June 2020. 301 USA 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: USA, United Kingdom, 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 organizations 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 organization – can quickly spread with devastating consequences.

The result is that organizations 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 defenses and drive risk out of partner networks.

We asked more than 1500 CIOs, CISOs and CPOs across five countries to share their approach to managing third-party vendor cyber risk; 301 respondents were from the USA. We explored 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 operationalizing their cyber risk management program 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 operationalizing third-party vendor cyber risk management.

At a
Glance

Findings

01





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



92%

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



3.1

Average number of breaches experienced in the past 12 months



69%

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

- Methodology
- Foreword
- At a Glance
- Key Findings
- Recommendations
- Full Survey
- Contact Us

Key
Survey
Findings

02

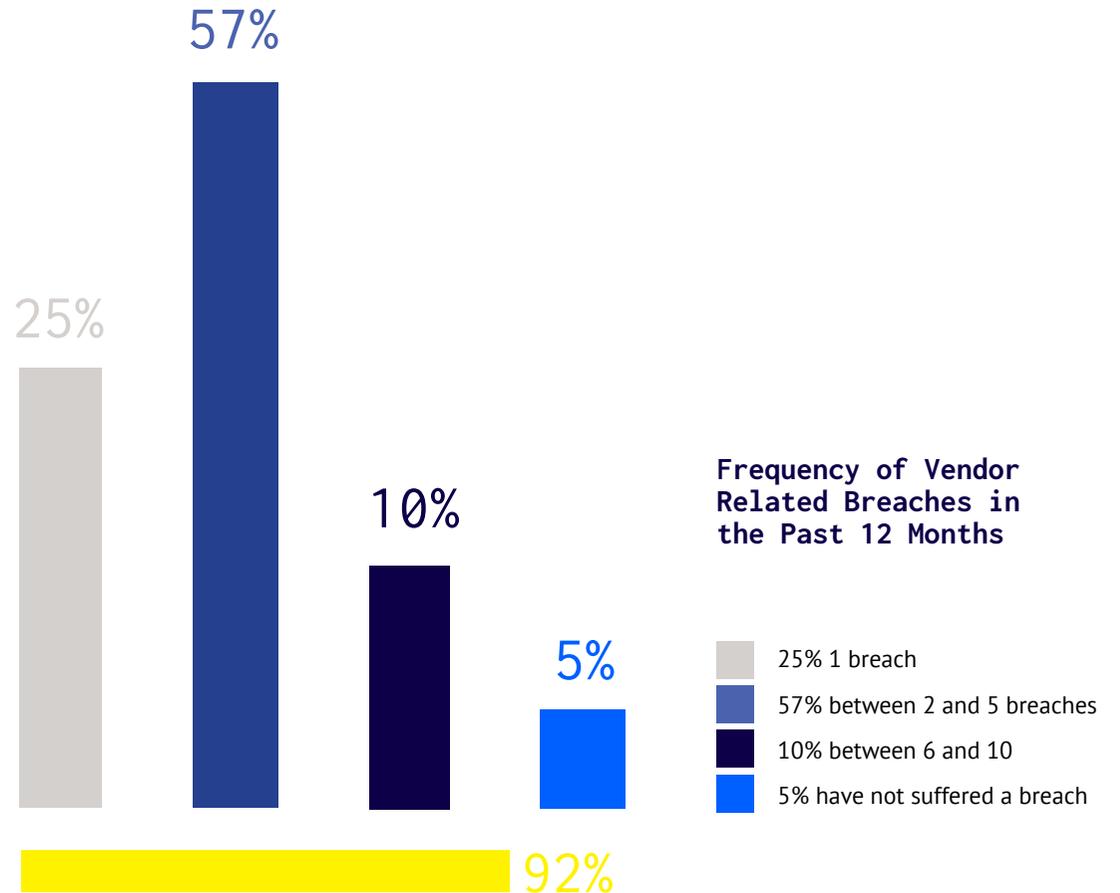


Key Survey Findings

Vendor ecosystems are expansive and vendor-originated breaches are common

The research found that US organizations have a lot of vendors in their supplier ecosystem, an average of 1420. This was the second highest average number of vendors out of the five countries surveyed. These vendors are causing significant cyber risk with 92% saying they have suffered a breach in the last 12 months as a result of weakness in the supply chain. This was the highest number of breaches out of the five countries surveyed. The high number of vendors and high percentage of organizations reporting breaches via the supply chain is proof that monitoring the extended supply chain is a large and growing challenge for US organizations.

