# All supply chains are digital

*Cybersecurity for a software-defined future*

IBM Microsoft

## About the Microsoft-IBM partnership

Microsoft and IBM have a strategic partnership to help organizations achieve holistic enterprise-wide threat management. Our aligned security solutions enable confidence to accelerate migration, modernization, and business transformation using Microsoft cloud.

IBM brings a comprehensive cloud security portfolio, including strategy and risk consulting to align and optimize security resources, solutions to protect and achieve digital trust, implementation and operation of threat management capabilities, and open, multicloud solutions to transform security using your existing resources. For more information, please visit: https://ibm.biz/msftsecurity

## How IBM can help

IBM Security® is your trusted partner that evolves with your business, offering technology and services infused with AI. Our modern approach to security strategy empowers you to take advantage of digital innovations and thrive in the face of uncertainty and cyber threats. For more information, please visit: https://ibm.com/security

# Key takeaways

*Cyber and supply chain risks are converging.*

- For organizations to secure their supply chains, they must secure their *digital* supply chains.

  Physical operations are increasingly intermediated by digital controls.

- Executives too often choose suppliers based on cost, overlooking (costly) risk factors.

  Direct and indirect suppliers often do not have routine cyber risk management practices in place.

- AI can improve operational resilience by enabling better integration across cyber and supply chain operations.

  Leveraging advanced technologies can position organizations to improve collaboration and mitigate supplier risks.

# Navigating the new age of risk

In the past, supply chains were predominantly physical in nature. But today, digital technology plays a central role. That generates enormous efficiency, but it also creates new, underappreciated risks. While organizations are focused on enhancing the resilience of their supply chains, too many are leaving their networks exposed to cyber risk.

With dark web cybercrime marketplaces maturing rapidly, cyber adversaries are sharing resources in a booming cybercrime-as-a-service ecosystem—empowering bad actors to prey upon any weak links in supply chains.[1] They often target niche suppliers with fewer resources and more vulnerabilities.[2] In other words, the companies that make up the lion's share of large supply chain networks.[3]

Hundreds—even thousands—of third parties are connected directly or indirectly, offering a myriad of paths into critical systems. One study reported 98% of organizations had at least one vendor compromised by a data breach in the last two years.[4] Other research found that a data breach originating at a business partner costs nearly 12% more than other types of data breaches.[5]

To better understand how cybersecurity factors are shaping the evolution of value chains, supply chains, and ecosystems, the IBM Institute for Business Value (IBM IBV) partnered with Microsoft to conduct a global survey of 2,000 cross-industry security and operations executives (see "Study approach and methodology" on page 26). The findings indicate a distressing lack of awareness around supplier risk and cyber vulnerabilities. While 74% of respondents say supply chain resilience is critical to the success of their organizations, only 40% acknowledge that ecosystems are expanding cyberattack surfaces. And fewer than one in three are prioritizing investments in a secure, connected ecosystem for their supply chain operations.

*Organizations that view cyber risk and supply chain risk management as interdependent see notably less disruption.*

Our research also shows that those who view cyber risk and supply chain risk management as interdependent see notably less disruption. Yet for too many organizations, siloed decision-making and weak cybersecurity hygiene fuel negative outcomes, clouding visibility into potential threats and their impact on operations.

In this report, we explore three critical cyber risk management challenges that emerged from our research. With each challenge, we also present an opportunity—how addressing that challenge can strengthen supply chain resilience. A brief action guide punctuates each section, providing specific steps leaders can take to initiate better integration of cyber risk and supply chain risk management across their organizations and ultimately their ecosystems.

**Perspective**

## Starting point: What do we mean by "supply chain"?[6]

A supply chain is the network of individuals, organizations, resources, activities, and technology/IT systems involved in the creation and sale of a product. A supply chain encompasses everything from the delivery of source materials from the supplier to the manufacturer through to its eventual delivery to the end user.

A software supply chain consists of everything and everyone that touches code in the software development lifecycle, including information about the components (such as infrastructure, hardware, operating systems, cloud services), the people who wrote them, and the sources they come from, like registries, GitHub repositories, code bases, or other open-source projects. It also includes any vulnerabilities that may negatively impact software security.

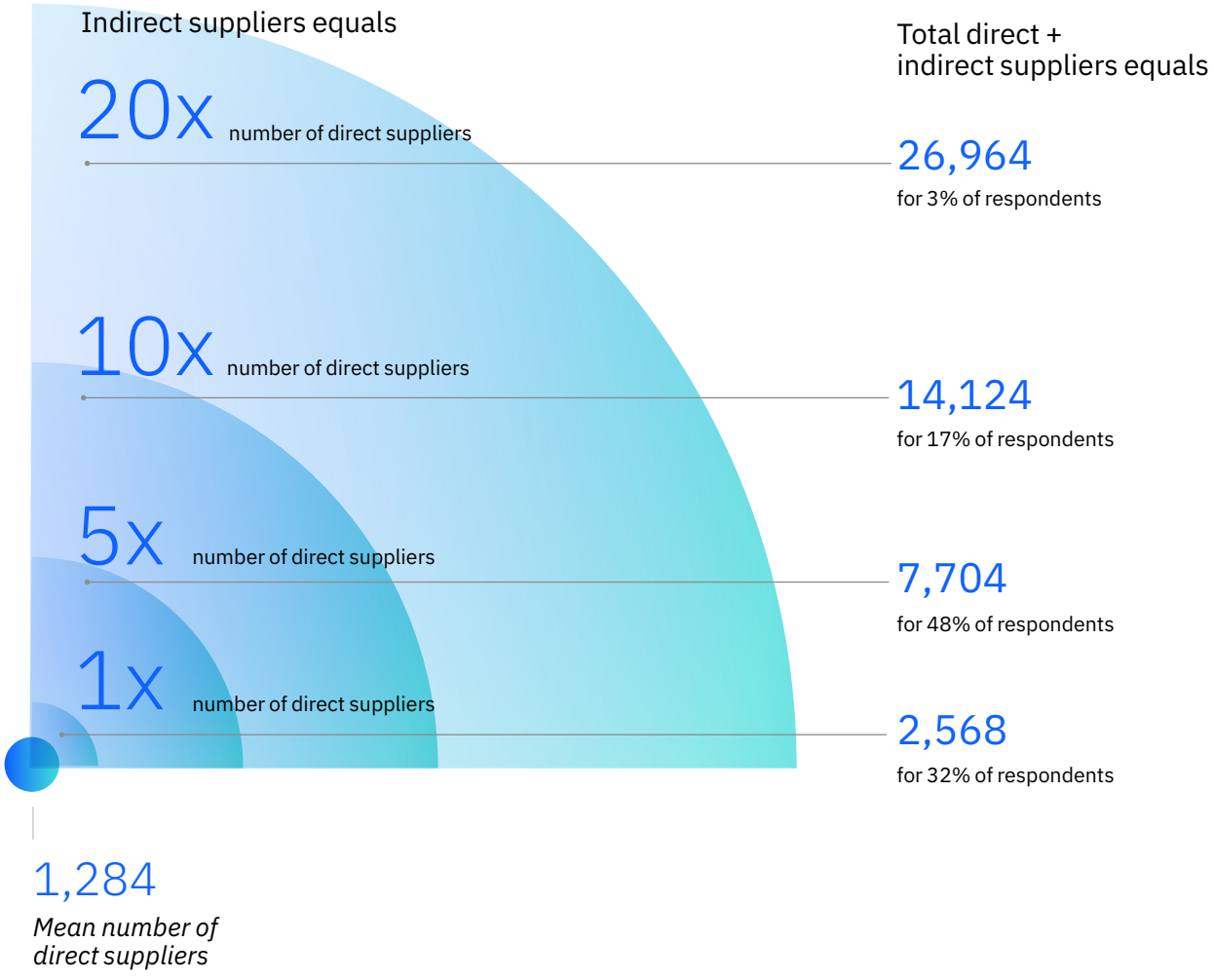
**Challenge 1:**
**Overwhelming scale**

# Digital supply chain operations—and risks—are rapidly multiplying

Supplier networks are proliferating. Our respondents report a massive web of direct and indirect suppliers. Executives indicate the mean number of direct suppliers across all sectors is 1,284. When accounting for indirect suppliers, the number of third parties explodes (see Figure 1). Almost half (48%) of respondents estimate the number of indirect suppliers is five times their number of direct suppliers, or 6,420. When combined, the total number of direct and indirect suppliers represents a massive attack surface: at least 7,700 potential threat vectors into the organization.

FIGURE 1

**An expanding supplier footprint presents a massive attack surface, offering numerous entry points to critical infrastructure and operations.**




*Q. How many direct suppliers enable and support your organization's critical supply chains?*

*Q. How many indirect (n-party) suppliers do you estimate support your direct suppliers?*

Such a vast supplier network makes it difficult, if not impossible, to anticipate potential disruptions, let alone coordinate an effective response. The impact on operations can be substantial. When comparing organizations with the fewest number of total suppliers to those with the most, organizations with more suppliers report a 17% higher incidence of severe operational impacts. This analysis encompasses impacts across a range of factors including cyber incidents, talent and raw material shortages, and extreme weather events (see analysis on page 20).

