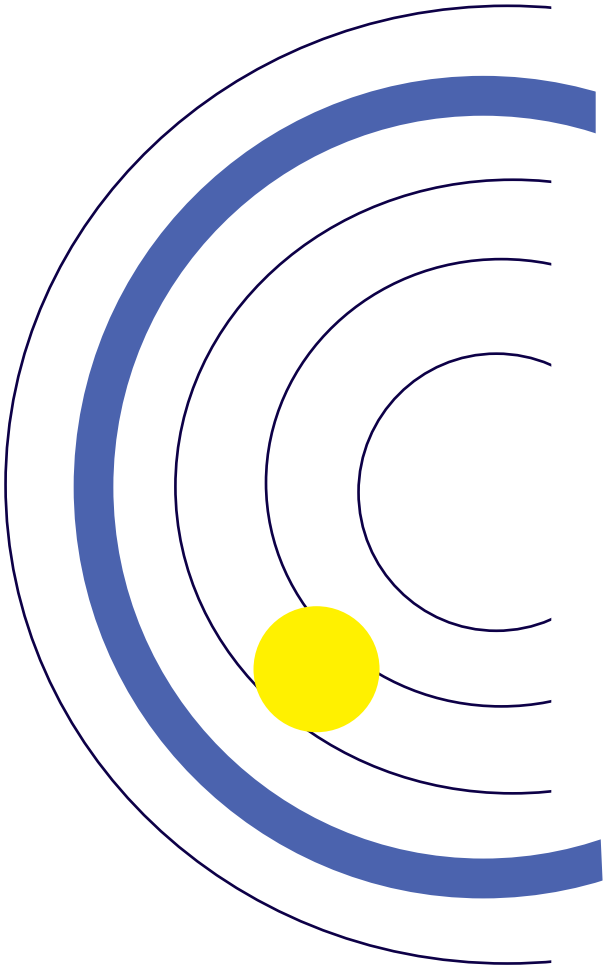
BlueVoyant

GLOBAL REPORT

GLOBAL INSIGHTS:
SUPPLY CHAIN CYBER RISK

MANAGING CYBER RISK ACROSS THE EXTENDED VENDOR ECOSYSTEM

Table of **Contents**



Report Survey **Methodology**

BlueVoyant commissioned its first annual survey undertaken by independent research organization, Opinion Matters, in June 2020. 1505 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, 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 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.

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.

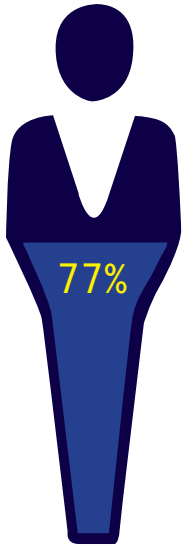
DEBORA PLUNKETT, BlueVoyant Board of Directors and former Director of Information Assurance, NSA

80%

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

2.7

Average number of breaches experienced in the past 12 months



77%

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

Key Survey Findings

02

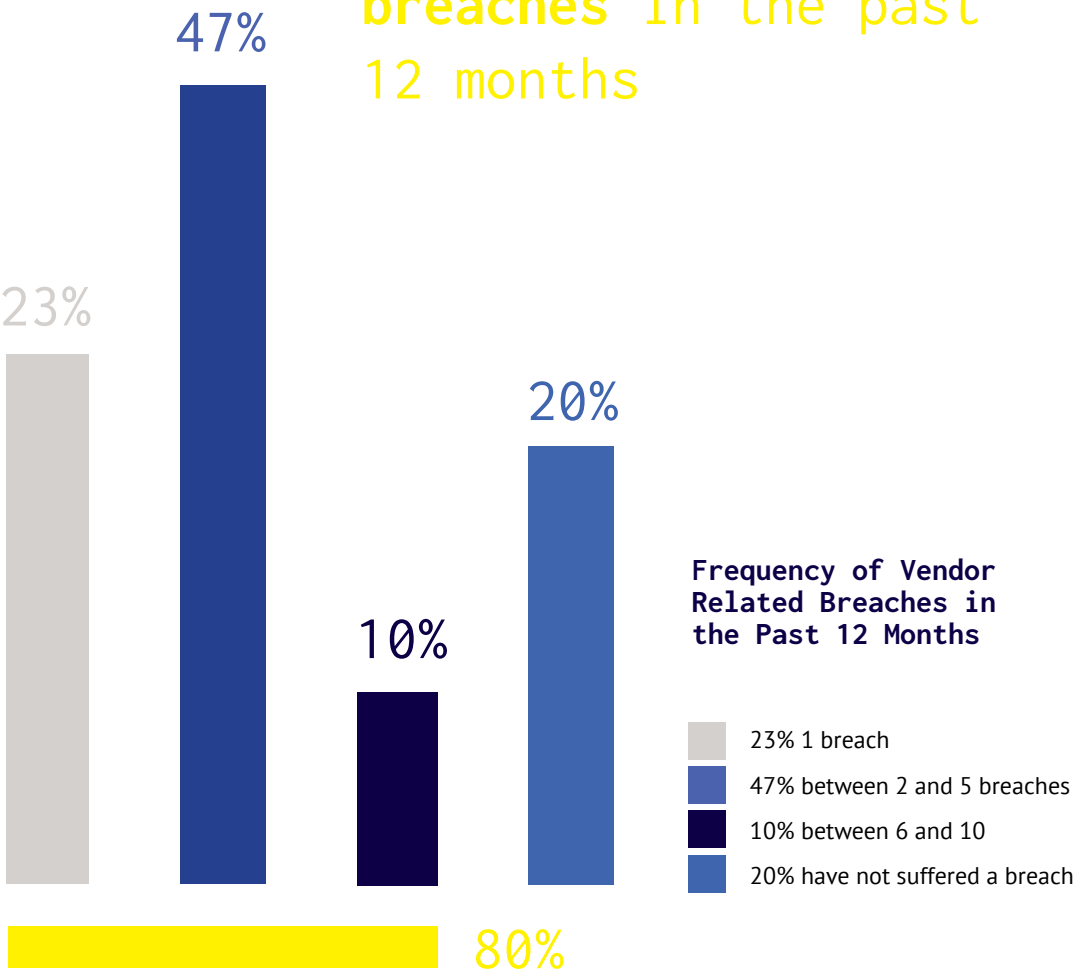
Key Survey Findings

Vendor ecosystems are expansive and vendor-originated breaches are common

The organizations we surveyed work with a high number of vendors. Respondents from all countries apart from Mexico and all sectors except financial services reported that they work with more than 1000 different vendors, giving a sense of the scale of the third-party cyber risk management challenge. The number of respondents who said they had suffered a breach via the supply chain was sobering: overall 80% had been victims of a breach originating in their partner network in the past 12 months; most had suffered at least two breaches and one in ten had suffered more than six.

> BlueVoyant Viewpoint: In a regulatory environment that is increasingly complex and punitive and where financial, operational and reputational impacts of breaches are severe, this rate of vendor-originated breach frequency demands urgent attention at senior levels.

Overall, **80%** have suffered one or more **breaches** in the past 12 months



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 programs.

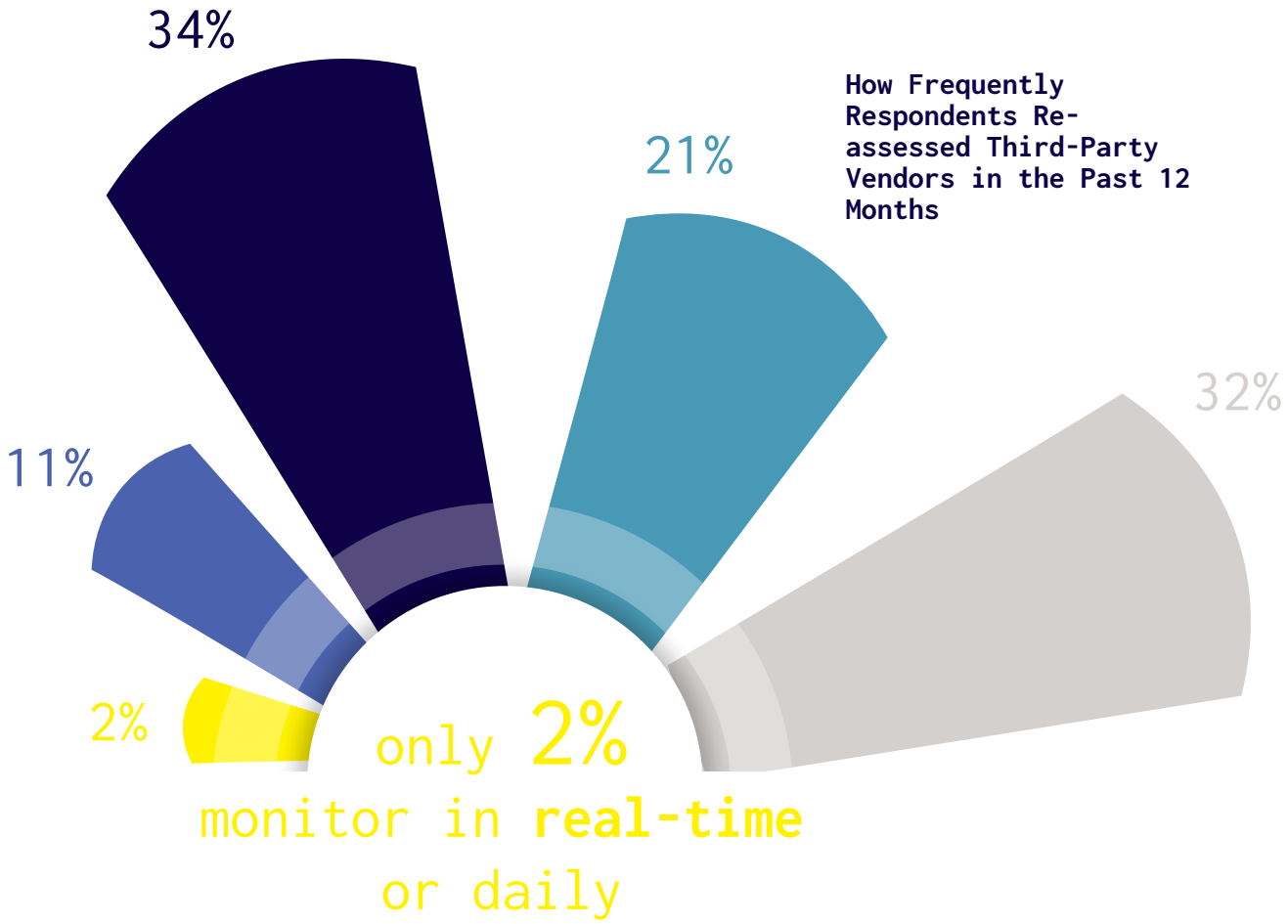
This risk is compounded by the relative infrequency of third-party cyber risk assessment and reporting compared to the fast-changing cyber threat landscape. Real-time or daily monitoring is rare – just 2% of respondents are managing to achieve this.

Almost one third (32%) only assess and report six-monthly or less frequently meaning they spend at least half a year with no insight into the changing risk in their supply chain. 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.

The longest lags in auditing and reporting were seen in the manufacturing and utilities sectors. Ironically, these are industries with long experience of managing complex supply chains, but it seems they may be failing to adapt to the real-time nature of cyber risk.