Overall, **92%** have suffered one or more breaches in the past 12 months



33%
of respondents said they had no way of knowing if a risk emerged in a third-party

- Methodology
- Foreword
- At a Glance
- Key Findings
- Recommendations
- Full Survey
- Contact Us

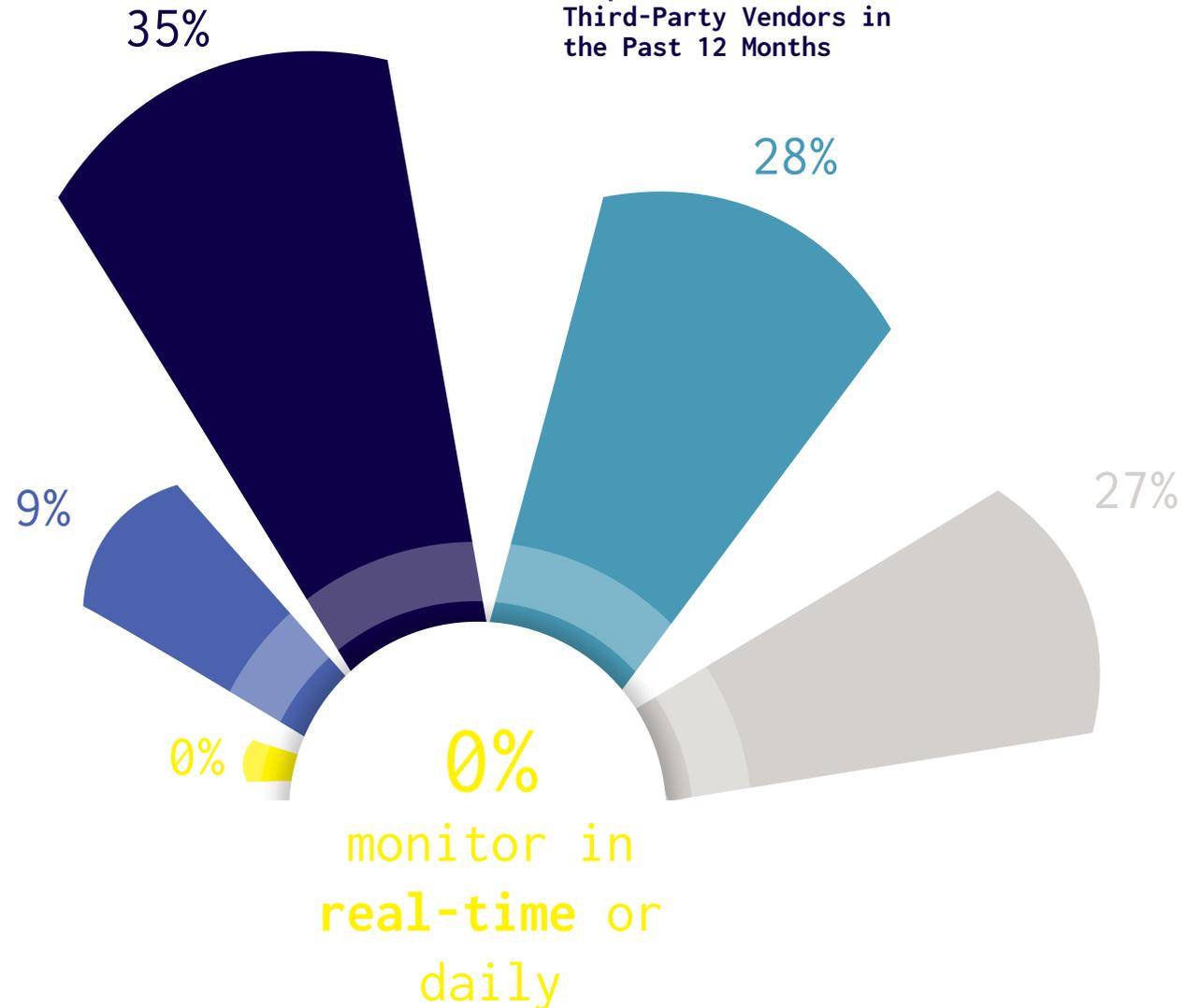
Vendor risk visibility and continuous monitoring is concerningly low

The scale of third-party vendor ecosystems is causing difficulties across the board, with evidence that limited resources are forcing organizations to compromise on the scope of their monitoring program. Only just under one third (31%) said they monitor all vendors, leaving 69% without full visibility. 19% said they monitor only critical vendors while 16% 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.