In fact, in a highly interconnected supply chain environment, cyber incidents are often the spark for far-reaching disruption. While our respondents do not report widespread cyberattacks through suppliers, 30% have suffered an attack in the past three years because of a third-party vulnerability. A recent report suggests the problem is growing: 41% of organizations surveyed suffered a material cyber incident caused by a third party.[7]

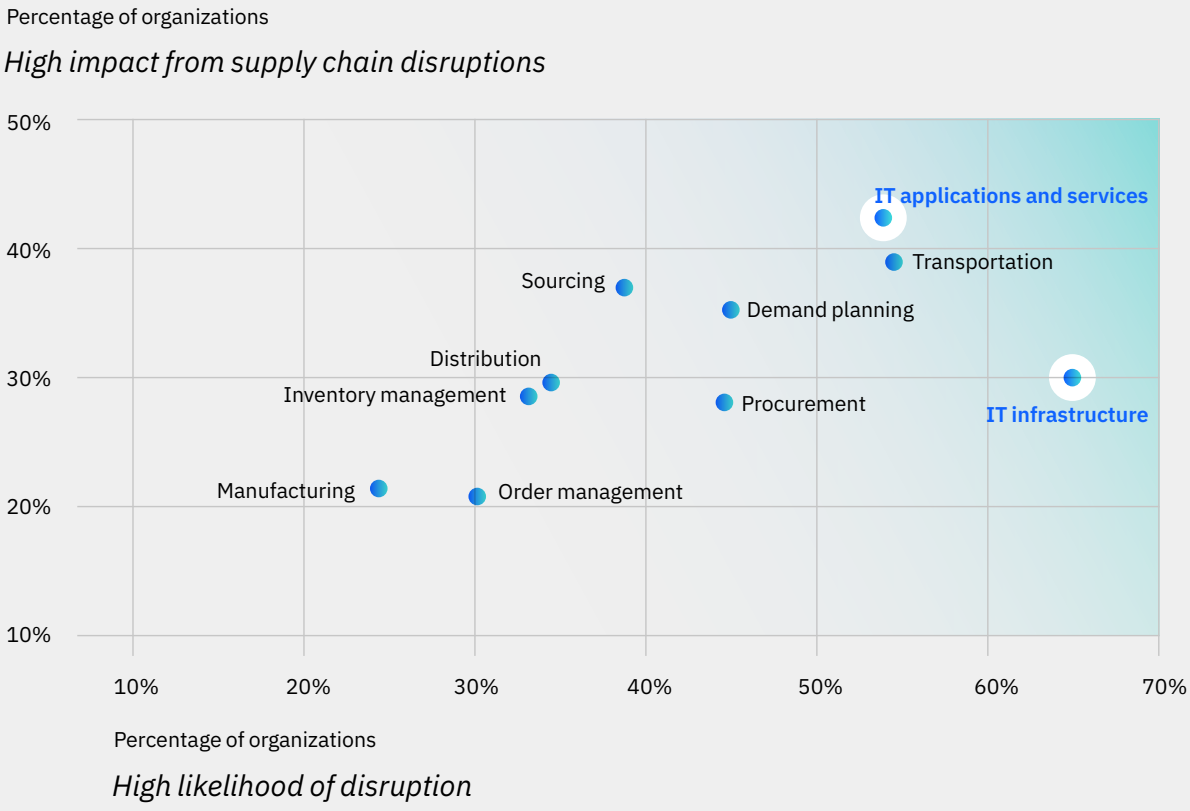
This reality puts enormous pressure on the security of supply chain applications and services. Key takeaways from respondents across industries for the last three years include:

- Nearly 40% say their organizations experienced cybersecurity incidents either requiring extraordinary measures to resolve or posing a lasting material impact on operations.
- More than half (52%) report significant or severe disruption in their supply chain IT applications and services.
- Disruptions to IT applications and services impacted operations more than disruptions to other functional areas.

Looking ahead, 65% say supply chain disruptions are likely to occur in their IT infrastructure with another 53% citing IT applications and services (see Figure 2).

FIGURE 2

**IT-related functions are the most likely and most impacted areas of supply chain disruption.**




*Q. Where are supply chain disruptions most likely to occur? Percentage of respondents answering likely and extremely likely.*
*Q. Which functional areas would be most impacted by supply chain disruptions? Percentage of respondents answering moderate impact and major impact.*

## Opportunity: A secure-by-design approach enhances both cyber and supply chain resilience.

Given the vast scope of business partner relationships, securing a supply chain requires a new approach—one that recognizes the common functionality connecting internal and external IT platforms and services. Many supply chain inputs and outputs are enabled and delivered using common infrastructure, and that provides an advantage. If cyber risk and supply chain risk management are viewed as connected, they each get stronger.

Think of a DNA double helix where cyber resilience and supply chain resilience reinforce each other. Together, they represent a common thread that enables efficiency, coordination, and value creation; yet they also represent two distinct capabilities that are interdependent and evolving in parallel. Improving visibility and governance is essential within the organization and, more importantly, across the supply chain and partner ecosystem.

More practically, what does this level of integration look like? It is a culture where cyber risk, security, and resilience are elevated in importance across the supply chain—from initial design to sourcing materials and suppliers to distribution to the end of the product lifecycle. As a first step, supply chain and risk management leaders can follow the lead of the software and hardware development communities, which have adopted secure-by-design principles, also known as “shift left.”

This approach puts security at the forefront of decision-making, not as an afterthought.[8] Applying secure-by-design to each stage of the supply chain forces parties across operations to prioritize cyber risk management and coordinate their governance practices. It facilitates collaboration both across functions and out into the partner ecosystem. The advantages are many, namely the ability to identify potential vulnerabilities early, share best practices, and help ensure a coordinated response to threats (see case study, “How one auto manufacturer embraced a new security-first mindset” on page 8).

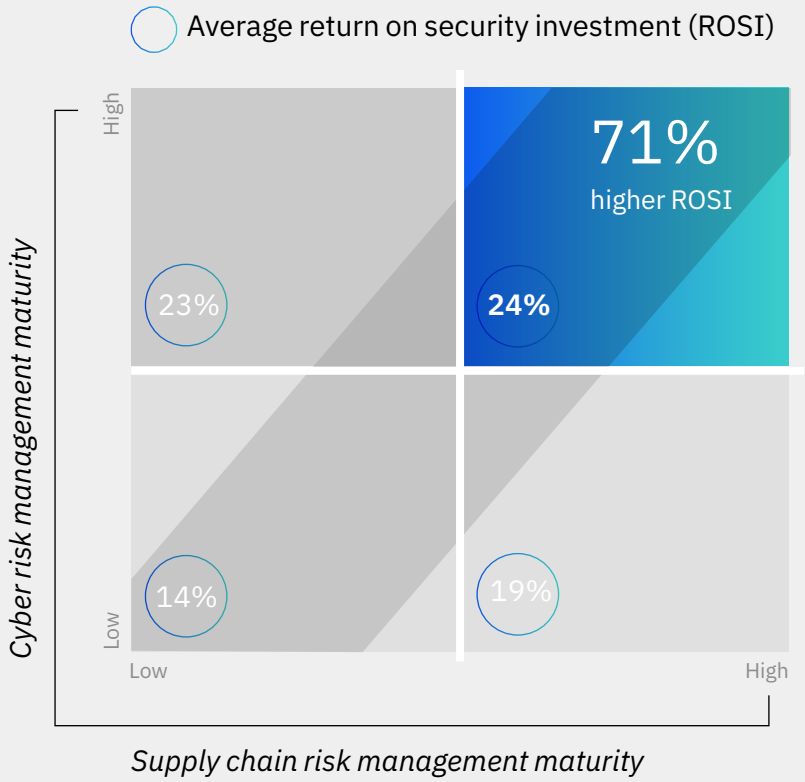
Such an approach leads to better operational and business outcomes. Our analysis shows that organizations demonstrating greater maturity in both cyber risk and supply chain risk management see a significantly higher return on their security investments (see Figure 3). The two dimensions of maturity reinforce each other. This sub-group saw 89% fewer cyber incidents over the previous three years, as compared to other organizations reporting similar severe impacts from cybersecurity incidents.

## Action: Prioritize security in supply chain operations with a secure-by-design approach.

1. Create a cross-functional supply chain risk management team—including IT, OT, and product security experts—to review current supply chain processes and systems.
2. Compile a list of suppliers and segment them by criticality and risk exposure. Task the team with identifying all potential points of vulnerability, from supplier sourcing to logistics to software distribution channels.
3. Then, have the team work together to design and integrate security controls to mitigate risks identified.

FIGURE 3

**Organizations that are integrating cyber risk and supply chain risk management more successfully are seeing greater value from their security investments.**




*Based on IBM IBV analysis.*

**Case study**

# How one auto manufacturer embraced a new security-first mindset[9]

As vehicles become more software-enabled, security becomes an imperative for safety. The modern car contains upwards of 150 million lines of code, increasing the opportunities for cyberattacks. In response to these threats, new regulations have emerged, including the United Nations Economic Commission for Europe (UNECE) WP.29 regulations and ISO/SAE 21434 standards for managing software cybersecurity risks throughout the product lifecycle.[10]

One global automaker realized the critical role security plays in its ambitions of going fully electric and expanding its install base of connected vehicles. And they recognized the need to accelerate cybersecurity maturity: the company quantified the assessed risk from a sample of its critical IT assets at an annualized loss expectancy upwards of $1 billion—a staggering price tag that could threaten future operations and brand perceptions.

Taking advantage of long-standing investments in Microsoft Azure infrastructure and services, the company worked with IBM to embark on a journey to re-envision security—moving from a manual, reactive security posture to proactively anticipating what could happen.