- 2% monitor in real-time or daily
- 11% weekly
- 34% monthly
- 21% quarterly
- 32% six-monthly or less frequently

BlueVoyant Viewpoint: Taken together, these findings illustrate a striking lack of situational awareness when it comes to third-party cyber risks associated with vendors. If almost one third have no way of knowing when risk emerges, and only one fifth are monitoring all vendors, that leaves a majority who have no visibility over their vendor ecosystem or – if they do – it comes with a significant time lag.



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 40%. However static, point-in-time tactics, such as on-site audits and supplier questionnaires remain common.

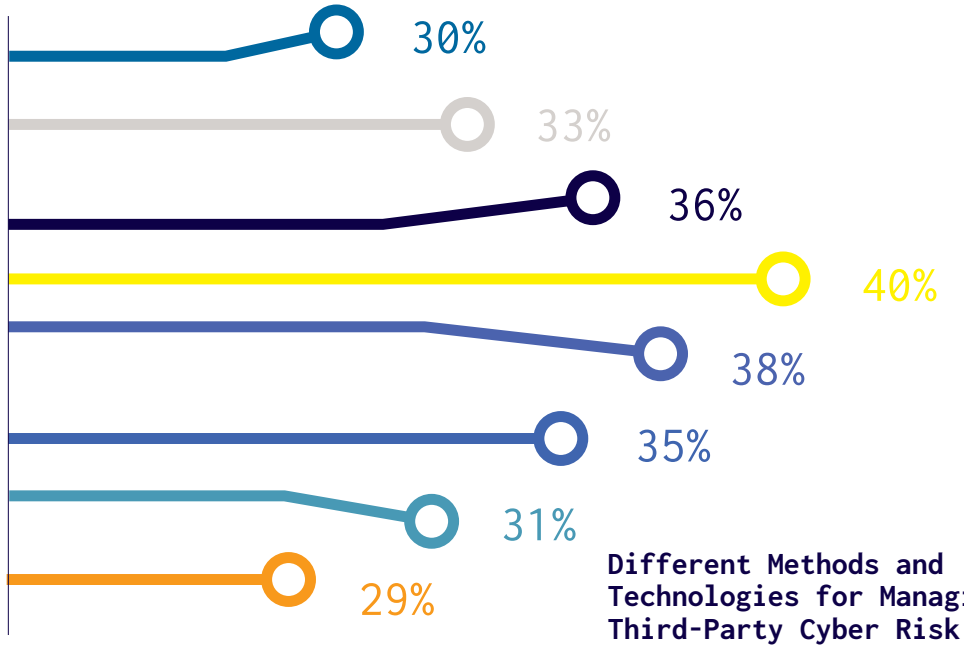
The multiple approaches used by organizations also presents a management challenge when it comes to integrating, analyzing and prioritizing all the data.

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. 81% of global respondents said their budget for third-party cyber risk management has increased compared to the past twelve months. The percentage increase was 40% on average overall, but varied between countries, with the UK and US committing an additional 45% to the issue while in Singapore the planned increase was lower, at 28%. The financial services industry expects the biggest increase, at 50%. These budget increases will likely be partly allocated to headcount: respondents said they had between 10 and 15 people in their in-house teams, and those that outsourced cyber risk management typically handed it to teams of similar sizes.

40% use **supplier risk** data and analytics

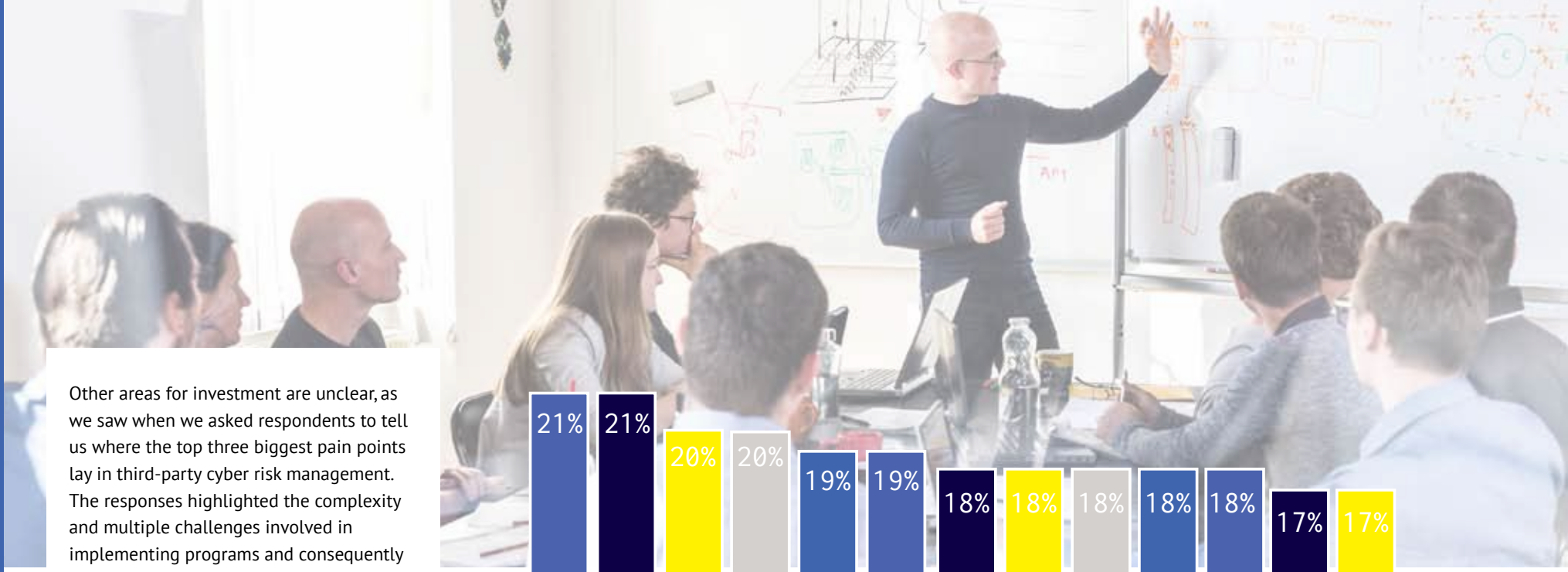
BlueVoyant Viewpoint: Increasing budgets are a positive sign that firms are aiming to move the dial on third-party cyber risk management, but much depends on the business case for increasing those budgets and how organizations plan to allocate resources to operationalize cyber risk management. The broad spread of areas in which firms have concerns about their programs suggests that many may struggle to work out where to start. However, the frequency of cyber breaches is testament to the fact that current approaches are falling short, making investments in operational capabilities that purposefully drive down risk day-by-day an area where concentration of investment would yield the most return.



Different Methods and Technologies for Managing Third-Party Cyber Risk

Respondents could tick more than one answer

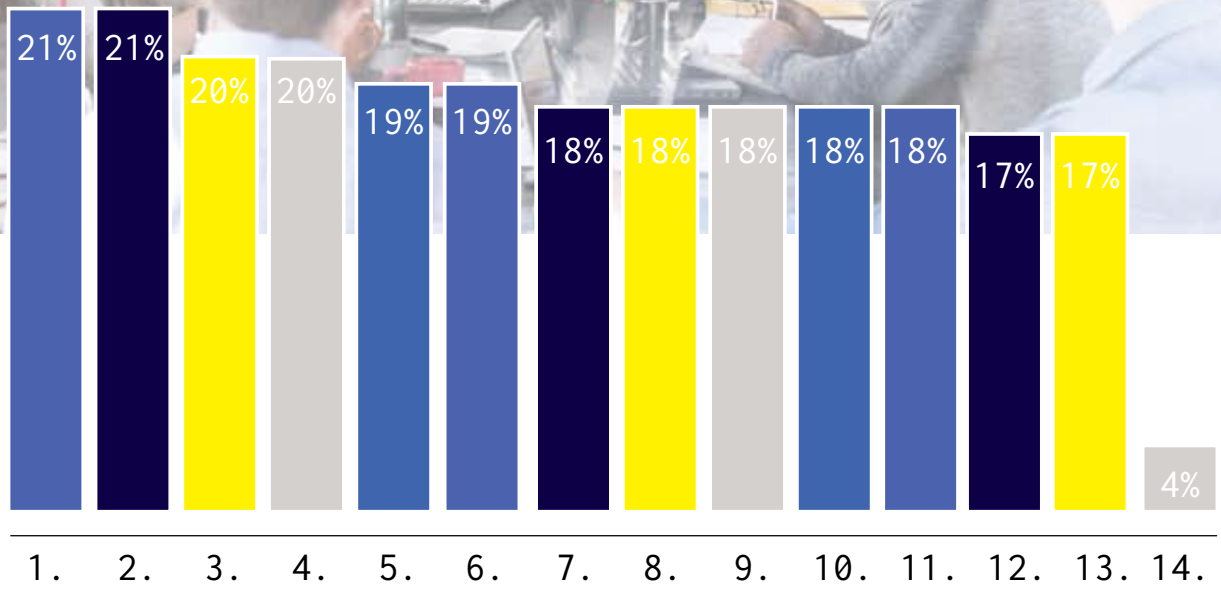
- supplier risk data and analytics
- vendor risk management
- security ratings services
- external consultants
- integrated risk management
- exchanges and marketplaces
- onsite audits
- questionnaires



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 consequently how difficult it is to choose a priority area to work on. The most common pain points were handling the volume of alerts generated by the program and challenges working with vendors to improve security performance (both 21%), but this was closely followed by difficulties prioritizing which risks are urgent and which are not (20%), blind spots where they don't have resources and visibility to spot emerging risk (20%) and too many false positive alerts (19%).

Overall, given the choice of 13 possible pain points, no single issue scored lower than 17%.

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.



Pain Points Experienced with Third-Party Risk Management Programs

1. handling volume of alerts – 21%
2. working with suppliers to improve security – 21%
3. prioritizing which risks are urgent – 20%
4. blind spots around emerging risks – 20%
5. too many false positive alerts – 19%
6. dealing with unresponsive suppliers – 19%
7. onboarding suppliers with rigor– 18%
8. offboarding suppliers with rigor – 18%
9. understanding how to penalize suppliers – 18%
10. internal understanding around third-party – 18%
11. enforcing supplier SLAs – 18%
12. real-time visibility on suppliers – 17%
13. lack of in-house resources – 17%
14. n/a we don't have any challenges – 4%

Respondents could tick more than one answer

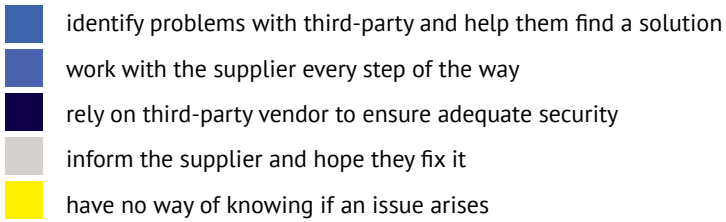
More than a third take a hands-off approach when they find a vendor problem

Organizations are not always upfront with suppliers when they do discover a problem. 36% inform the supplier and hope they fix the issue, while the same percentage 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 - 17% say a lack of in-house resources is one of the biggest pain points they face.