Over a quarter (27%) 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 third (35%) are re-assessing and reporting monthly. A further 28% are doing this quarterly. Just 9% are succeeding in re-assessing third-party cyber risk weekly. This severely limits their ability to respond to emerging threats and can lead to serious negative findings when audits take place, due to the extent to which threats have matured by the time they are identified.



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



Patchwork of approaches creates operational drag

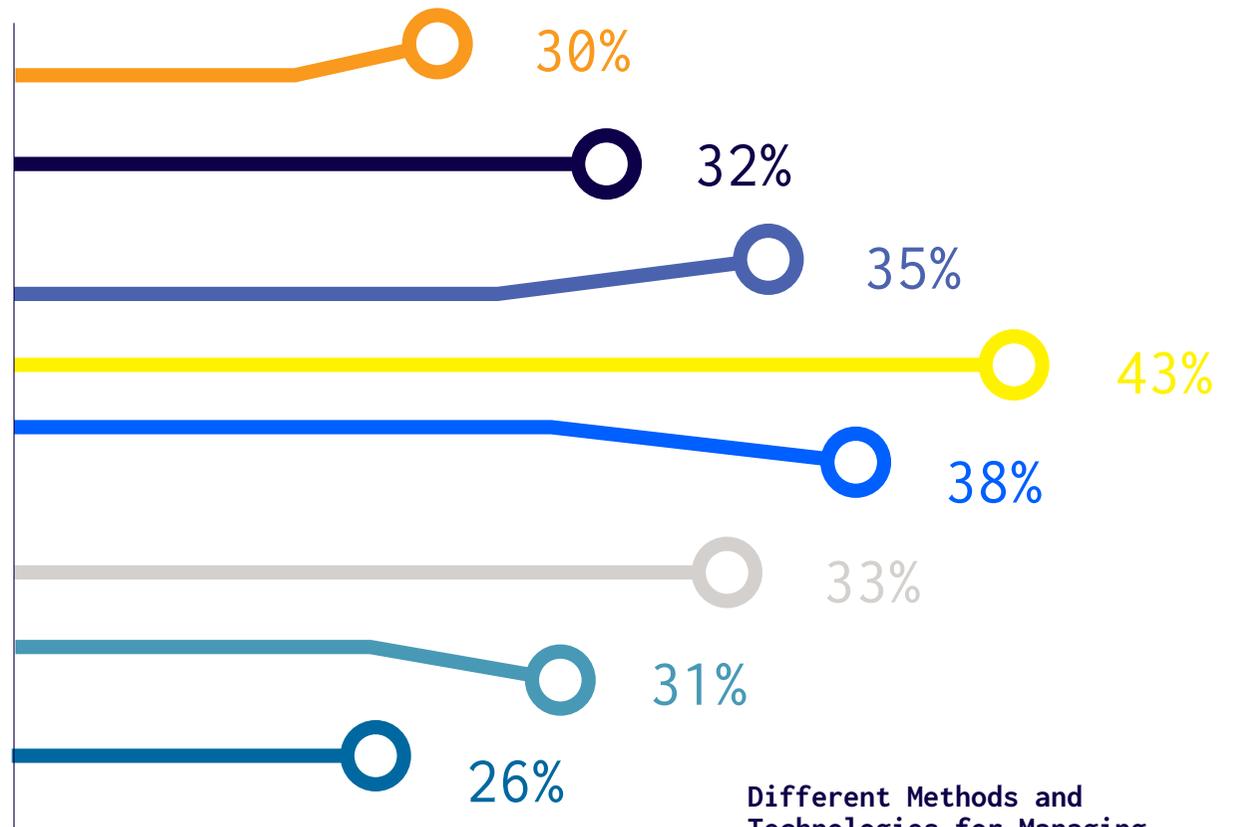
This lag in risk discovery was also evident when we asked about the tools in place to implement third-party risk management; we found a mix of approaches with no single strategy dominating. Many organizations are evolving towards a data-driven strategy, with supplier risk data and analytics in use by 43%. However static, point-in-time tactics, such as on-site audits and supplier questionnaires remain common.