The process embodied a holistic "secure by design" methodology, where security functionality is embedded and security controls are integrated, from manufacturing/OT and enterprise/IT, to rationalizing suppliers for connected products, to the way the company hires and trains its workforce. For this OEM, that meant a new mindset. No longer should they close security gaps after they appear, but instead, security becomes an essential element connecting the vehicle fleet to backend services, and the supplier ecosystem to the factory floor—including the software suppliers contributing to their codebase.[11] The transformation roadmap is expected to cut risks in half in less than three years.

*A holistic "secure-by-design" approach embedded security functionality and controls across operations—from manufacturing/OT and enterprise/IT, to rationalizing suppliers for connected products, to workforce hiring and training practices.*

**Challenge 2:**
**Fragmented management**

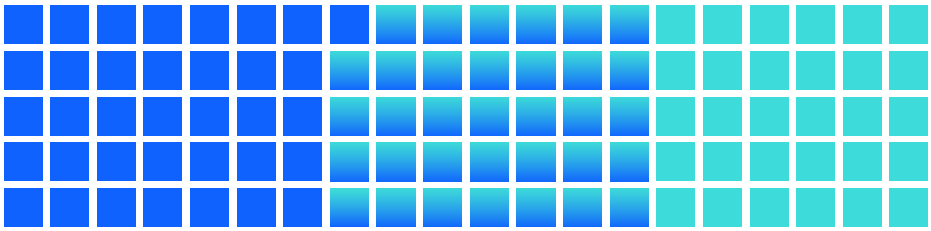
# The consequences of splitting cyber from supply chain risk management

Risk management in most organizations lives in a house divided. Yet, as severe risks are typically cross-functional in nature, they don't align to organizational boundaries, especially those that govern physical and digital supply chains. While both physical and digital supply chains contribute significantly to revenue (see Figure 4), organizations lack a holistic view that bridges accountability for risks across both areas. 70% of executives report that physical and cyber risks are managed through different parts of the organization—meaning common risks comprising physical and digital threat vectors can be overlooked or underestimated.

FIGURE 4

**Supply chains are now predominantly digital.**

*Percentage of organizational revenue*



35%
via physical supply chain

34%
via a combination

30%
via digital supply chain

*Digital supply chains represent nearly 2/3 of organizational revenue*

*Q. Estimate the proportion of your organization's revenue that is enabled and delivered as follows: via physical supply chains, via digital supply chains, and via a combination of physical and digital supply chains. 2023. Percentages do not equal 100% due to rounding.*

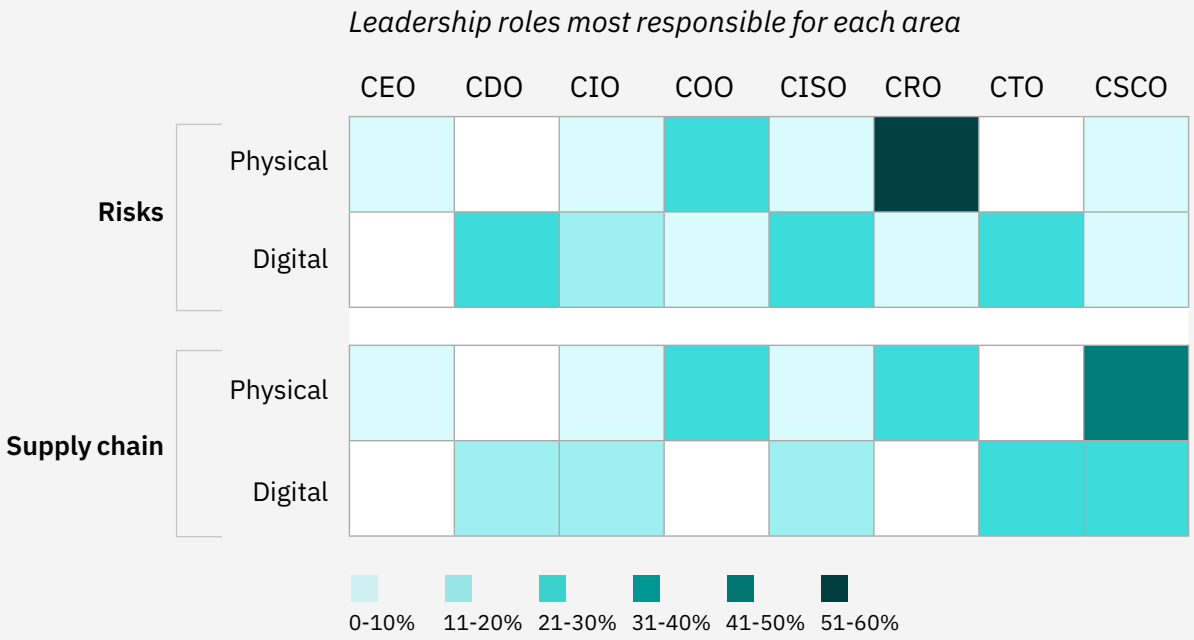
Looking more specifically at who is responsible for physical and digital risks, as well as overall physical and digital supply chains, our research reveals duties are spread across the C-suite (see Figure 5). No single executive role sits squarely in the driver's seat with a view of all hazards on the horizon. Titles may vary based on company size and organizational structure, but if risk management and supply chain operations are organized by traditional functional towers, coordination across the organization is difficult. This challenge is even greater for organizations striving to stay in sync with ecosystem partners. For many organizations, the right hand doesn't know what the left hand is doing—posing a fundamental challenge for security and supply chain leaders.

## Opportunity: Better internal visibility and coordination—backed by AI and automation—fuels external results.

With proper governance, digital value chains improve visibility and drive effective coordination —transcending functional boundaries within organizations and enhancing capabilities across the supplier base. Enabled by technologies such as cloud services, IoT, and AI, supplier connectivity facilitates real-time communication, collaboration, governance, and data sharing. These are the critical capabilities enabling effective coordination across supply chain and ecosystem partners at production efficiency and scale.

FIGURE 5

**Risk and supply chain responsibilities are dispersed across the C-suite, making it difficult to generate a holistic view across physical and digital domains.**

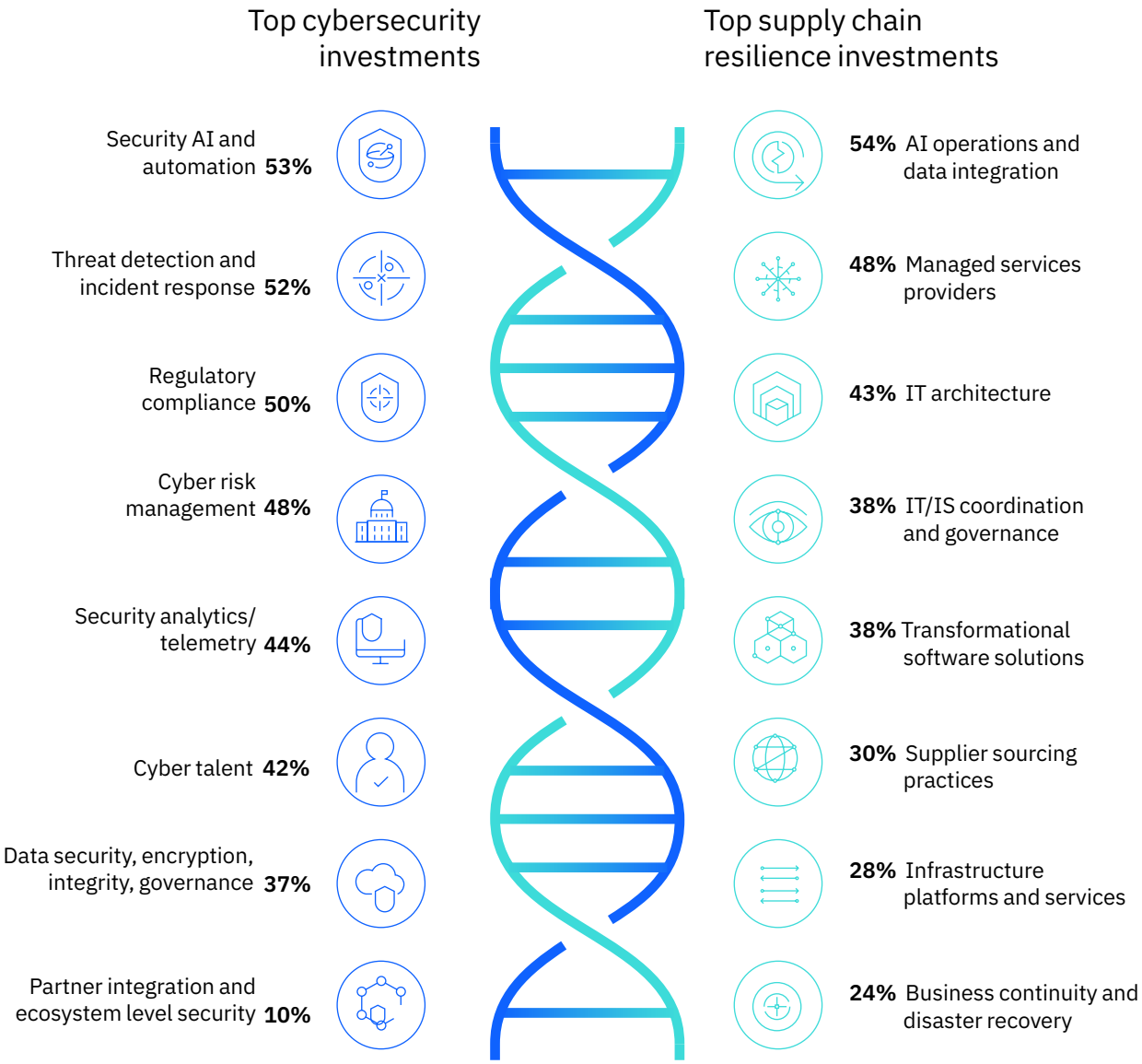



*Q. Specify the senior most executive responsible for physical risks, digital risks, physical supply chain, digital supply chain.*

The majority (84%) of organizations report making moderate to major investments in building a secure connected ecosystem, and in fact, they appear committed to advanced technologies for improving their supply chain and cyber defense capabilities (see Figure 6). AI tops the list of investment priorities for supply chain resilience in both security and operations (see Perspective, “The role of generative AI in securing the ecosystem” on page 15).