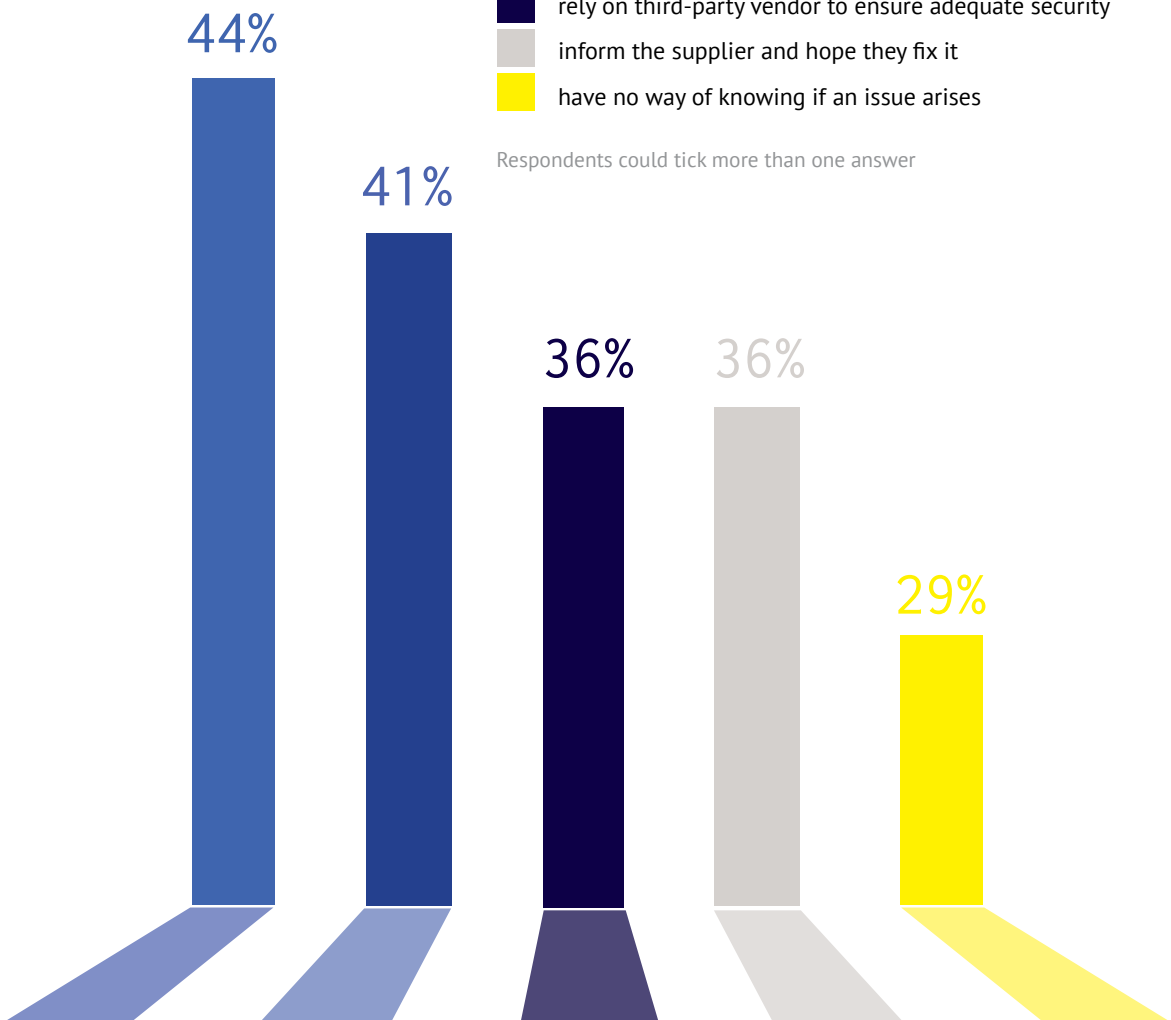
> BlueVoyant Viewpoint: By devolving responsibility for fixing cyber risk issues to vendors, firms relinquish control as they cannot confirm that the vendor has acted to fix the problem. Given that working with vendors to improve security posture is one of the biggest pain points faced by survey respondents it seems there is a need to discover what is preventing a positive relationship with the vendors. In BlueVoyant's experience, a big part of the problem is that when firms highlight an issue with vendors, the information they share may contain false-positive alerts and further lack specifics. Vendors also are more likely to act upon a detailed list of the steps they need to take to fix the issue.

29% have no way of knowing if an issue arises

How Do Supplier Problems Get Handled?



Respondents could tick more than one answer

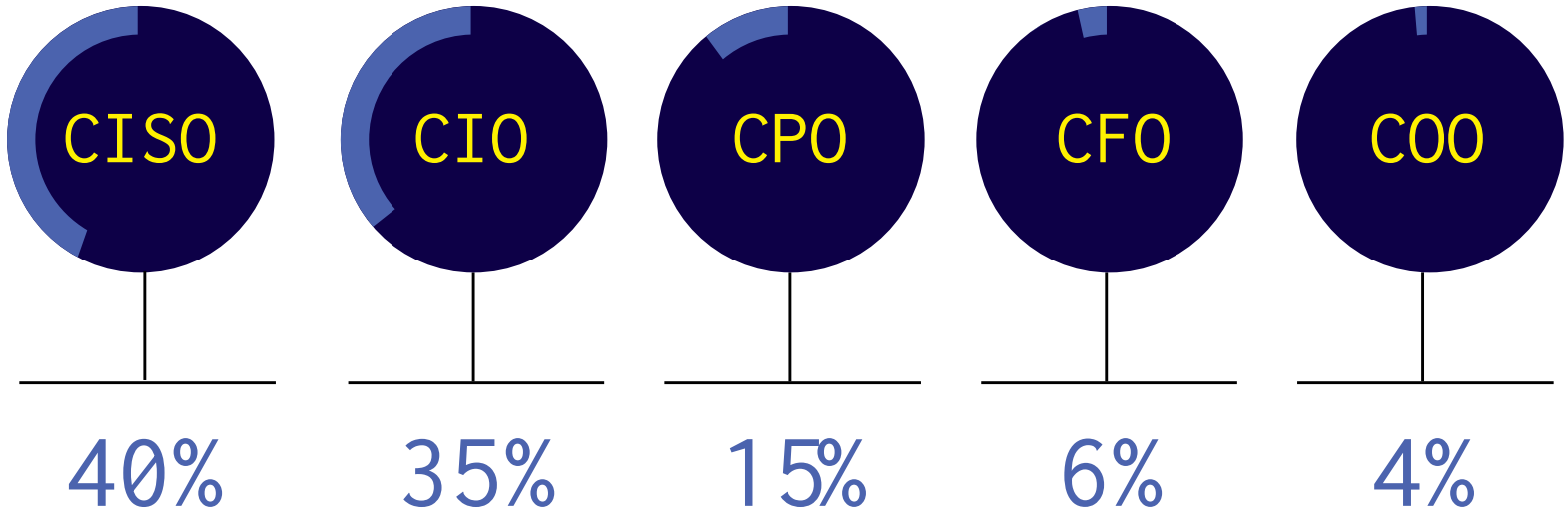


Split over third-party vendor risk ownership

When the CEO asks about cyber risk in the supply chain, who answers the question? For 40% of our surveyed organizations the answer is the CISO, while 35% say it is the CIO. 15% say it is the Chief Procurement Officer. Interestingly, the answer varied widely depending on whom we asked. 68% of CIOs said they had responsibility, while 64% of CISOs said the buck stopped with them on cyber risk. Ask a CPO, and 41% say they have responsibility.

It is interesting that there appears to be ambiguity over who ultimately owns cyber risk. Delving deeper into the differences between traditional procurement functions and IT and security professionals, CPOs are also far more likely to be assessing third-party cyber risk only six-monthly or annually: 44% re-assess six-monthly or annually, while only 27% of CIOs and 29% of CISOs were re-assessing on this time-frame. CPOs are also slightly more likely to be using point-in-time tools such as onsite audits and questionnaires.

Who has responsibility for third-party supplier risk in your organization?



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.

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 business 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.

We have also examined third-party cyber risk management in each country and across five vertical sectors to identify where territory and industry-specific factors are shaping the landscape.

BlueVoyant Viewpoint: This division over the ownership of third-party cyber risk exposes a deeper problem with third-party cyber risk management that we find evident in many firms we work with: cyber risk is caught in a silo, with organizations attempting to partition it from other areas of business risk. Here at BlueVoyant we advocate that cyber risk is integrated fully into business risk and owned at board level and the risk tolerance of all stakeholders is incorporated into cyber risk management so there is a working balance between productivity, protection, continuity and compliance. A cyber risk management program needs to be operational, and it needs additional investment to become an operational activity versus a point-in-time compliance exercise.

> "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.

Vertical Market Analysis

03

Financial services sector:

innovation and regulation pull in competing directions to drive third-party cyber risk management needs

The financial services sector is experiencing considerable commercial disruption coupled with rapid innovation. Established institutions are striving to become more agile and meet evolving customer demand. At the same time new market entrants compete fiercely for customers.

Escalating regulatory pressure

Increasing operational flexibility, through the deployment of cloud infrastructure, for example, is critical for future financial services competitiveness, but it has also driven regulatory evolution around the use of third-party suppliers, in what was already a highly regulated sector.

The Security and Exchange Commission's Office of Compliance Inspections and Examinations earlier this year listed vendor management as a key area in its best practice guidance for regulated companies, underlining that this is a topic of growing focus for regulators. Add to this the growth in non-sector specific regulation, such as CCPA, GDPR and other global privacy legislation, and it is understandable why compliance is a key driver for managing third-party cyber risk in this sector.

Intense cyber threat environment

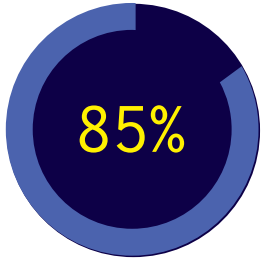
Financial services are also the number one target for cyber-attacks and hackers are rejecting frontal assaults on well-defended walls in favor of infiltrating networks via vulnerabilities in third-party vendors. This means every blind spot in the vendor ecosystem is highly likely to be obscuring cyber risk.

Reputations on the line

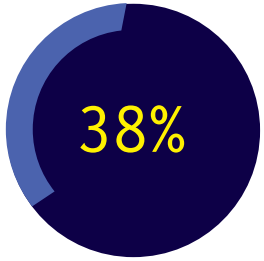
Finally, Financial Services organizations must maintain their good reputation and ensure customer trust. Firms are keen to demonstrate that they are protecting customer assets, providing an ultra-reliable service and working with trustworthy partners, something in which vendor cyber risk management must play a central role.