The multiple approaches used by organizations also presents a management challenge when it comes to integrating, analyzing and prioritizing all the data.

- 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

43% use supplier risk data and analytics



Different Methods and Technologies for Managing Third-Party Cyber Risk

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 organizations are ramping up investment to tackle the issue. 86% of US respondents said their budget for third-party cyber risk management has increased compared to the past twelve months. These budget increases will likely be partially allocated to headcount: US respondents said they had an average of 10.8 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, US companies will not be able to stem the tide of third-party vendor 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 programs and how difficult it therefore is to choose a single area to work on. The most common response was handling the challenges of working with vendors to improve security performance (23%). Overall, given the choice of 13 possible pain points, no single issue stood out, indicating the diversity of fronts on which programs are causing problems. This shows that there is a very long way to go before organizations can be confident that they have an effective, comprehensive third-party cyber risk management program in place.



86%

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



10.8

Average people in their own in-house teams

40% take a hands-off approach when they find a vendor problem

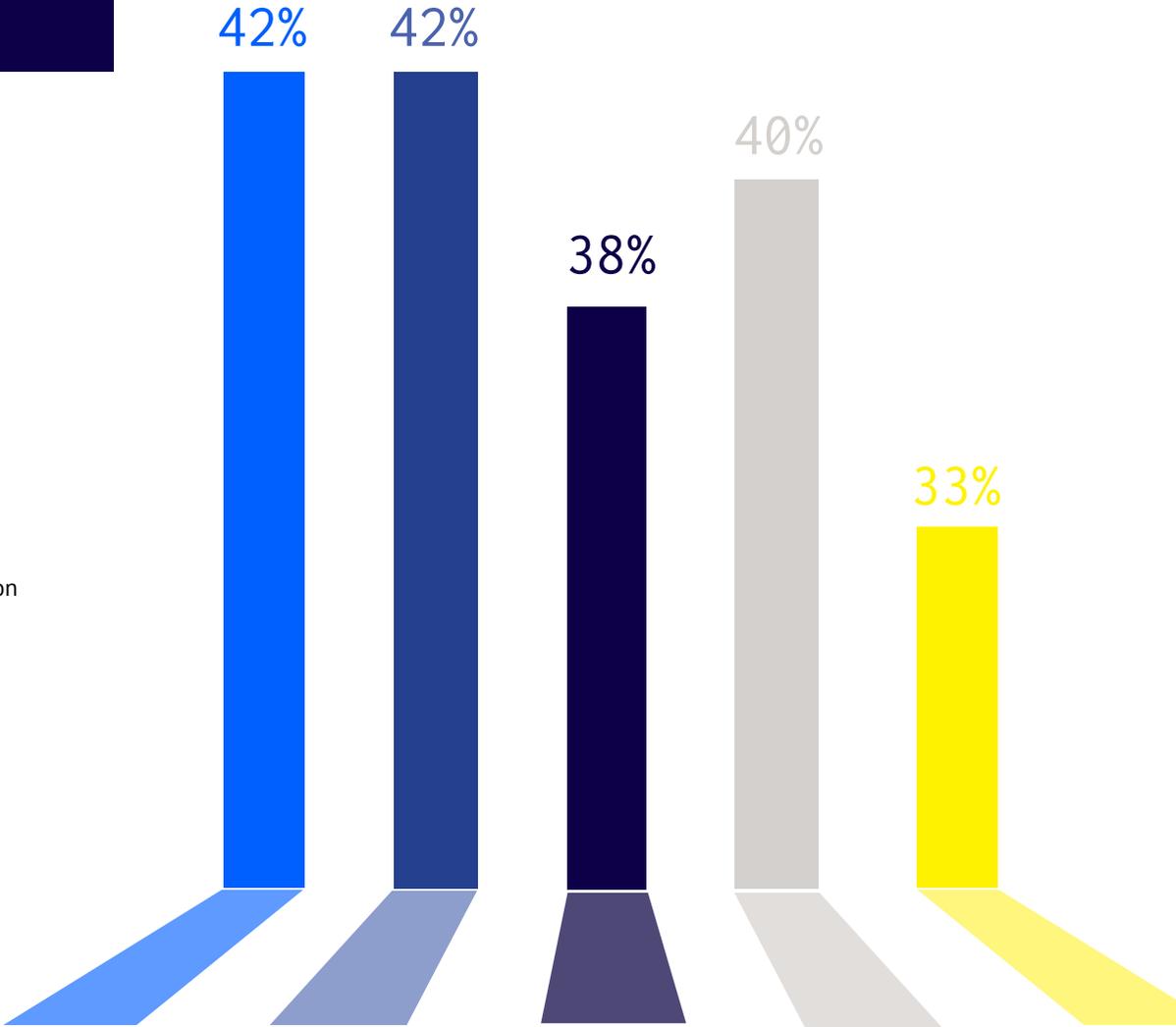
Organizations are not always upfront with suppliers when they do discover a problem. 40% inform the supplier and hope they fix the issue, while 38% rely on the supplier to ensure adequate security. This lack of control and proactivity when it comes to protecting the business is a matter of concern, but likely derives from the pressure under which teams operate.