FIGURE 6

**Executives are prioritizing advanced technologies for operational resilience, positioning them for improved collaboration.**




*Q. What are your organization’s highest priority cyber investments for improving your supply chain resilience? Q. What are your organization’s highest priority investments for improving your supply chain resilience?*

More than half (54%) report leveraging AI and data integration in operations, which improves efficiency, predictability, and responsiveness across the supply chain. Executives indicate they are also focused on building a more modern, scalable, and reliable IT infrastructure with investments in managed services providers (48%) and IT architecture (43%). Because they are built upon standard design patterns and common governance frameworks, cloud platforms can facilitate greater insights, collaboration, and automation.

For cybersecurity investments, security AI and automation (53%) rank first, followed closely by threat detection and incident response (52%). Adopting AI-powered automation positions organizations to take a more preventive and proactive security posture with improved insights, productivity, and economies of scale.[12] AI-driven operations, in turn, drive the Security Operations Center (SOC) and, increasingly, virtual SOCs through partners.

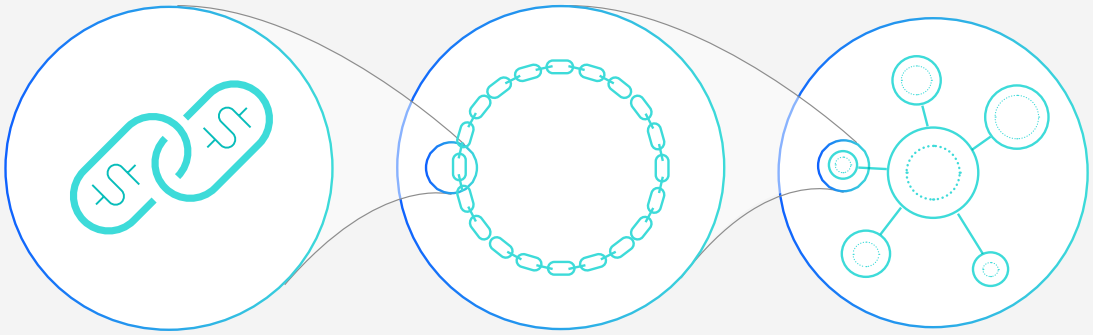
*The true test of a modern operating model is how seamlessly it extends capabilities across the supplier base and out into the ecosystem environment.*

But organizations need to focus more on updating operational governance and support practices versus just investing in new technologies. The true test of a modern operating model is how seamlessly it extends capabilities across the supplier base and out into the ecosystem environment.[13] Applying a shared responsibility model to supply chain security helps as each supply chain participant then contributes to maintaining the integrity and security of the collective security posture—from value chains to supply chains to partner ecosystems (see Figure 7). In this way, the supplier footprint becomes a source of greater resilience, not greater risk.

Leaders are moving in this direction: 58% of executives agree value chains, supply chains, and ecosystems are interrelated and connected. They also recognize the importance of involving partners in risk management: 70% say they improved supply chain resilience by integrating partners into their risk and governance models.

FIGURE 7

**Value chains, supply chains, and ecosystems are evolving in parallel.**



| | Value chains | + Supply chains | + Ecosystems |
|---|---|---|---|
| **Scale** | x1 | x10 | x100 |
| **Emphasis** | Value creation and efficiency | Coordination and fulfillment | Scale and orchestration |
| **Inputs/outputs** | Known and typically don't vary | High-capacity, dedicated, purpose-built | Dynamic; can scale on demand |
| **Direction** | Linear; organized to maximize value-adding activities | Unidirectional; provider supplies customer | Multidirectional; standardized patterns and governance mean intermediaries can add value |
| **Design** | Self-contained but modular | Unilateral; one-party to one-party, often via intermediaries | Multilateral; optimized for complex supplier relationships |
| **Orientation** | Speed, removing friction and waste | Capacity and resilience | Standards and governance to improve efficiency and posture management |
| **Risk** | Contained and mitigated to prevent disruption of value | Transferred; supplier absorbs uncertainties but buyer absorbs impacts | Shared; uncertainties and impacts are distributed wherever possible |

## Action: Strengthen how you share responsibility for supply chain security—both internally and with suppliers.

1. Bring together C-suite leadership to define expectations and allocate resources that support improved cross-functional collaboration for supply chain resilience. Define standards and set expectations for coordination, communication, and governance.
2. Charter teams and assign process owners for investigating how security responsibilities are handled within your organization and across key suppliers. Define standards, policies, and associated controls for maintaining a robust security posture, detailing what is expected from stakeholders, process owners, suppliers, and partners. Determine how these responsibilities should be managed and how oversights can become a source for improvement.
3. Create an inventory of all direct suppliers with access to internal and external systems, services, and data stores. For key suppliers, request they create a map of similar dependencies for their own direct suppliers (your n-party suppliers).
4. As new supplier platforms are deployed, use bid and procurement processes to improve visibility, traceability, and cyber governance practices across your supplier footprint.

*By applying a shared responsibility model to supply chain security, the supplier footprint becomes a source of greater resilience, not greater risk.*

**Perspective**

# How generative AI can help secure your ecosystem

In recent IBM IBV research, 96% of US-based executives surveyed said adopting generative AI makes a security breach likely within their organization within the next three years.[14] Our respondents are more optimistic. Only 39% expect generative AI to pose fundamental risks to the security and resilience of their operations, while 52% say the benefits will outweigh any potential risks (see figure). Just as the technology gives cybercriminals new tools, it can empower defenders with more sophisticated abilities to detect and respond to attacks.[15]

As part of a broader security strategy, generative AI can play an important role in enhancing supply chain resilience. It can expedite supplier assessment and management practices, support simulation and planning for coordinated incident response, automate routine tasks to limit the impact of human error, and provide real-time monitoring of supply chain systems for timely alerts about security issues. As capabilities mature, generative AI will become more action-oriented—writing and remediating code, inspecting code repositories, and helping define and monitor security policies and controls. One study found that generative AI cut completion time for writing code by 35% to 45%.[16]

More than half of respondents (55%) see the potential for generative AI to transform supply chain operations. Leading supply chain use cases where companies are investing in generative AI now or within the next 12 months are operational efficiencies such as resource allocation, risk management (including cybersecurity), and better visibility to improve forecasts and decision-making. Longer-term goals include regulatory compliance and logistics such as robotics, drones, and autonomous vehicles.

**Transforming cybersecurity and supply chain operations, together**

Executives express optimism—and somewhat tempered expectations—for generative AI.

**62%** Generative AI will fundamentally transform cyber risk and cybersecurity capabilities

**55%** Generative AI will transform supply chain operations

**52%** The benefits of generative AI outweigh the risks

**45%** Generative AI will fundamentally change how we approach ecosystem partnerships

**39%** Generative AI poses fundamental risks to the security and resilience of our operations

*Q. Thinking about your organization's strategy over the next 3 years, to what extent do you agree with the following statements about generative AI?*

**Challenge 3:**
**The weakest link**

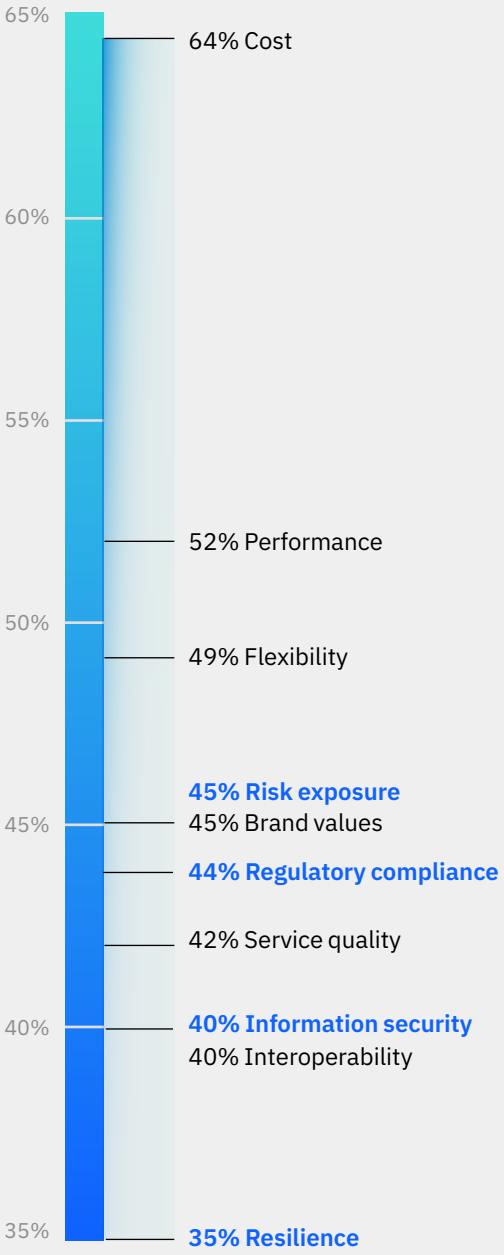
# Many supply chain partners come up short in security hygiene

If a supply chain is only as secure as its weakest link, then partners who do not adhere to an organization's security guidelines leave it vulnerable. Yet for executives interviewed, security hygiene traits are not primary considerations when choosing suppliers. In fact, cost is their top deciding factor by a significant margin—23% more important than risk exposure, information security, regulatory compliance, and resilience collectively (see Figure 8).