Key financial services sector findings

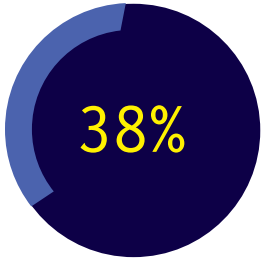
253 CIOs, CISOs and CPOs from the Financial Services sector



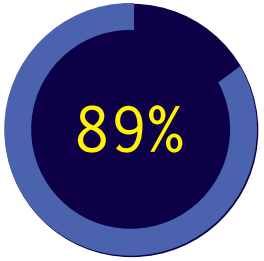
Have suffered a breach because of weaknesses in their supply chain in the last 12 months



User supplier risk data and analytics in their third-party cyber risk management program



Audit and report third-party cyber risk six-monthly or less frequently



Have seen increases in their cyber risk management budget in the past 12 months

41%
Say the CISO owns cyber risk

25%
Have no way of knowing if a risk emerges in a third party

912
Average number of third-party vendors Financial Services organizations use

74%
Do not monitor all third-party suppliers for cyber risk

66%
Work with more than 501 third-party vendors

Compared with other sectors, financial services respondents work with a relatively low number of vendors – 912 versus more than 1000 in all other industries surveyed. Nevertheless, the sector reported one of the highest vendor-originated breach percentages, with 85% of respondents saying they had been affected by a vendor-originated breach in the last 12 months.

Despite a smaller vendor ecosystem, only just over one quarter (26%) said they monitor all vendors for cyber risk, leaving close to three quarters without full visibility.

Third-party vendor monitoring is conducted monthly by 33% of respondents, while 5% are able to assess weekly and 2% are succeeding in achieving real-time oversight. However, 38% only assess vendors six monthly or less frequently. With growing regulatory scrutiny and high penalties for breaches or non-compliance, it seems that the sector is under-scrutinizing its vendors, as those that only detect issues on a half-yearly basis could find a problem has become endemic by the time they identify it. While cyber risk can never be fully eliminated, organizations should be focusing on reducing the amount of unknown cyber risk and managing known cyber risk more effectively.

Looking at actual breaches caused by vendor vulnerabilities in the past 12 months, the financial services sector respondents paint a high-risk picture. 54% have suffered between two and five cybersecurity breaches due to a vendor and 7% have suffered between six and ten.

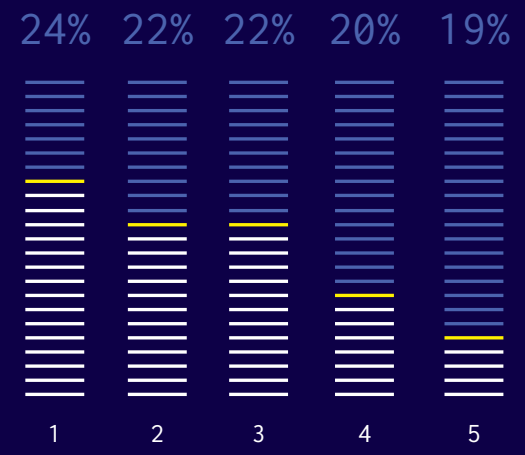
Recognition of under-resourcing and growing risk is evident in the fact that the financial services sector is ahead of other sectors surveyed in the percentage that are boosting budgets. 89% have seen budgets increase and of those 42% have grown by more than 50% compared with

the previous year. Where that budget is allocated will be key, however. At present financial services companies are using a varied mix of tools from point-in-time audits and questionnaires, to cybersecurity ratings and supplier data and analytics. Getting all the collected data integrated to deliver a holistic picture of risk will be the main challenge.

The pain points most commonly chosen by financial services sector respondents indicate a desire, if not yet a successful one, to drive improvement through better vendor relationships. "Working with suppliers to improve performance" and "dealing with unresponsive suppliers when problems emerge" are both in the top five, as is the importance of rigorous off-boarding of critical suppliers, showing that the sector is aware of this issue. The other pain points are reflective of the huge volume of alerts and lack of context with which they are delivered by typical third-party cyber risk management and monitoring tools.

As an industry at the frontier of cyber threats, with the shadow of regulatory compliance omnipresent, the financial services sector will be looking to gain better visibility and drive deeper constructive relationships with vendors to achieve the cyber risk control needed.

Top pain points in managing third-party cyber risk – financial services sector



1. Working with suppliers to improve security
2. Prioritizing urgent risks
3. Too many false positive alerts
4. Dealing with unresponsive suppliers
5. Offboarding suppliers with rigor

Respondents could tick more than one answer

Business services sector:

drivers for third-party cyber risk management

The business services sector, including legal, accounting and consultancy firms, is a critical component of the global economy. From legal services integral to the functioning of justice in society to consultancies helping organizations navigate volatile environments, the sector makes a major contribution to global economic and social continuity.

Like many other sectors, business and professional services firms have been undergoing rapid digital transformation, with the adoption of third-party managed IT services and sector-specific as-a-service applications becoming widespread. This has increased the potential cyber attack surface.

Disruption or infiltration has long-term impacts

There are numerous examples of high-profile incidents where professional services firms have suffered major breaches that have resulted in significant long-term impact or closure of the firms involved. The highly privileged corporate or geopolitical data they hold on behalf of clients makes them compelling targets. Incidents such as the DLA Piper NotPetya ransomware attack and the '9/11 papers' hack illustrate the different motives, from financial gain to hacktivism, that drive threat actors to target the sector. As a result, a high-volume barrage of targeted, sophisticated threats is constantly aimed at professional services firms and their partner ecosystems.

Partner pressure for regulatory compliance

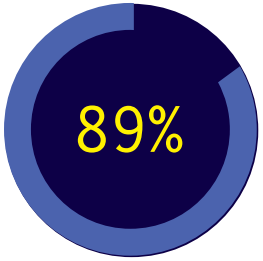
Pressure from clients is a further driver for controlling third-party cyber risk. Firms working closely with clients in highly regulated sectors such as finance and healthcare must comply with the requirements of those clients or risk losing business. However, whether professional services firms can guarantee the cybersecurity compliance of their wider vendor ecosystem, as well as their own operations, is uncertain, as the responses to our survey show.

Trust and ethics

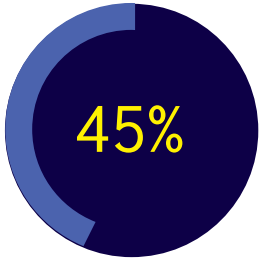
Professional services organizations hold a position of trust with clients and partners. They handle highly sensitive information, the loss of which can prove catastrophic for those affected. As such, firms in this sector can be said to have a higher ethical and legal responsibility than others to safeguard client information.

Key business services sector findings

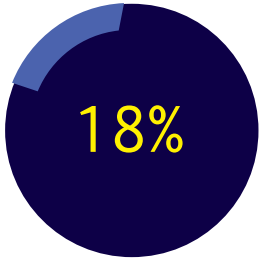
251 CIOs, CISOs and CPOs from the Business Services sector



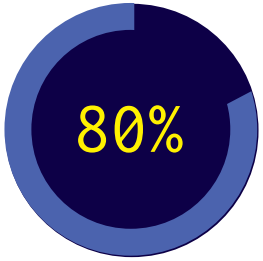
Have suffered a breach because of weaknesses in their supply chain in the last 12 months



User supplier risk data and analytics in their third-party cyber risk management program



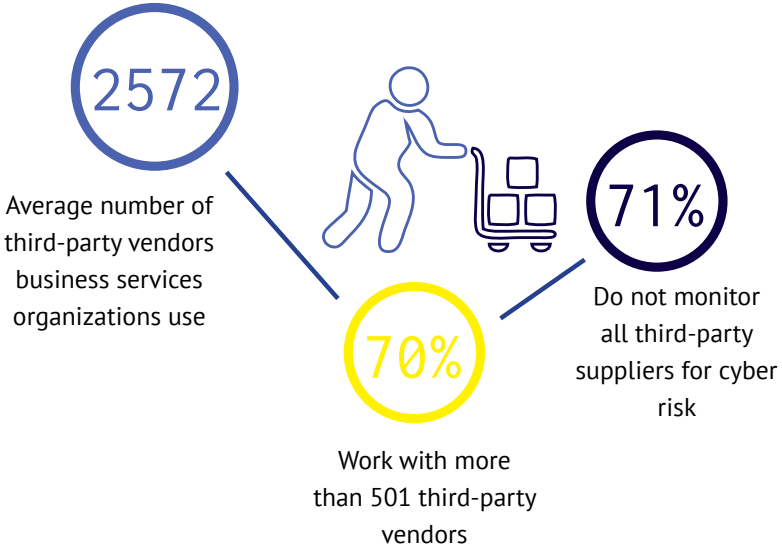
Audit and report third-party cyber risk six-monthly or less frequently



Have seen increases in their cyber risk management budget in the past 12 months

46%
Say the CISO owns cyber risk

34%
Have no way of knowing if a risk emerges in a third party



A large vendor ecosystem is creating correspondingly high risk in the business services sector. The average respondent works with 2572 vendors – the highest number of all the sectors surveyed. 89% of respondents said they had suffered at least one breach originating from their supply chain in the last 12 months, with the average organization suffering 3.6 incidents. Again, this outstripped the figures reported from other sectors.

In terms of monitoring, this sector is performing slightly better than others on average, with 29% saying they monitor all third-party suppliers for risk. Vendor re-assessment and reporting frequency is higher too, with 10% of respondents monitoring vendors weekly or more often. The majority (38%) assess and report on supplier risk monthly, but, given their programs don't typically encompass the whole ecosystem, this still leaves significant gaps. This is evidenced by the high percentage of respondents (34%) who said they had no way of knowing if a risk emerged in their vendor network.

Given the sophistication and volume of threats faced by the sector, it is not surprising that breaches are frequent.

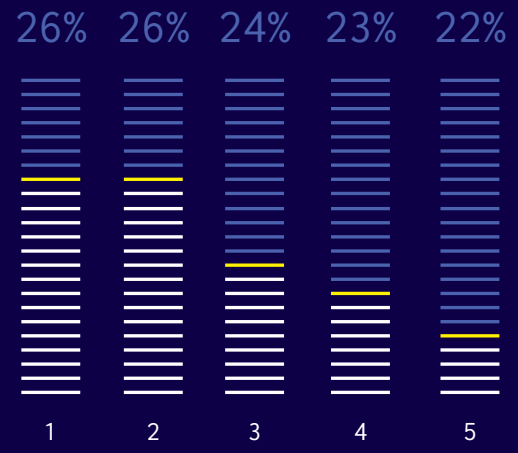
Four out of five of the business services firms we surveyed said they are seeing budgets increasing compared to the past 12 months as their organization responds to the scale of the third-party cyber risk management challenge. What will be interesting to observe is where that budget is being targeted. Clearly, given the rate of breaches, what is in place right now is not proving effective. If business services opt for more of the same, they are unlikely to shift the dial on third-party cyber risk.

Right now, the most commonly used tool is supplier risk data and analytics, selected by 45% of respondents. This is complemented by integrated risk management, in use by 37%. Onsite audits and questionnaires are also in the

toolkit, as are external consultants and security ratings services.

Multiple pain points were experienced in the sector. Respondents most commonly selected issues around dealing with suppliers – either improving supplier performance or difficulties dealing with unresponsive suppliers when problems emerged. However, there is also an acknowledgement that blind spots exist, with 24% saying this was a top-three pain point. Overall, challenges were evenly spread across a wide range of pain points. This highlights that, for many organizations, knowing where to start is a major challenge when it comes to tightening up third-party cyber risk management. It is one thing to have budget to address the issue, but if business services organizations don't have a clear objective and a roadmap to achieving it, the outcome – frequent breaches and continuing risk – will be unchanged.