33% have no way of knowing if an issue arises

How Do Supplier Problems Get Handled?

- identify problems with third-party and help them find a solution
- work with the supplier every step of the way
- rely on third-party vendor to ensure adequate security
- inform the supplier and hope they fix it
- have no way of knowing if an issue arises

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 organizations plan investment, but the scale and scope of the challenge seems to be leading many organizations 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 organizations struggling to work out what is important and unable to manage suppliers proactively in order to prioritize 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 program.



“

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 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

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 organization'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 operationalizing the data that you already collect

so you gain better insight and maximize 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 programs

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

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

Prioritize and triage critical risks in the context of their impact on the organization.

Reduce false positive alerts

and remove the “noise”, so in-house teams can focus on analyzing 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 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.

Full
Survey
Findings

03



How many vendors/suppliers do you currently work with?

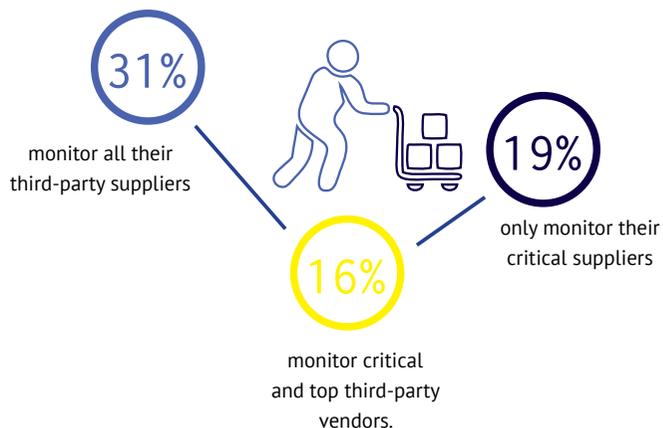
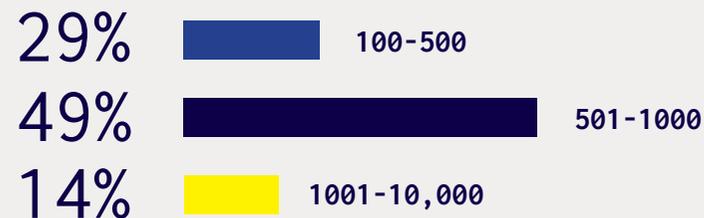
US respondents work with a mean number of vendors of 1420. Typically, bigger companies work with more vendors.

The sector with the highest average number of vendors/suppliers was business services – 1916 followed by manufacturing - 1847. In fact, 26% of manufacturers work with between 1001-10000 vendors.

In terms of job role, the CPO is working with the largest number of suppliers and had the highest average of 1771, yet the CPO does not own third-party cyber risk.



29% of the respondents said they work with 100-500 vendors, while 49% reported that they work with 501-1000 vendors. A staggering 14% 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]

47% of respondents said that handling of cybersecurity risk and third-party suppliers is on their radar. However, 31% said it was not on their radar. 34% of respondents said it is a key priority while 33% said it was somewhat a priority and a sixth (15%) said it was not a priority at all.

31% of respondents said they monitor all their third-party suppliers while 19% admitted they only monitor their critical suppliers and 16% said they monitor critical and top third-party vendors.