However, any financial savings on acquisition costs may be short-lived, as neglecting to consider a supplier's security practices could lead to greater deferred costs in the long run. Over time, limited visibility into risk and resilience can drive up operational support costs, while investments in risk and resilience can reduce them (see Perspective, "How compounding risks can push organizations to the brink" on page 20).

FIGURE 8

**When choosing suppliers, prioritizing cost over risk and resilience factors may be more expensive in the long run.**

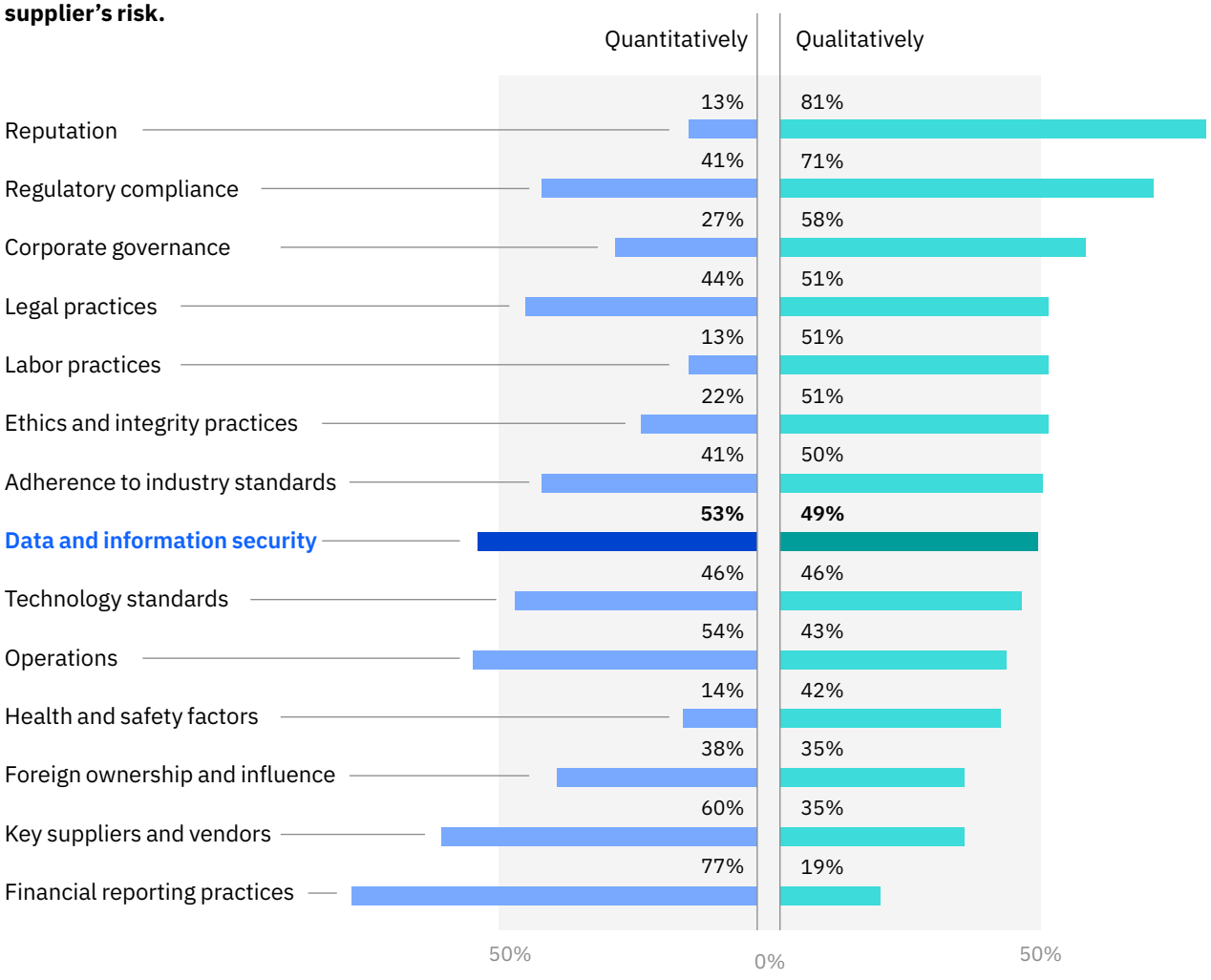



*Q. Which factors are most important when choosing suppliers?*

Even when assessing supplier risk, only about half of respondents include data and information security in their procurement process. This falls well below the leading factors of brand reputation and financial reporting—neither of which offer real visibility into risk management practices (see Figure 9).

FIGURE 9

**Only half of respondents factor in data and information security when assessing a supplier's risk.**

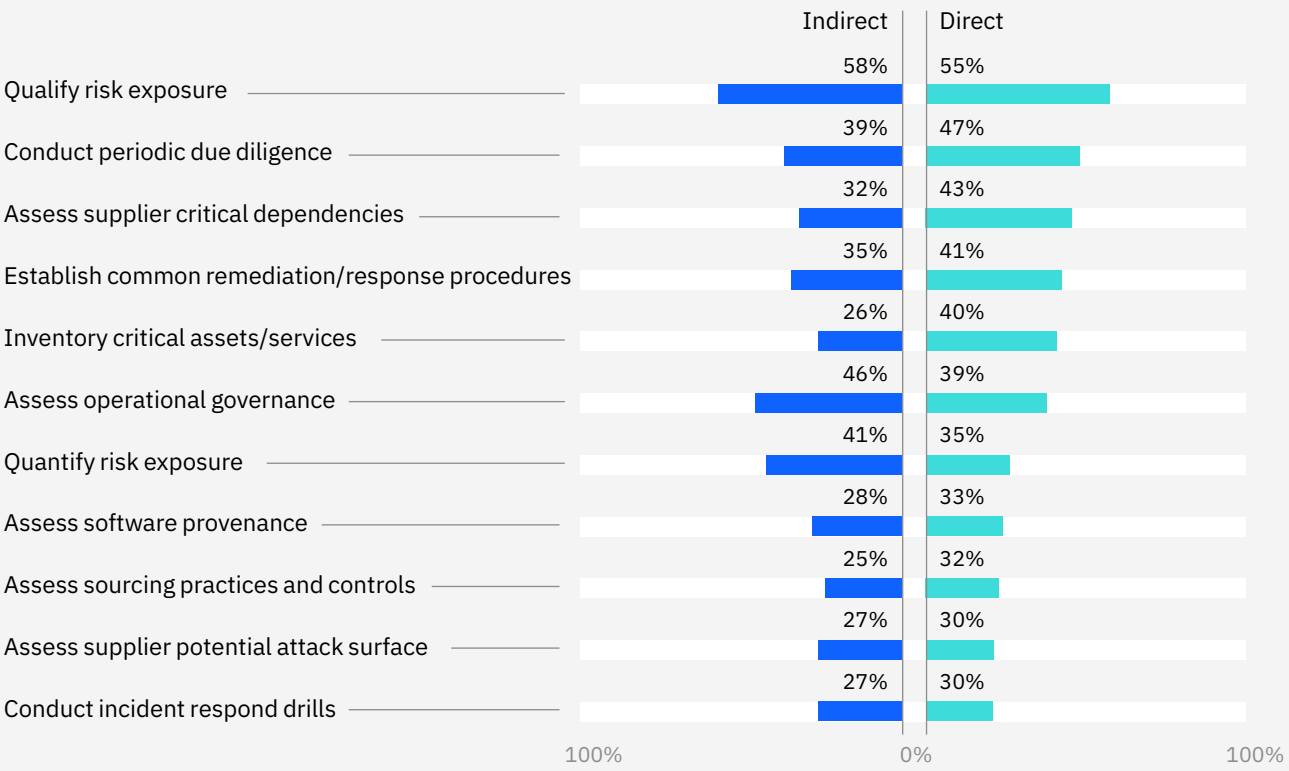



*Q. How does your organization assess potential suppliers for risks (quantitatively)? Q. How does your organization assess potential suppliers for risks (qualitatively)?*

And of greatest concern: respondents indicate their suppliers exhibit low adoption of recommended practices for cyber risk management (see Figure 10). For example, just over half of organizations report qualifying risk posture for both their direct and indirect suppliers. While this is the most common practice, it's still a bare minimum for improving the organization's overall risk posture. When it comes to supplier onboarding, all other assessment practices are being used by less than half of respondents.