Top pain points in managing third-party cyber risk - business services sector



1. Dealing with unresponsive suppliers
2. Working with suppliers to improve security
3. Blind spots where we do not have resources
4. Onboarding new suppliers with rigor
5. Getting up-to-date cyber risk visibility

Respondents could tick more than one answer

Healthcare & pharmaceutical sector:

IP, data protection and patient safety drive third-party cyber risk management

In the healthcare & pharmaceutical sector third-party cyber risk takes on direct human relevance. The COVID-19 crisis has thrown the sector into the spotlight and made it an even more attractive target for cyber attacks. However, even before the virus struck, risks were high and their vectors diverse.

Patient data protection

The data held by healthcare providers is some of the most confidential and valuable to individuals, and consequently is highly attractive to cyber criminals. The dark web market for health-related PII and insurance data is booming. As a result, attackers are becoming increasingly creative about how they gain access to healthcare provider networks, employing island hopping tactics that mean the larger the supplier ecosystem, the greater the associated risk.

Innovation increases attack surface

Innovations such as Internet-of-Things (IoT)-based remote patient monitoring systems are changing the lives of patients, but they also represent risk. Typically delivered by third-party suppliers, their compromise would jeopardize patient safety.
At the other end of the innovation scale, but no less dangerous for patients, is the risk of an outage caused by conventional attacks such as ransomware. The NotPetya attack of 2017 cut a swathe through healthcare organizations and exposed the physical disruptions that can be caused by a cyber risk event.

Regulatory pressure

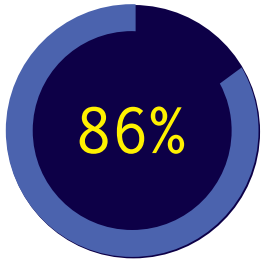
Evolving to match the scale of threats to patient data and safety are the regulations governing the sector, such as HIPAA and the associated HITECH Act. These put the onus directly on healthcare providers to safeguard patient information. Similarly, pharmaceutical companies face strict regulation in clinical innovation, requiring strong risk management.

IP in the crosshairs

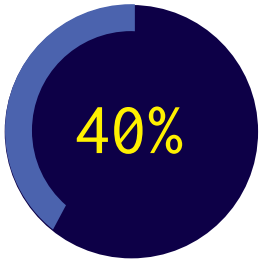
Away from direct patient-facing risks are those upstream in the highly competitive pharmaceutical sector. As firms race to develop cures and vaccinations – particularly in the current COVID-19 environment – their intellectual property data is a prime target for both financially motivated and nation state-sponsored threat actors.

Key healthcare & pharmaceutical sector findings

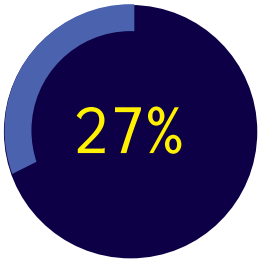
250 CIOs, CISOs and CPOs from the healthcare & pharmaceutical sector



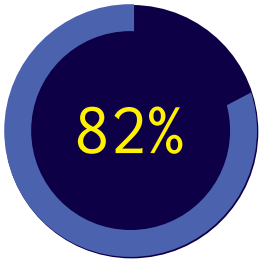
Have suffered a breach because of weaknesses in their supply chain in the last 12 months



User supplier risk data and analytics in their third-party cyber risk management program



Audit and report third-party cyber risk six-monthly or less frequently



Have seen increases in their cyber risk management budget in the past 12 months

54%

Say the CISO owns cyber risk

30%

Have no way of knowing if a risk emerges in a third party

1424

Average number of third-party vendors healthcare and pharmaceutical organizations use

75%

Do not monitor all third-party suppliers for cyber risk

42%

Work with more than 501 third-party vendors

Our research found that budgets are rising in the healthcare & pharmaceutical sector, likely in response to the high proportion of breach incidents – at an average of 2.9 per organization in the last 12 months - the second highest of all the sectors we surveyed.

These cyber risk events are originating in a large vendor ecosystem. With 1424 suppliers reported on average, the sector is second only to the business services sector in terms of supply chain size.

It is therefore concerning, but perhaps not surprising, that only one quarter of healthcare & pharmaceutical organizations say they are monitoring all vendors for third-party cyber risk and that more than one quarter (27%) are re-assessing third-party vendor risk six monthly or less frequently.

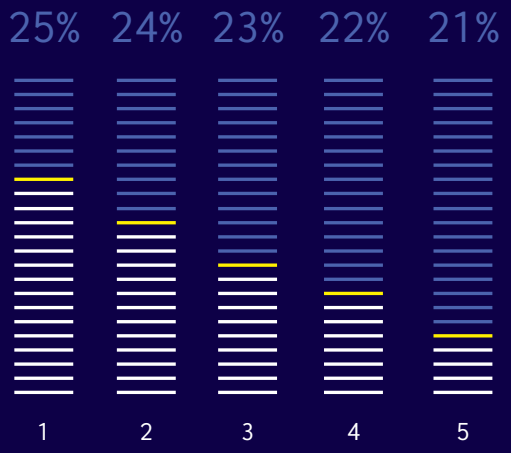
The unavoidable consequence is visibility gaps, evidenced by the fact that 30% of respondents said they would have no way of knowing if cyber risk emerged in their vendor ecosystem. These blind spots were also top of the list of pain points respondents experienced in their third-party cyber risk management program, coming in just ahead of difficulties managing the volume of alerts generated by the program.

The healthcare & pharmaceutical sector is one of the more coherent in identifying where its challenges lie: it has a volume and visibility problem that, in light of the intense threat environment, is leading to breaches originating in its vendor ecosystem.

Interestingly, when asked what methods and technologies they are using to manage third-party cyber risk, respondents from the sector were much less likely to be using integrated risk management compared to their peers in other sectors (only 22% selected this compared with a minimum of 32% in all other sectors) . This may be further indication of the challenges the sector is facing in gaining visibility over all elements of its broad supply chain.

When allocating those growing budgets, the healthcare and pharmaceutical sector needs to be targeting the objective of increasing visibility across its supplier network, so it has better control of cyber risk and can respond more effectively to emerging threats.

Top pain points in managing third-party cyber risk - healthcare & pharmaceutical sector



1. Blind spots where we do not have resources
2. Handling the volume of alerts
3. Understanding how to penalize non-compliant third-parties
4. Onboarding new suppliers with rigor
5. Working with suppliers to improve security

Respondents could tick more than one answer

Energy sector:

reputation and resilience

The energy sector is at an inflection point. Diminishing natural resources and changing consumer values are powering demand for renewable alternatives and, while global energy demand contracted during the first phase of COVID-19[1], this is likely only a temporary effect compared with the dominant trend for growth. Innovation is key to navigating turbulent markets and energy companies are turning increasingly to third parties to power that transformation.

As a core element of critical national infrastructure, energy companies face threats arising from growing cyber-physical integration, as well as more conventional attacks targeting customer data. The increasing interconnectivity of systems and controls, and a receding capability to recover manually due to system complexity and interdependencies, creates shared systemic cyber risks.

For this sector, Distributed Denial of Service (DDoS) attacks that interrupt their ability to deliver key services are a major concern, while third-party compromise of Supervisory Control and Data Acquisition (SCADA) systems is also an ever-present cyber risk to resilience and continuity as companies move towards greater automation and efficiency.

Further, as IoT sensors are increasingly deployed across energy networks in a bid to optimize energy efficiency and monitor performance, the attack surface has increased exponentially.

Nation state-sponsored threats

Nation state-sponsored activity is a particular cyber risk for the energy sector – examples include Russia's 2015 cyber attack on a Ukrainian power station which succeeded in turning the lights out for large sections of the country. Energy companies need to be alert to vulnerable partners in their supply chain that could inadvertently allow an adversary to hop into their network and orchestrate attacks of this type.

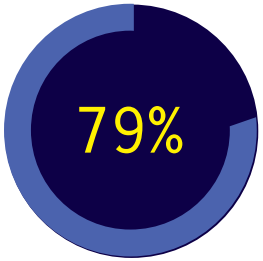
Reputations are of rising relevance

Energy companies have been treading a fine line with consumers as awareness of climate change impacts has sharpened. Acting as a responsible business is now one of the highest priorities for companies in the sector as they bid to address their image problem. Protecting customer data and services from the impacts of cyber risk events is a critical element of this drive to build energy brands that resonate with today's consumers.

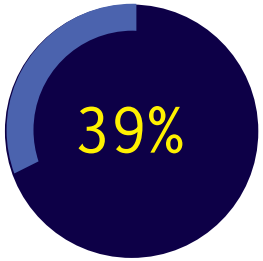
[1]https://www.iea.org/reports/global-energy-review-2020

Key energy sector findings

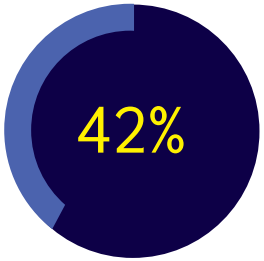
251 CIOs, CISOs and CPOs from the energy sector



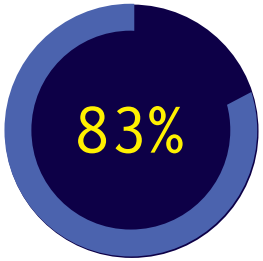
Have suffered a breach because of weaknesses in their supply chain in the last 12 months



User supplier risk data and analytics in their third-party cyber risk management program



Audit and report third-party cyber risk six-monthly or less frequently



Have seen increases in their cyber risk management budget in the past 12 months

34%
Say the CISO owns cyber risk

30%
Have no way of knowing if a risk emerges in a third party

1208
Average number of third-party vendors energy organizations use

80%
Do not monitor all third-party suppliers for cyber risk

63%
Work with more than 501 third-party vendors

Our research found that the energy sector is performing lowest of all the sectors surveyed when it comes to the frequency of re-assessing third-party cyber risk and briefing senior management teams. Over one fifth (21%) only audit and report annually, with a further 21% reporting six-monthly. This means that a large segment of the sector has no visibility over emerging cyber risks within at least a six-month horizon, supported by the finding that 30% say they have no way of knowing when cyber risk emerges in third parties.

Just under four in five respondents said their organization had suffered a breach originating in weakness in the supply chain in the last 12 months. This is lower than those in the business services and finance sectors, but arguably the direct human impacts of these breaches could be far higher.

The drive to compete and diversify through third-party engagement is evidenced through the scale of the vendor ecosystem: energy companies work with 1208 suppliers on average and 63% work with more than 501 suppliers. However, only 20% say their monitor all their suppliers, meaning four in five have only limited visibility.

This scale, coupled with the lack of frequent assessment and reporting of risk over much of it, creates a large reservoir of unknown third-party cyber risk.

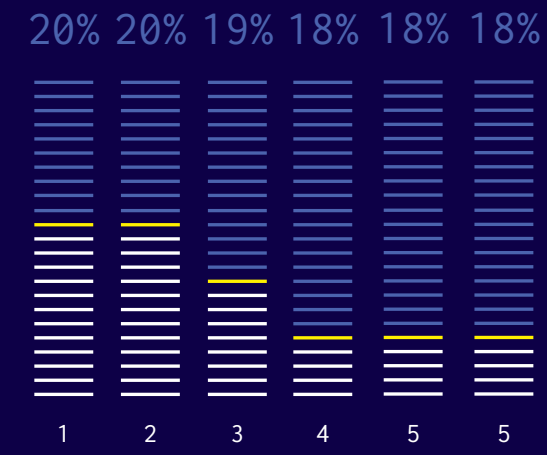
It seems that energy companies are struggling even with the third-party cyber risk monitoring they do succeed in conducting: managing the volume of alerts generated by the system is the top pain point which, when you consider that 80% are not monitoring all suppliers, shows a concerning inability to scale to the extent of the problem.