The manufacturing sector was most likely (62%) to say third-party cybersecurity risk was a key priority. While the business services sector (52%) was the highest in saying that it was not on their radar. Healthcare (48%) scored highest in monitoring all suppliers.

Out of the three, CPOs were most likely to say third-party cyber risk is both on their radar (62%) and a key priority (47%).

- Methodology
- Foreword
- At a Glance
- Key Findings
- Recommendations
- Full Survey
- Contact Us

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

The highest response was supplier risk data and analytics (43%) followed by the use of external consultants (38%) and in third place 35% of respondents said vendor risk management. Security ratings services was in fifth place with 32%.

The manufacturing sector is using most tools altogether, with supplier data and analytics and vendor risk management jointly top of the list with 52% respectively followed by integrated risk management with 50%. The healthcare & pharmaceutical sector scored highest in using questionnaires (40%). While the financial services sector scored highest in using onsite audits (36%) and the energy sector scored highest for using external consultants (45%) and security ratings (37%).

The CIOs scored highest on onsite audits (32%) and CISOs highest for questionnaires (32%) while CPOs scored highest on security rating services (38%).

32%

Over a quarter of US respondents (26%) still use onsite audits and 30% 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 10.8. This rises to 12.7 in the business services sector.

The average outsourced team size is 10.7. This rises to 11.7 in the business services 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?

Over one third (35%) of US respondents are auditing and reporting monthly. A further 28% are auditing quarterly and 27% are auditing either annually or six-monthly. Just 9% audit and report weekly.

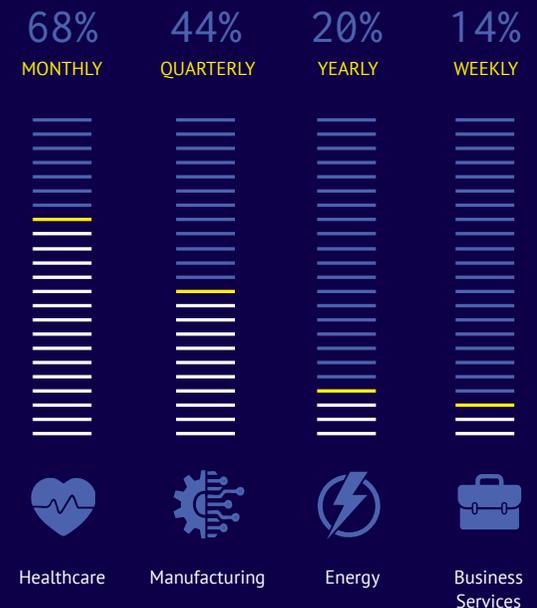
Healthcare & pharmaceutical (68%) are most likely to be re-assessing/reporting monthly. Manufacturing scored highest on reporting quarterly (44%), that said over a quarter (26%) said they were only re-assessing third-party cyber risk every six months. One fifth (20%) of energy respondents only audit once a year while 26% of manufacturing respondents audit only every six months. Business services was the highest sector to be looking at this on a weekly basis (14%).

CPOs scored highest out of the three to be auditing on an annual basis (19%), while CIOs were more likely to be looking at this on a quarterly basis (40%) and CISOs on a monthly basis (40%).



How frequently do you re-assess?

Vertical markets that scored highest in each category



- Methodology
- Foreword
- At a Glance
- Key Findings
- Recommendations
- Full Survey
- Contact Us

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. 86% of US respondents said their budget had increased. 49% have seen increases of between 26-50% and 33% have seen increases of between 51-100%. The average budget increase was 45%.

8% of those in the financial services sector have increased their budgets by more than 100%. Healthcare & pharmaceutical witnessed the biggest percentage increase with an average of 55%.

CIOs had seen the highest average budget increase – 46% - but at the same time 18% of CIOs said their budgets had stayed the same or decreased.

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?

92% of US respondents have suffered a breach because of supply chain/third-party cybersecurity weakness in the past 12 months. 57% have had between 2 and 5 breaches. 10% have had between 6 and 10. The average number of breaches for US respondents was 3.1.

Business services suffered most breaches with an average of 3.8. 18% of respondents in the business services sector have experienced between 6 and 10 cybersecurity breaches. Manufacturing has the lowest average at 2.2.