FIGURE 10

**Understanding supplier risk exposure: Immature cyber risk assessment practices lead to greater downstream vulnerabilities.**



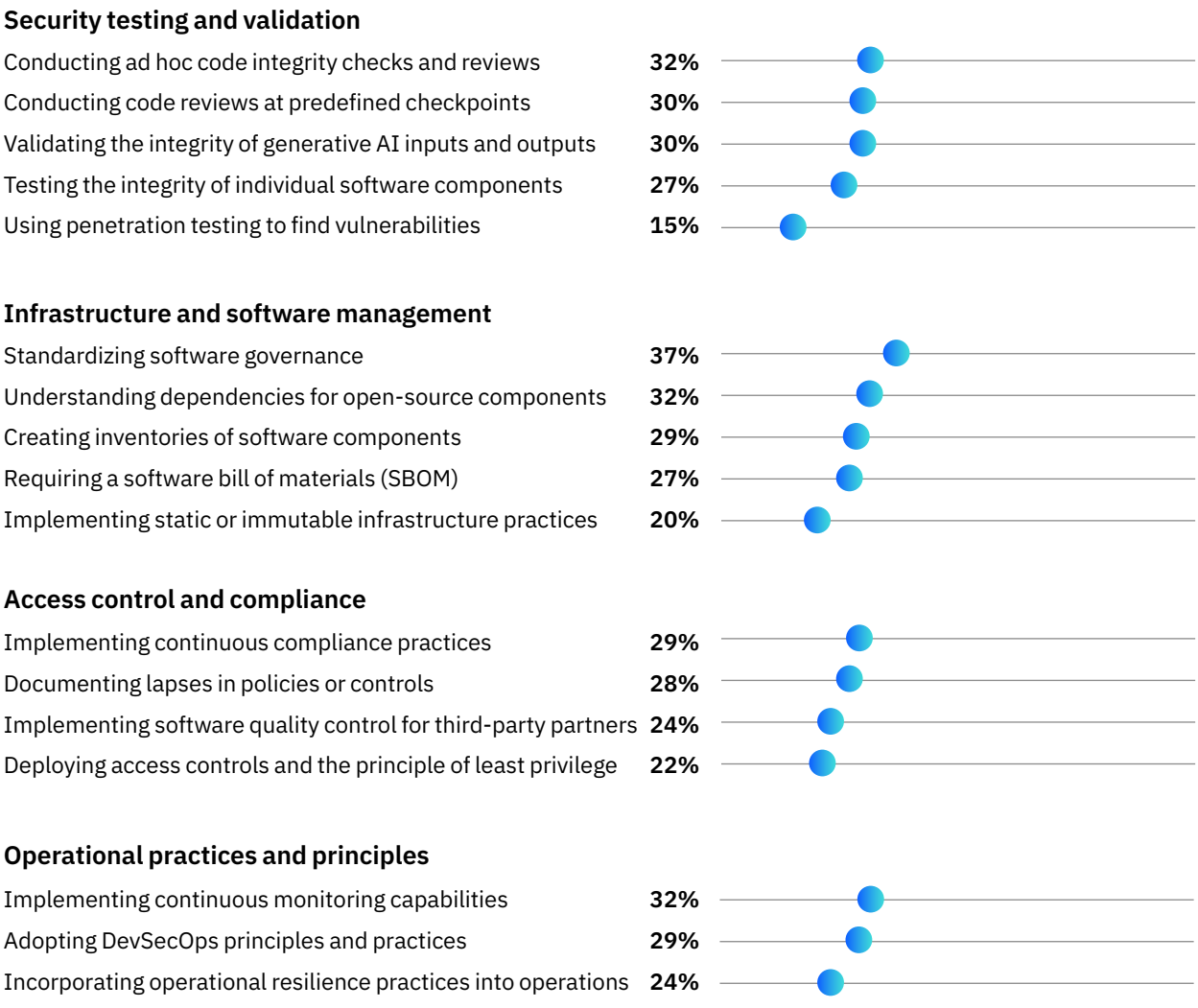

*Q. Which leading practices are routine across your supplier base among your direct suppliers? Q. Which leading practices are routine across your supplier base among your indirect suppliers?*

Our respondents' own software supply chain management practices reflect a similar lack of maturity. While a set of leading practices exists, they are only in the early stages of adopting them (see Figure 11).

Take, for example, access control and compliance measures. Only 22% of respondents indicate they deploy access controls and the principle of least privilege to secure their software supply chain, making them a ripe target for a growing attack method noted by the IBM X-Force threat intelligence group. Recent research showed a significant year-over-year increase (+71%) in the volume of attacks using valid credentials—sold via the dark web—allowing attackers to shift tactics from *hacking in* to *logging in*.[17] Without a strong risk culture that proactively identifies and manages supplier and software vulnerabilities, supply chain resilience will remain elusive.

FIGURE 11

**Respondents are still in the early stages of adopting best practices for software supply chain security.**




*Q. What steps are you taking within your organization to secure its software supply chain?*

**Perspective**

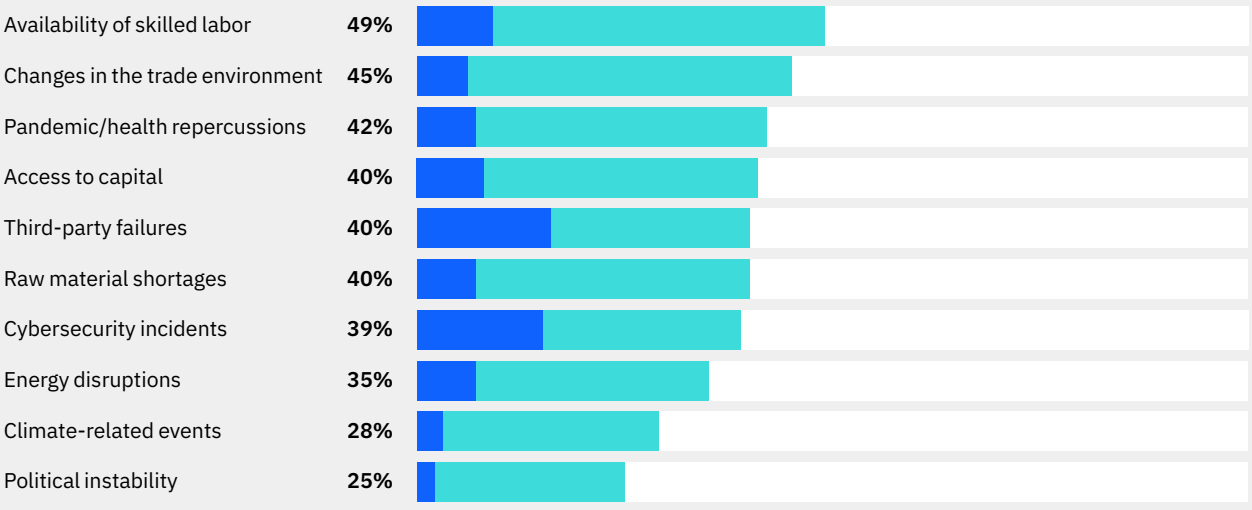
# How compounding risks can push organizations to the brink

Resilience is not simply a matter of vigilance. Operational disruptions are typically a result of complex, follow-on risks that defy standard risk modeling. The past five years made it strikingly clear that risks emerge gradually, then suddenly, as a result of unforeseen combinations of factors—triggering a chain reaction that wreaks havoc up and down the supply chain.[18] Think of a ransomware attack plus a talent shortage. Add in a devastating weather event. Then a shipping route is blocked and requires a lengthy detour.

Given the growing dependency on digital services, risks quickly expand beyond IT/IS domains to disrupt core operations and revenue generation (see figure). Roughly one-third of our respondents have experienced at least significant effects from multiple risk factors—meaning extraordinary steps were required to resolve them. And a smaller but still sizable percentage report experiencing even more severe, lasting disruption.

**As risk factors multiply, compound risk becomes a growing concern.**

Factors impacting operations from 2021-2023




**Severe:** Disruption posed a lasting and material impact to our continuing business operations

**Significant:** Resolution required extraordinary measures and had a noticeable impact on our business

*Q. For the period 2021-2023, what have been the operational impacts associated with the following factors? Percentage of respondents reporting significant or severe impacts.*

As the next decade unfolds and new trade relationships emerge, supply chain operations are likely to see significant changes. Even as organizations shift from complex supply chains to secure, resilient ecosystems, new uncertainties will emerge and new risks will demand greater attention.[19] Of particular concern, we suspect the relatively large percentage of organizations that have experienced significant impacts may be operating at the limit of their capabilities for managing multiple risks. It won't take much to push them into the "severe operational impact" category, where revenue impacts can be monumental.

According to our analysis, the addition of risk factors can snowball unexpectedly into a revenue-destroying avalanche, endangering over 75% of revenue in the most severe cases. Based on respondents' estimates of the impact on revenue from each risk factor shown above, our analysis determined that organizations struggling with managing multiple severe risks must contend with a sobering degree of revenue exposure: from $160.5 million annual revenue-at-risk for smaller organizations to over $22 billion annual revenue-at-risk for larger organizations.

For some organizations, the timing couldn't be worse: the elevated risk environment comes amid growing economic uncertainty. Respondents tell us their average revenue growth plummeted 55% and profits fell 49% over the past three years (for the period 2021-2023).

**The incidence of multiple, severe risks endangers an eye-watering amount of revenue**

| | Estimated revenue-at-risk from factors causing severe impact | | | | | |
|---|---|---|---|---|---|---|
| **Organizational size** | **Low** +1 risk factor | **Average** +1 risk factor | **High** +1 risk factor | **Low** +4 risk factors | **Average** +4 risk factors | **High** +4 risk factors |
| **Average annual revenue $120M–$838M** | $37.0M | $71.0M | $125.6M | $160.5M | $274.6M | $413.3M |
| **Average annual revenue $838M–$5.2B** | $151.7M | $291.0M | $515.8M | $472.9M | $809.3M | $1.22B |
| **Average annual revenue $5.2B–$16.1B** | $648.6M | $1.24B | $2.20B | $2.99B | $5.11B | $7.69B |
| **Average annual revenue $16.1B–$202.5B** | $2.34B | $4.49B | $7.96B | $8.59B | $14.70B | $22.12B |

*Figures are rounded; M = millions USD; B = billions USD*

*Note: Low, average, and high are based on respondents' answers to a set of questions about specific events impacting operations: For the shocks categorized as ''severe,'' what percentage of your organization's revenue was at risk?*

## Opportunity: A strong, shared security culture across direct and indirect suppliers creates greater resilience for all.