Perhaps unsurprisingly, the second most common pain point is blind spots where they do not have resources and visibility to spot emerging cyber risks. Third is difficulties in offboarding suppliers with the rigor they were onboarded, indicating awareness that managing former key suppliers safely out of the business is critical in a core infrastructure sector to avoid continued exposure.

In common with all the other sectors surveyed, the majority of energy sector respondents are seeing investment in third-party cyber risk programs, with budgets set to grow by 41%. But, also in common with other sectors, taking a strategic approach to this rather than opting for "the same, but more of it", will be essential to improving the third-party risk posture for the sector. Certainly, simply having more alerts, for example, will not help firms get the essential context that allows them to prioritize risk and triage response.

With the sector facing rising nation state-sponsored activity and growing consumer pressure to do the right thing, getting better control of third-party cyber risk should be high on the priority list.

Top pain points in managing third-party cyber risk - energy sector



1. Too many false positive alerts
2. Blind spots where we do not have resources
3. Offboarding suppliers with rigor
4. Internal understanding that suppliers are part of security posture
5. Getting up-to-date cyber risk visibility
6. Dealing with unresponsive suppliers

Respondents could tick more than one answer

Utilities sector:

reliability and resilience

As components of critical national infrastructure, the utilities sector is the backbone on which society depends for water and sewage services, transportation and more.

Often viewed synonymously with the energy sector, utilities shares many of its key cyber risk factors and drivers for third-party cyber risk management.

The utilities sector has also been undergoing digitization as organizations aim to improve efficiency, reliability and customer experience. This has involved the deployment of Industrial Internet of Things (IIoT) devices across the board to monitor operations and deliver critical data for use in decision-making.

The push for smart cities, which use IIoT-generated data from utility sites such as traffic management schemes and air quality monitoring to improve the quality of life for citizens, has drawn utility firms in and consequently increased the cyber risk should any of their IIoT network become disrupted or compromised.

Defending against cyber physical attacks

In the same way that the energy sector faces risks from the compromise of connected Industrial Control Systems (ICS) and SCADA systems, these are also common features of utilities networks and as such represent a key area of cyber-physical risk. Should these systems be compromised, and control achieved by threat actors, the potential impacts are severe. Here nation state-sponsored activity is a key consideration and third parties must be monitored for their potential use as vectors for island hopping attacks.

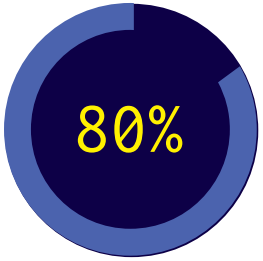
Acting responsibly on climate change and more…

Like the energy sector, the utilities sector is coming under increasing customer pressure to clean up its act. Corporate social responsibility demands are extending from purely environmentally focused behaviors to the wider assessment of large utility companies as corporate citizens.

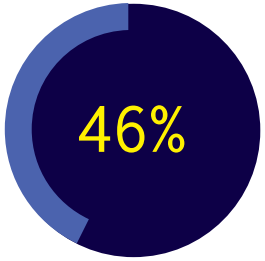
This extends to the safe management of customer data as well as protection of critical supply services against interruption originating from cyber attacks. Part of the responsibility devolves to working with third parties that operate to the cybersecurity standards required and which are prepared to act to mitigate identified cyber risks.

Key utilities sector findings

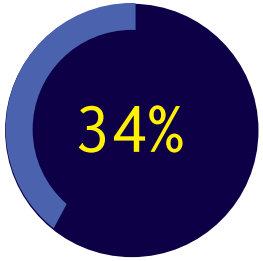
251 CIOs, CISOs and CPOs from the utilities sector



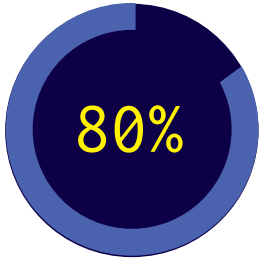
Have suffered a breach because of weaknesses in their supply chain in the last 12 months



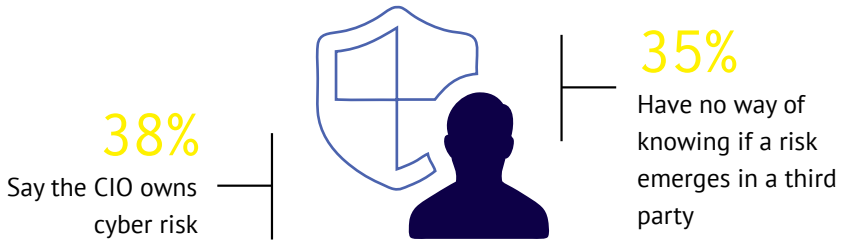
Use vendor risk management in their third-party cyber risk management program



Audit and report third-party cyber risk six-monthly or less frequently



Have seen increases in their cyber risk management budget in the past 12 months



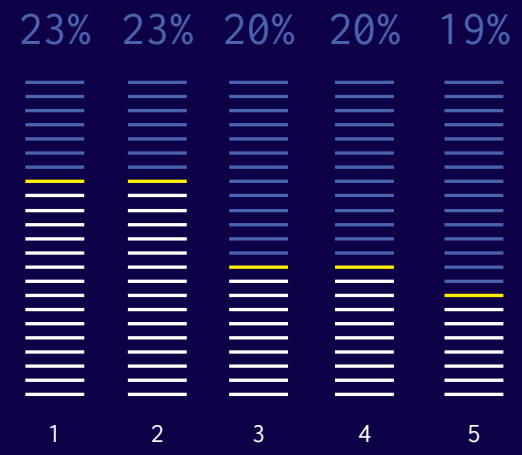
Respondents from the utilities sector also reported working with a large number of suppliers (1013), and a correspondingly high percentage of breaches emanating from weaknesses within them. Four out of five respondents said they had suffered a cyberbreach via the supply chain in the last 12 months and the average respondent's organization had been breached 2.6 times.

It seems that, for the utilities sector, driving improvement within third parties and ensuring they comply with the SLAs that they signed up to are the two biggest pain point areas in managing third-party cyber risk. However, in common with other sectors, there was a broad spread of pain points mentioned, indicating that organizations may struggle to identify where to focus investment and strategic effort to gain material improvements.

Certainly, broadening visibility is advisable. Only 18% monitor all suppliers and 35% say they would have no way of knowing if issues emerged in a third party – the highest percentage stating this in any sector. Add to this the fact that 34% are not re-assessing third-party cyber risk any more frequently than six monthly and it is clear that gaps are unavoidable. Given the potential real-world consequences of cyber breaches, gaps of this nature cannot be acceptable.

Utilities respondents also report growing budgets, with four out of five expecting to see increased investment, but the average increase is lower than most other sectors, at 32%.

Top pain points in managing third-party cyber risk - utilities sector



1. Working with suppliers to improve security
2. Enforcing SLAs with third-parties
3. Internal understanding that suppliers are part of security posture
4. Dealing with unresponsive suppliers
5. Offboarding suppliers with rigor

Respondents could tick more than one answer

Manufacturing sector:

focus on continuity and resilience

At the vanguard of the fourth industrial revolution, the manufacturing sector is evolving rapidly as innovations such as additive manufacturing and the Industrial Internet of Things (IIoT) bring big data and optimization to bear on the manufacturing process itself and its supply chain.

IIoT reliance introduces cyber risk

Deployment of the Industrial Internet of Things sits at the center of transformation in the manufacturing sector. IIoT adoption is creating greater automation and autonomy, optimized stock and raw material control, increased production flexibility and better oversight of the production environment.

As devices are deployed on an industrial scale and connections and dependencies created between information technology and operational technology, the potential impacts of cyber attacks disabling all or part of the IIoT, or harvesting data from it, increase.

Supply chain management expertise: fine-tuning for the digital age

The manufacturing sector is accustomed to large supply chains, the fragile balance of just-in-time production and the fine-tuning of processes to deliver the optimum output in the contracted timescale. As such, overall risk management has always incorporated physical impacts on the supply chain but, with the advancing reliance on technology, has cyber risk awareness kept up? As it has digitized, the sector has again turned to suppliers to deliver the best components, services and software, but at the same time this has introduced a broad spectrum of risk that must be managed.

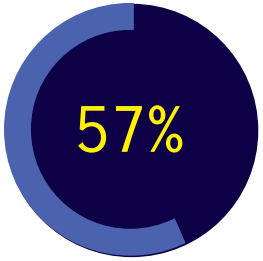
Continuity

Continuity is a critical factor for manufacturers – with production schedules tuned down to the second, any interruption to operations is high cost and risks breaching customer contracts and SLAs, doing damage to reputations and balance sheets alike. As such, the sector is vulnerable to DDoS attacks and ransomware incursions.

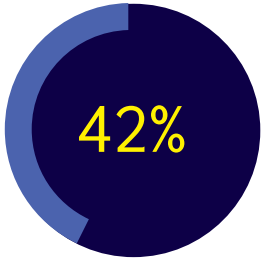
On the other hand, the sector is less exposed than some others to the risk of personal data theft, as it typically doesn't handle data of the volume and quality required to make it attractive to data thieves.

Key manufacturing sector findings

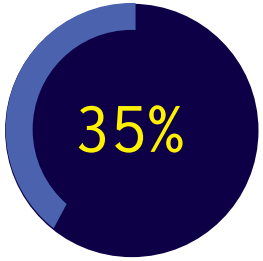
250 CIOs, CISOs and CPOs from the manufacturing sector



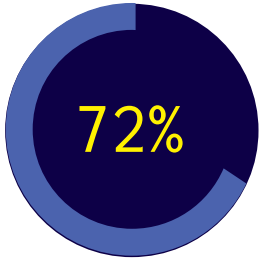
Have suffered a breach because of weaknesses in their supply chain in the last 12 months



Use supplier risk data and analytics in their third-party cyber risk management program

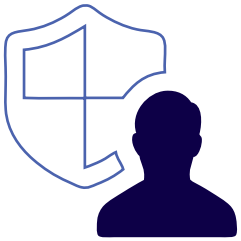


Audit and report third-party cyber risk six-monthly or less frequently



Have seen increases in their cyber risk management budget in the past 12 months

43%
Say the CIO owns cyber risk



20%
Have no way of knowing if a risk emerges in a third party

Average number of third-party vendors utilities organizations use

Do not monitor all third-party suppliers for cyber risk

Work with more than 501 third-party vendors

The manufacturing survey respondents painted a somewhat different picture to their counterparts in other sectors.