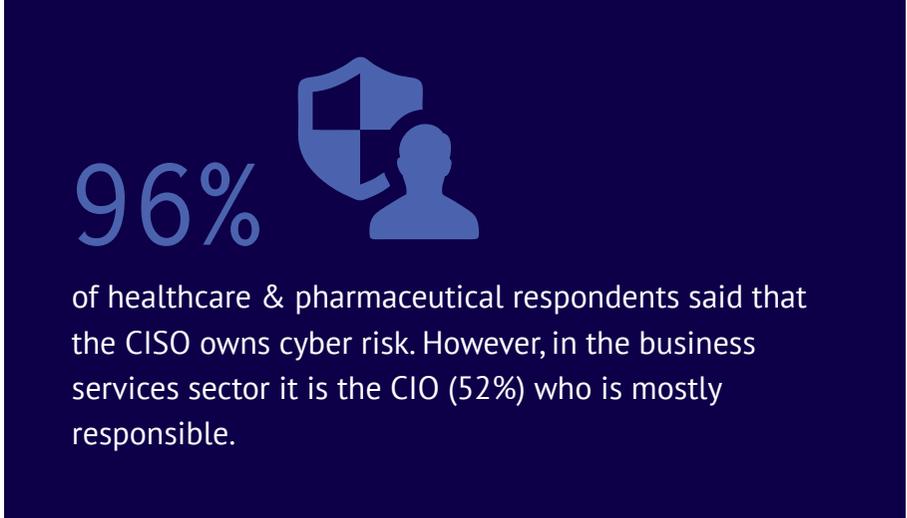
CISOs report more breaches (3.2) than CIOs (3.0) and CPOs (3.1). 62% of CIOs surveyed have had between 2 and 5 cybersecurity breaches.

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

More than half of respondents (54%) said the CISO owns cyber risk, while 27% said the CIO and just 10% said the CPO.

96% of healthcare & pharmaceutical respondents said that the CISO owns cyber risk. However, in the business services sector it is the CIO (52%) who is mostly responsible.

Interestingly, if you're a CIO you're more likely to say it's the CIO who has responsibility (64%) while 75% of CISOs say it is they who have responsibility! 49% of CPOs say cyber risk is their responsibility.



If you find a problem with regard to your third-party/supply chain cyber security how you go about remediation? [tick all that apply]

42% 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 half - 56% - in the business services sector). 42% work with the supplier every step of way until the issue is rectified. However, 40% inform the supplier and hope they fix it while 38% rely on the third-party supplier to ensure adequate security.

One third (33%) admitted to having no way of knowing if any issues arise with third-party cybersecurity. This rises to 47% in the energy 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: Working with suppliers to improve their security performance (23%), prioritizing which risks are urgent and which are not (22%) and offboarding suppliers with the rigor we onboarded them (20%).



About BlueVoyant

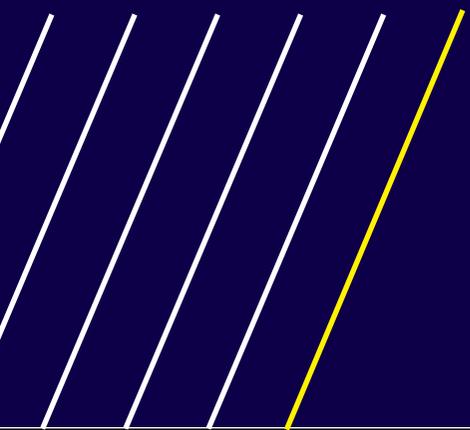
BlueVoyant is an expert-driven cybersecurity services company whose mission is to proactively defend organizations of all sizes against today's constant, sophisticated attackers and advanced threats. Led by CEO Jim Rosenthal, BlueVoyant's highly skilled team includes former government cyber officials 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 utilize 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 organization'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 utilize industry recognised best practices and methodologies, including Standardized 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 Headquarters
335 Madison Ave, Suite 5G
New York, NY 10017

Tel: 646-558-0052 (8-5 EST)
Email: contact@bluevoyant.com
www.bluevoyant.com



DVV Solutions Head Office
Grosvenor House, St. Thomas's Place
Stockport, SK1 3TZ, United Kingdom

Tel: 0044 (0)161 476 8700
Email: enquiries@dvvs.co.uk
www.dvvs.co.uk