Moving forward, organizations need to make security awareness a cultural touchstone, where cyber risk, security, and resilience are emphasized across the entire operations environment. This focus means adopting a holistic approach to the supply chain, the cybersecurity lifecycle, and the IT/IS support ecosystem. To contain risks and vulnerabilities, organizations should be adopting zero-trust principles internally and across their vendor networks. These are practical applications of the secure-by-design approach.

Because new threat vectors may arise at different points in the operations lifecycle, organizations should emphasize an end-to-end approach to cyber risk and cybersecurity—from initial design to sourcing materials to supplier selection to distribution to end user operational support. Our analysis determines that this transformation begins by ramping up the organization's own adoption of software supply chain management best practices, including compliance with the latest regulations, such as those adopted by the auto industry.[20]

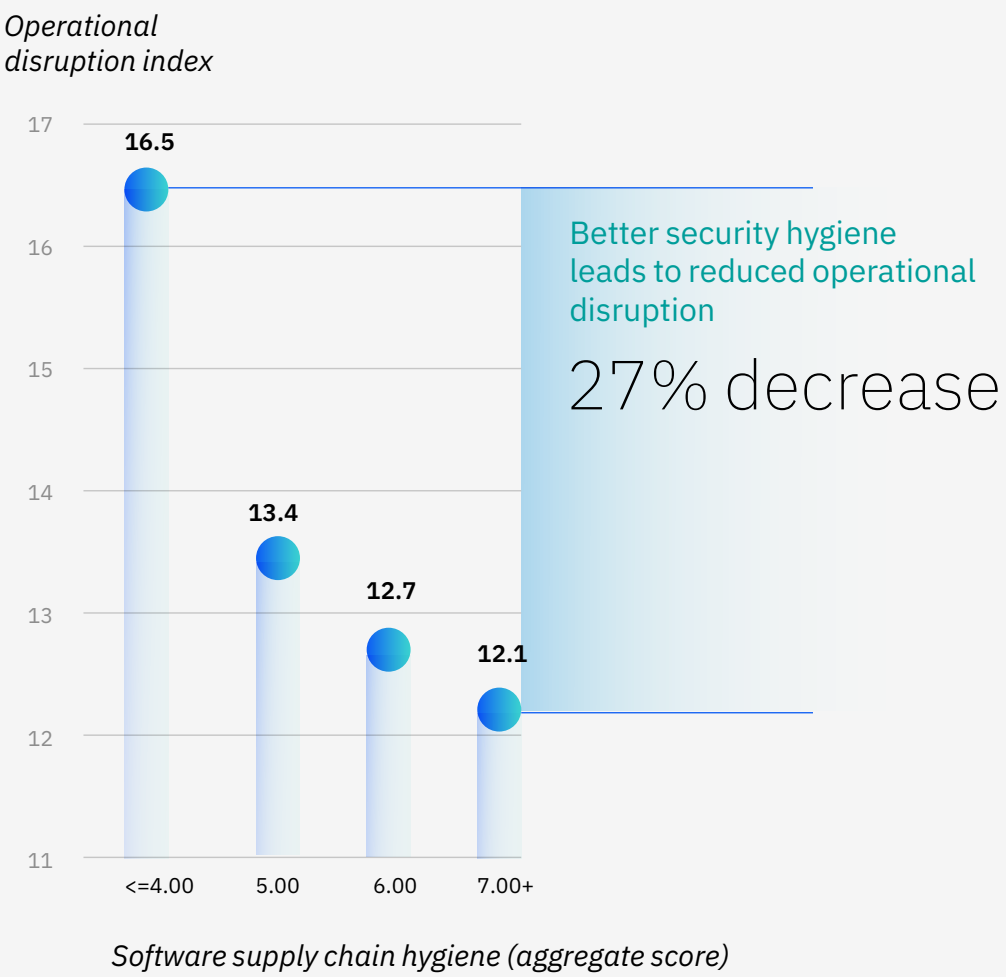
Respondents who are further along in their adoption of these practices are reaping the benefits of strong software security hygiene. These organizations are experiencing a notably lower incidence of operational disruption across their supplier base (see Figure 12).

Second, out of self-interest, leaders must make a point of investing in business partner commitment to risk management and resilience. Broader adoption of supplier assessment, selection, and procurement processes should include an evaluation of security vulnerability controls as well as risk-related performance measures, preferably those focused on criticality and potential revenue-at-risk. This may also include new criteria for software quality and validation.[21]

*To contain risks and vulnerabilities, organizations should be adopting zero-trust principles internally and across their supplier network.*

FIGURE 12

**Organizations with stronger software security hygiene experience a 27% decrease in operational disruption.**

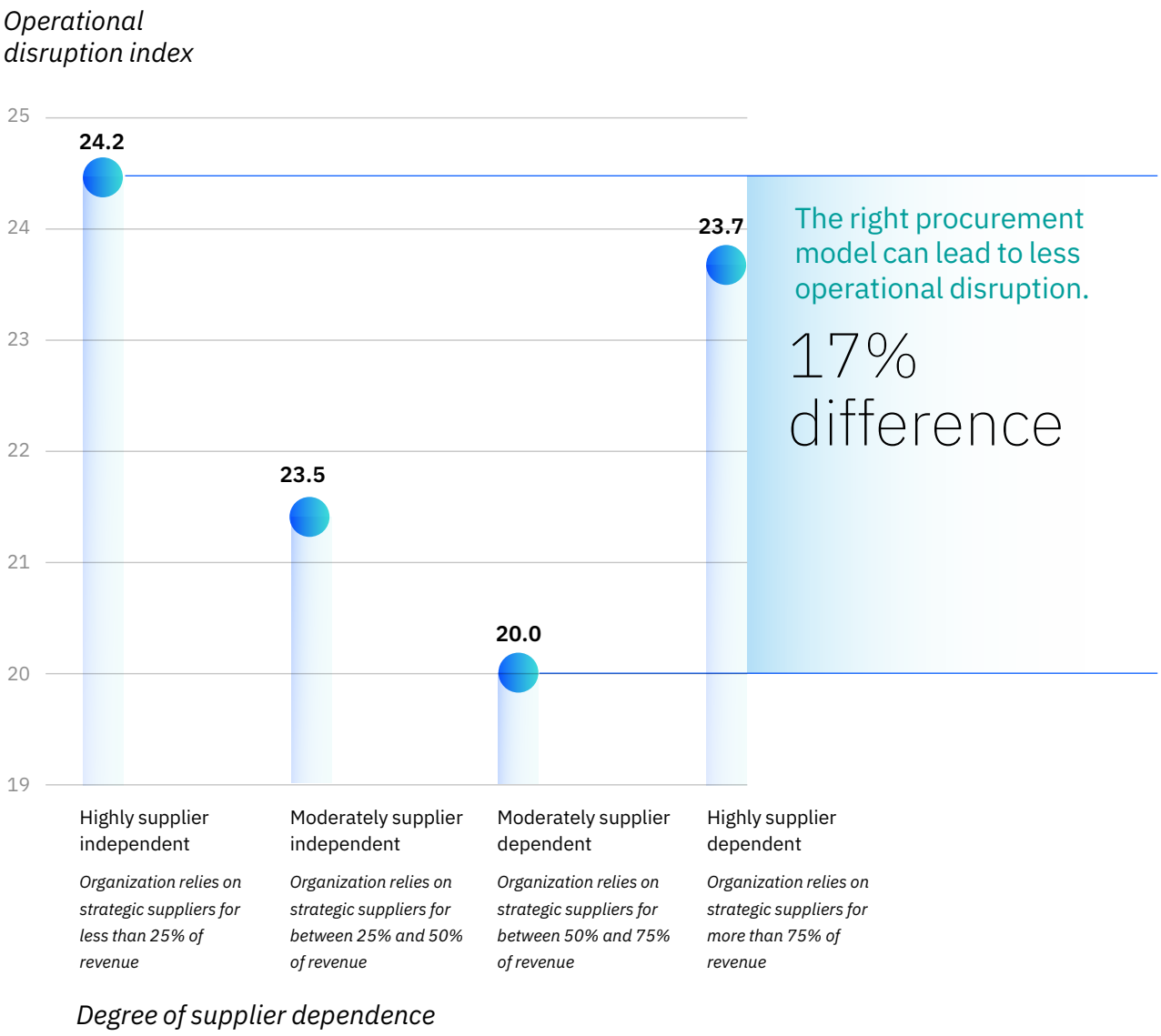



*Based on IBM IBV analysis. The operational disruption index (y-axis) is a composite measure of the organization's propensity for disruption based on a set of common risk factors. The x-axis represents a composite score reflecting the adoption of software supply chain security practices. A higher score represents greater adoption of software supply chain leading practices. This corresponds to a reduced incidence of operational disruption.*

Our analysis also suggests procurement models may play a role in operational resilience. We found moderately supplier-dependent organizations—meaning their strategic supplier relationships account for 50%-75% of revenue—experienced a 17% lower incidence of operational disruption (see Figure 13).