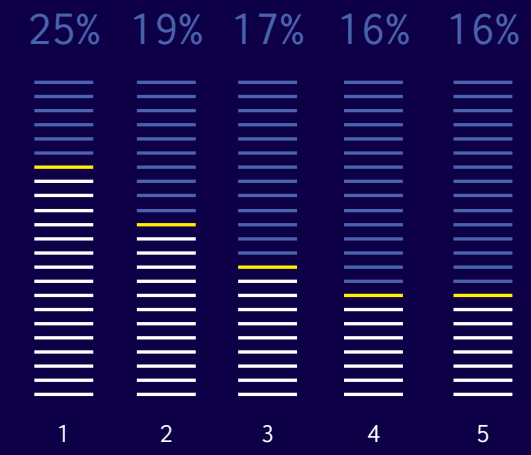
While, as expected, manufacturers report a large vendor ecosystem – 1325 suppliers on average – the rate of breaches originating from the supply chain is much lower than that reported in other industries. A comparatively low 57% said they had experienced a breach resulting from vulnerabilities in their supplier network in the past 12 months and the average number of breaches was only 1.7.

That said, it is possible that a large proportion of cyber risk is simply undetected. Fewer than a fifth of respondents monitor all suppliers for third-party cyber risk; a fifth would not know if a cyber risk emerged in a third party; and more than a third re-assess and report on their third-party cyber risk position six-monthly or less frequently. While this time frame may be adequate for risks such as raw material shortages and climate events, it is unsuited to assessing and addressing the rapid evolution of risks emerging in cyber space.

Compared to other sectors, manufacturing respondents showed less of an even spread over pain points in their third-party cyber risk management programs. Top of the list is handling the volume of alerts generated, but compared with other sectors, manufacturers seem to have less concern or difficulty in working with suppliers

to improve their cybersecurity performance (only 13% selected this compared with an average of 22% across other sectors). The same was true around enforcing SLAs – only 10% were finding this a pain point compared to 19% across the other sectors surveyed. In fact, 13% of respondents said they had no concerns or pain points in their third-party cyber risk management program. This may be because extended supply chains and reliance on third parties has always been an intrinsic feature of manufacturing and they are more experienced. Alternatively, it may be that the management strategies adopted by manufacturers are more suited to traditional supply chain risk management and much third-party cyber risk is simply unknown.

Top pain points in managing third-party cyber risk - manufacturing sector



1. Handling the volume of alerts
2. Prioritizing urgent risks
3. Internal understanding that suppliers are part of security posture
4. Offboarding suppliers with rigor
5. Blind spots where we do not have resources

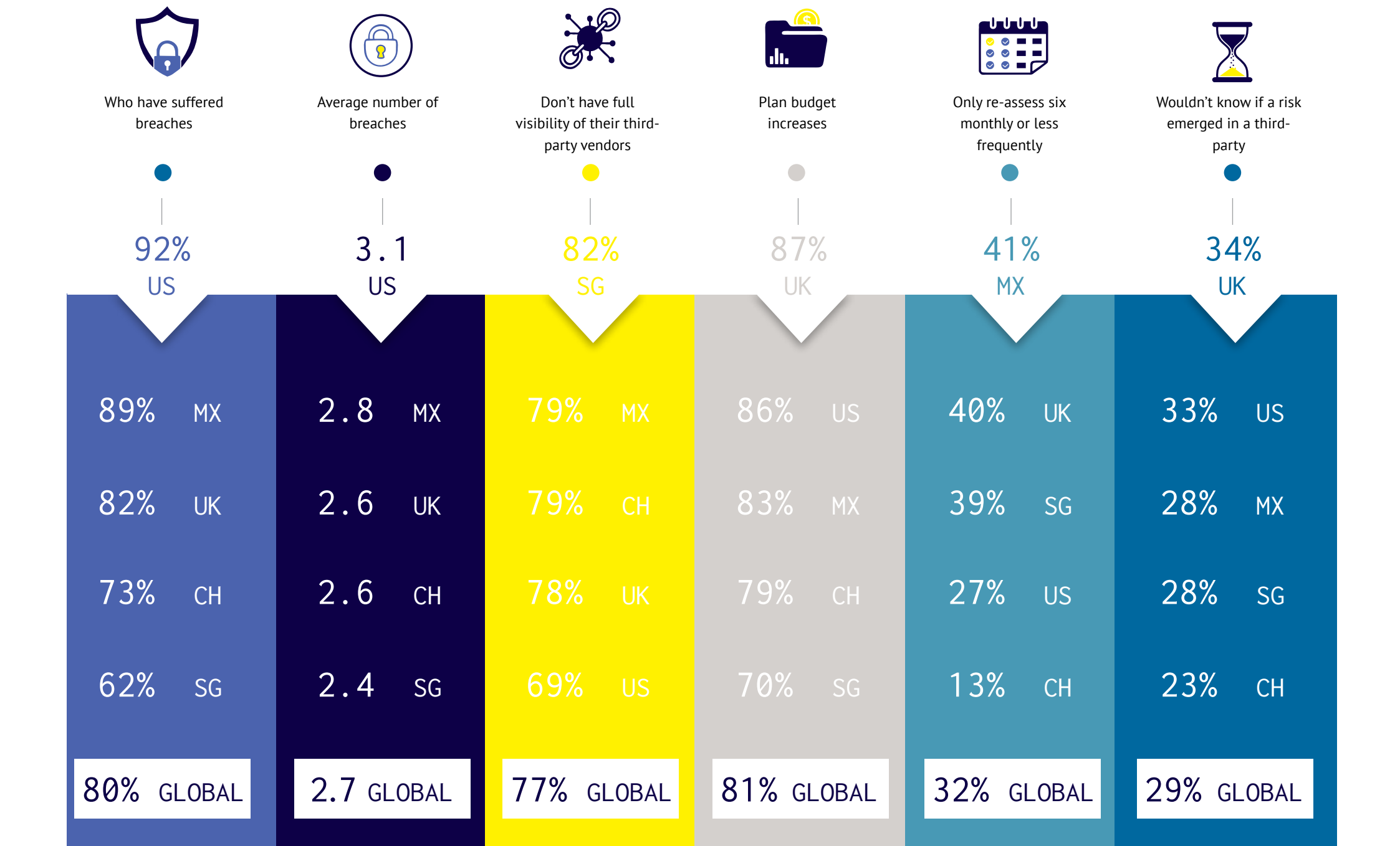
Respondents could tick more than one answer

Country Specific Findings

04

Global Insights: Supply Chain Cyber Risk Key Country Comparisons

US: United States of America
UK: United Kingdom
MX: Mexico
CH: Switzerland
SG: Singapore



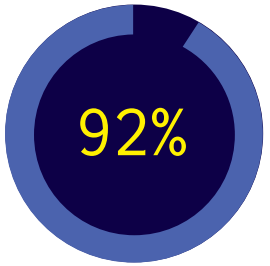
USA Overview

Those responsible for managing third-party cyber risk in US organizations face a considerable challenge. 92% had experienced a breach that originated from weakness in their supply chain in the last 12 months and the average organization is working with 1420 vendors.

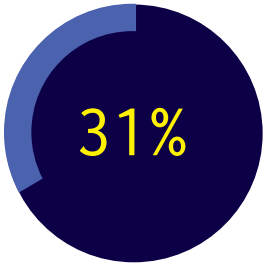
Visibility is a problem for US respondents, with one-third stating that they have no way of knowing if risk arises in a third-party vendor. Only 31% said they monitor all vendors, leaving 69% without full visibility.

Responsibility for third-party cyber risk lies with the CISO for more than half (54%) of US organizations surveyed. However, 27% say the CIO has responsibility and 10% say it lies with the CPO.

Standout statistics



have suffered breaches emerging from the supply chain



say third-party cyber risk is not on their radar

3.1 Breaches on average

Variations compared with other countries:

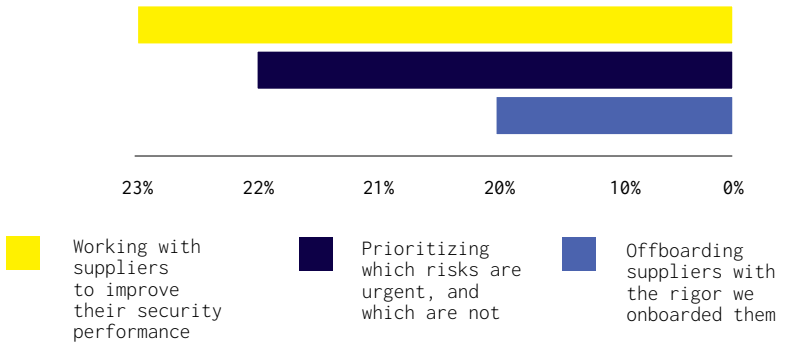
Of the five territories surveyed, US respondents reported the second largest vendor ecosystem, on average, and the highest percentage experiencing breaches caused by vulnerabilities in their supply chain in the past 12 months (92%). This corresponded with the highest breach frequency of all countries surveyed – an average of 3.1 per organization.

However, there are signs that US respondents are responding to the severity of the situation. They were doing better on average when it came to monitoring vendors; 31% said they monitor all vendors for cyber risk compared with an average across all respondents of 23%. US respondents are also re-assessing and reporting more frequently than most other countries surveyed – 35% report monthly and 9% report weekly. However, more than one-quarter (27%) only re-assess and report six-monthly or annually, leaving a significant period when they are blind to any emerging third-party cyber risk.

To combat the challenges they are facing, 86% of US respondents are reporting increased budgets and, at an average increase of 45%; along with the UK they are committing the most money to tackling the issue.

Top three pain points

There was an even spread of respondents selecting pain points across the board, with no real stand-out issues, but concerns across every aspect of third-party cyber risk management. This adds to the challenge of determining where to commit resources.



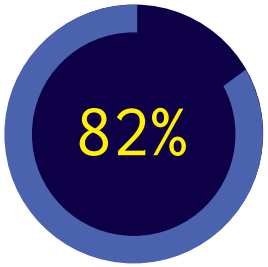
UK Overview

The research found that UK organizations 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 because of weakness in the supply chain.

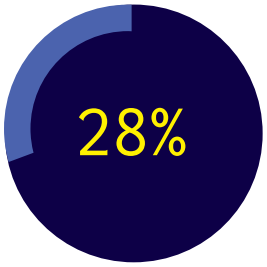
40% only report third-party cyber risk to senior management teams six-monthly or annually, meaning they spend at least half a year with no insight into what is happening in the supply chain. 27% are re-assessing and reporting on risk quarterly, 29% monthly and just 4% weekly. Just over one fifth (22%) said they monitor all vendors, meaning 78% do not have full visibility.

Finally, there is division over who owns cyber risk within organizations, 47% of respondents say the CIO, while 38% say it is the CISO. 11% say it is the Chief Procurement Officer.

Standout statistics



have suffered breaches emerging from the supply chain



say third-party cyber risk is not on their radar

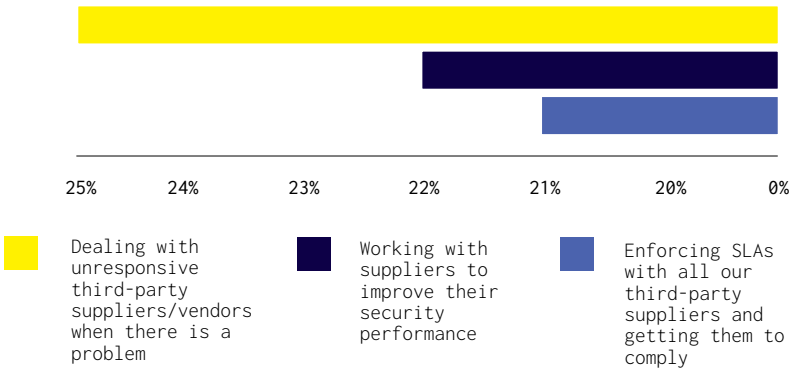
2.6 Breaches on average

Variations compared with other countries:

The UK had the highest percentage out of the five countries surveyed when it comes to having visibility into their partners with 34% admitting that they had no way of knowing if a risk emerged. This means that these organizations are effectively flying blind until a breach takes place. Likewise, they had the highest percentage (40%) of respondents who are only re-assessing third-party cyber risk on a six-monthly basis. Combine this with those that are re-assessing on a quarterly basis (27%) and this means that over two thirds of the respondents don't know what risks exist in their vendor ecosystem from anywhere between three to six months, by which time a breach could have already taken place. The good news is that UK respondents are doing something about this and out of the five countries surveyed they reported the highest budget increase (87%). From the pain points highlighted, working with their vendors to improve security performance and ensure best practice and enforce SLAs is a top priority for UK respondents in order to combat further threats and potential breaches and have that all-important visibility into their extended ecosystem.

Top three pain points

Out of 13 different pain points listed there were many that were causing problems, however working directly with suppliers, and trying to get them to respond to issues identified, is causing UK respondents the most issues.



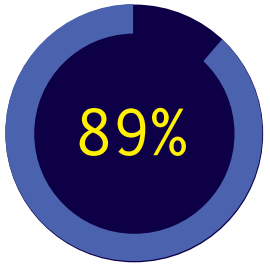
Mexico Overview

The research found that Mexico organizations typically have fewer vendors in their supplier ecosystem compared with other territories, an average of 846. These vendors are nevertheless causing significant cyber risk with 89% saying they have suffered a breach because of weakness in the supply chain in the last year.

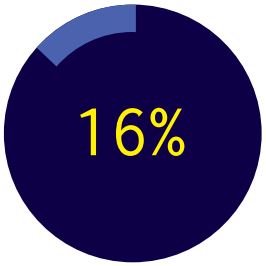
41% only re-assess and report on third-party cyber risk six-monthly or annually, meaning they spend at least half a year with no insight into what is happening in the supply chain. 16% are re-assessing and reporting quarterly, 32% monthly, 9% weekly and 1% daily. 21% said they monitor all vendors meaning 79% have limited visibility.

Finally, respondents are split over who owns cyber risk within organizations, 37% of respondents say the CISO, while 35% say it is the CIO. 22% say it is the Chief Procurement Officer. This fairly even split underlines the inconsistency over cyber risk ownership and potential tensions created because of this.

Standout statistics



have suffered breaches emerging from the supply chain



say third-party cyber risk is not on their radar

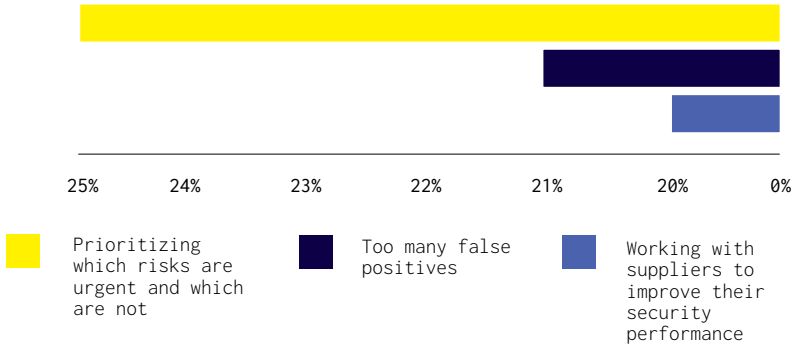
2.8 Breaches on average

Variations compared with other countries:

Mexico had the lowest number of vendors in their supply chain out of the five countries surveyed but had the second highest (USA was top) number of respondents saying that they had been breached in the past year (89%). Mexican respondents appear to be favoring manual processes, with 39% saying that they use external consultants as well as other static point-in-time tactics such as on-site audits and supplier questionnaires, when they were asked about the tools they utilize for third-party cyber risk management. These responses were somewhat out of step with other countries. Likewise, teams in Mexico are larger than the other countries surveyed with 15 people on average dedicated to third-party cyber risk programs. This again could be down to the fact that they are much more reliant on manual processes and need to automate in order to scale and reduce the resources dedicated to managing cyber risk.

Top three pain points

Out of 13 different pain points listed there were many that were causing problems, however prioritizing and understanding what risks to triage and take actions on is the main issues Mexican respondents are dealing with.



Switzerland Overview

Respondents in Switzerland have an exceptionally large vendor ecosystem, reporting an average of 2583 vendors each. Risk in an ecosystem this size is almost inevitable, and almost three-quarters (73%) have experienced a breach due to vulnerabilities within the supply chain in the last 12 months.

One-fifth (21%) of Swiss respondents say they are monitoring the whole of their large ecosystems, but the remaining 79% have less-than-complete visibility. Correspondingly, 23% say they have no way of knowing whether a cyber risk has emerged in their supply chain.

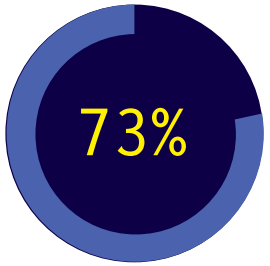
Ownership of third-party cyber risk varies, 44% lay it at the CISO's door, 37% say the CIO is responsible, and just 12% say it is the Chief Procurement Officer.

Variations compared with other countries:

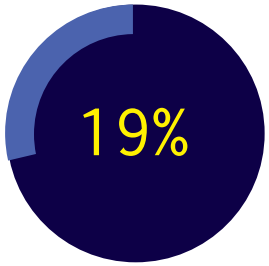
Survey respondents in Switzerland reported by far the largest vendor ecosystems, the average of 2583 being more than 1000 greater than any other territory surveyed. Despite this high number of partners, only 73% said they had suffered a cyber breach via a vulnerability in that ecosystem in the past year. While still a high percentage, this is lower than the UK, US, and Mexico, where the breach percentages were all more than 82%.

This may be in part due to the higher frequency of third-party cyber risk re-assessment and reporting seen in the region. One-quarter of respondents do this weekly, compared with an average of only 7% who achieve this in other countries surveyed. A further 3% review risk daily and 2% assess third-party cyber risk in real-time. To achieve this, 42% of respondents in Switzerland are using security ratings services and 45% use vendor risk management – a higher proportion are using these than seen in other regions.

Standout statistics



have suffered breaches emerging from the supply chain

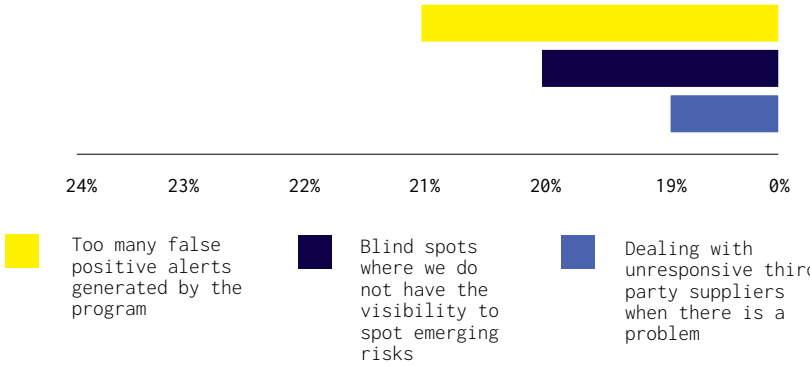


say third-party cyber risk is not on their radar

2.6 Breaches on average

Top three pain points

The comparatively large size of Swiss vendor ecosystems is reflected in the first two pain points, where numerous false positives and blind spots are obstructing efficiency. A high volume of suppliers also makes individual management difficult so, even if a risk is spotted, the route to resolution can be long and time-consuming.



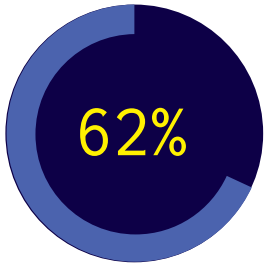
Singapore Overview

The research found that Singaporean organizations have a lot of vendors in their supplier ecosystem, an average of 1176. That said, Singapore has the lowest percentage (62%) of respondents who had suffered a breach at the hands of a third party in the last 12 months out of all five countries.

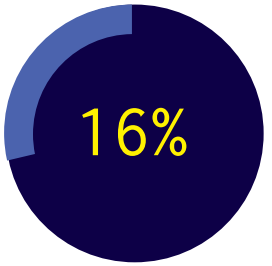
39% only re-assess and report on third-party cyber risk six-monthly or annually, meaning they spend at least half a year with no insight into what is happening in the supply chain. 20% re-assess and report quarterly and 32% monthly. 7% achieve weekly visibility, 2% monitor in real-time while 1% monitor daily. Correspondingly 28% say they have no way of knowing whether a cyber risk has emerged in their supply chain.

Finally, respondents are split over who owns cyber risk within organizations, 27% of respondents say the CISO and an equal amount also say the CIO. 18% say it is the Chief Procurement Officer. This even split underlines the inconsistency over cyber risk ownership and potential tensions created because of this.

Standout statistics



have suffered breaches emerging from the supply chain



say third-party cyber risk is not on their radar

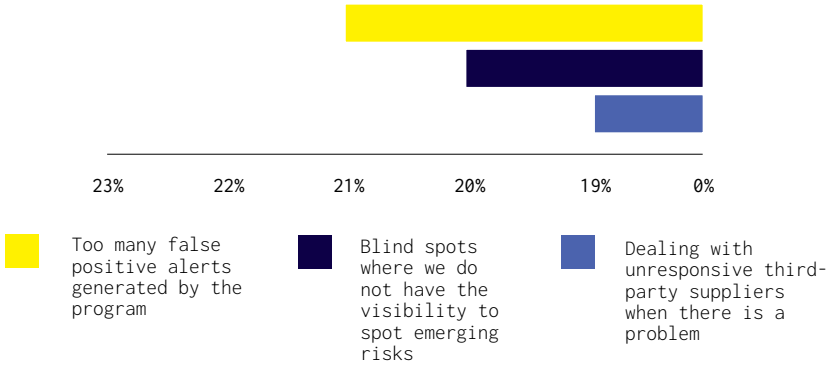
2.4 Breaches on average

Variations compared with other countries:

Singapore had the lowest number of breaches reported out of all five countries surveyed, but this is still surprising given that it is recognized as a key financial center and prides itself on security and stability. Singapore also had the lowest number seeing budget increases (70%) out of the countries surveyed, indicating that respondents are not as concerned as other countries about the need to tackle third-party cyber risk. 39% of Singaporean respondents are only re-assessing and reporting on third-party cyber risk six monthly or annually. It also had the lowest percentage (18%) of respondents out of all the countries who said that they are monitoring the whole of their large ecosystem, but the remaining 82% have less than complete visibility.

Top three pain points

Out of 13 different pain points listed there were many that were causing problems, however prioritizing and understanding what risks to triage and take actions on is the main issue Singaporean respondents are grappling with as well as getting others in the business to understand the security issues that suppliers.



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

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

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

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