FIGURE 13

**Some organizations are finding a sweet spot within their supplier procurement models for reducing operational disruption by as much as 17%.**




*Based on IBM IBV analysis of responses to "How would you describe your organization's supply chain sourcing model?" The operational disruption index (y-axis) is a composite measure of the organization's propensity for disruption based on a set of common risk factors.*
*A strategic supplier is defined as "a company that provides goods or services that are critical to the success of your business."*

We suspect this is because a moderately supplier-dependent procurement model represents an appealing compromise. Organizations gain the economies of scale, standardization, and governance that come with close partner relationships while retaining some flexibility to avoid vendor lock-in or the concentration of risk associated with a minimal supplier footprint. It's not surprising this happy medium of moderate supplier dependence, mutual investment, and shared responsibility is what a secure, connected ecosystem looks like. For many organizations, this may be the most expedient path to greater supply chain resilience.

*Organizations with moderate supplier dependence are sharing responsibilities efficiently—as integral partners within a secure, connected ecosystem.*

## Action: Make the creation of a strong security culture priority number one.

1. Schedule a workshop to kickstart a security awareness, behaviors, and culture initiative for IT/IS employees and partners.
2. Review and update existing policies to incorporate software supply chain best practices. Set and communicate new procurement standards and implement security controls for leading practices such as supplier security assessments, SBOM governance, software testing, and code quality reviews.
3. Review the US NIST framework on cybersecurity supply chain risk management for leading practices your organization can adopt.[22]
4. Prioritize security-savvy suppliers. To begin, choose three key suppliers and evaluate their core security practices—including whether they have a zero-trust architecture—and their associated performance and service levels. Assess whether contractual terms include compliance with security standards or performance thresholds. Monitor continuing compliance based on periodic security audits.

# Authors


*Kaivan Karimi*

Mobility Partnerships, and
Manufacturing & Mobility OT Security
Microsoft
kaivankarimi@microsoft.com
linkedin.com/in/kaivankarimi/

*Fabio Campos*

Managing Partner, Global Cyber
Strategy & Risk
Cybersecurity Services, IBM Consulting
camposf@us.ibm.com
linkedin.com/in/fabiolcampos/

*Brett Drummond*

Partner, Cybersecurity Services
IBM Consulting
Brett.Drummond@ibm.com
linkedin.com/in/brettdrummond/

*Gerald Parham*

Global Research Leader, Security & CIO
IBM Institute for Business Value
gparham@us.ibm.com
linkedin.com/in/gerryparham/



*Acknowledgments*

Many individuals have contributed to the design of this research and the development of these materials. What you see here reflects the ingenuity and creativity of many talented individuals working together across research design, data analysis, editorial and narrative development, graphic design, subject matter expertise, and sponsorship.

The authors would like to make special acknowledgment for the extraordinary contributions of the following individuals: Joanna Wilkins, Lily Patel, Kristin Biron, Sara Aboulhosn, Nagi Punyamurthula, Richard Hogan, Teresa Suarez, Allie Powell, Evelyn Anderson, Charles Chang, Liam Cleaver, and Dimple Ahluwalia.


## IBM Institute for Business Value

For two decades, the IBM Institute for Business Value has served as the thought leadership think tank for IBM. What inspires us is producing research-backed, technology-informed strategic insights that help leaders make smarter business decisions.

From our unique position at the intersection of business, technology, and society, we survey, interview, and engage with thousands of executives, consumers, and experts each year, synthesizing their perspectives into credible, inspiring, and actionable insights.

To stay connected and informed, sign up to receive IBV's email newsletter at ibm.com/ibv. You can also find us on LinkedIn at https://ibm.co/ibv-linkedin.

## Related reports

**The CEO's guide to generative AI: Cybersecurity**

*The CEO's guide to generative AI: Cybersecurity.* IBM Institute for Business Value. October 2023. https://ibm.co/ceo-generative-ai-cybersecurity

**AI and automation for cybersecurity**

*AI and automation for cybersecurity: How leaders succeed by uniting technology and talent.* IBM Institute for Business Value. June 2022. https://ibm.co/ai-cybersecurity

**Prosper in the cyber economy**

*Prosper in the cyber economy: Rethinking cyber risk for business transformation.* IBM Institute for Business Value. November 2022. https://ibm.co/security-cyber-economy

# Study methodology and approach

To understand how organizations are investing in security capabilities that improve their operational resilience, the IBM Institute for Business Value partnered with Oxford Economics to survey 2,000 executives who are responsible for supplier management, supplier sourcing, and ecosystem partner relationships. Surveys were administered using a double-blind approach, such that respondents did not know which organizations were conducting the survey nor did IBM or Microsoft know the identity of individual respondents.

The survey population consisted of executives in the following roles (or their functional equivalents): senior executives with primary responsibility for ecosystem strategy (CEO, president, Chief Strategy Officer, COO, general manager); CISOs; CIOs; CTOs; Chief Supply Chain Officers; Chief Risk Officers; Chief Procurement Officers; as well as senior executives (Vice President or above) within the information security function, the information technology function, and the supply chain function.

Respondents represented 31 countries across 16 industries: banking, public sector, automotive (OEM and suppliers), chemicals and petroleum (including oil and gas), electronics, industrial products, consumer products, energy and utilities, financial markets, healthcare (providers and payers), insurance, life sciences/pharmaceuticals, telecommunications, retail, transportation, and travel.

Respondents were screened for the following criteria: "Extremely familiar" with their organization's supply chain sourcing and methods, and from organizations that are implementing secure supply chain capabilities "to a significant extent."

Results were analyzed to identify key relationships between security practices and positive business outcomes such as improved operational resilience. Responses were sometimes grouped with similar items in a composite index and then analyzed together to understand more complex phenomena, such as the organization's propensity for operational disruption or the aggregate impact of software supply chain practices.

For estimates of the amount of organizational revenue at risk, calculations were based on the relative financial impact associated with individual risk factors described as "severe." The organization's financial risk exposure from multiple risk factors was derived by summing individual risk factors and then calculating the estimated financial impact based on total organizational revenue. The average estimates are based on the mean values for organizations that fall within the specified revenue quartile distribution. The low estimates are a combination of the individual risk factors with the smallest financial impact. The high estimates are a combination of the individual risk factors with the greatest financial impact.

# Notes and sources


1 Overby, Stephanie. "Cybercrime-as-a-Service: Commoditization Fuels Threat Surge." *Mimecast.* April 18, 2022. https://www.mimecast.com/blog/cybercrime-as-a-service-commoditization-fuels-threat-surge/

2 "Widening Disparities and Growing Threats Cloud Global Cybersecurity Outlook for 2024." World Economic Forum news release. January 11, 2024. https://www.weforum.org/press/2024/01/wef24-global-cybersecurity-outlook-2024/

3 Mills, Karen G., Elisabeth B. Reynolds, and Morgane Herculano. "Small Businesses Play a Big Role in Supply-Chain Resilience." *Harvard Business Review.* December 6, 2022. https://hbr.org/2022/12/small-businesses-play-a-big-role-in-supply-chain-resilience

4 *Close Encounters of the Third (and Fourth) Party Kind.* Security Scorecard and Cyentia Institute. February 2023. https://securityscorecard.com/wp-content/uploads/2024/01/Research-Close-Encounters-Of-The-Third-And-Fourth-Party-Kind.pdf

5 *Cost of a Data Breach Report 2023*. IBM Security and the Ponemon Institute. July 2023. https://www.ibm.com/reports/data-breach

6 "What is a supply chain?" TechTarget. Accessed May 6, 2024. https://www.techtarget.com/whatis/definition/supply-chain; "What is software supply chain security?" Red Hat. Accessed May 6, 2024. https://www.redhat.com/en/topics/security/what-is-software-supply-chain-security

7 "Widening Disparities and Growing Threats Cloud Global Cybersecurity Outlook for 2024." World Economic Forum news release. January 11, 2024. https://www.weforum.org/press/2024/01/wef24-global-cybersecurity-outlook-2024/

8 "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default." Cybersecurity and Infrastructure Security Agency. April 13, 2023. https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf

9 IBM internal case study.

10 Karimi, Kaivan. "The security cultural transformation of the automotive industry." Microsoft blog. October 31, 2023. https://www.microsoft.com/en-us/industry/blog/manufacturing-and-mobility/automotive/2023/10/31/the-security-cultural-transformation-of-the-automotive-industry/; *Coding the Car | Volume 1.* MotorTrend + BlackBerry. 2023. https://www.motortrendgroup.com/coding-the-car-leaders-of-the-software-defined-vehicle/; "WP.29 – Introduction." UNECE Sustainable Development Goals website. https://unece.org/wp29-introduction; *ISO/SAE 21434:2021. Road vehicles: Cybersecurity engineering.* ISO. August 2021. https://www.iso.org/standard/70918.html

11 "Vehicle Manufacturers Need to Know What's Inside Their Supplier's Code." Argus. February 27, 2022. https://argus-sec.com/blog/cyber-security-blog/vehicle-manufacturers-need-to-know-whats-inside-their-suppliers-code/

12 Fisher, Lisa and Gerald Parham. *AI and automation for cybersecurity: How leaders succeed by uniting technology and talent.* IBM Institute for Business Value. May 2022. https://ibm.co/ai-cybersecurity

13 Rajasekharan, Mahesh. "Need A Strategy For Driving Supply Chain Convergence? Think Ecosystem-First." *Forbes*. August 29, 2023. https://www.forbes.com/sites/forbestechcouncil/2023/08/29/need-a-strategy-for-driving-supply-chain-convergence-think-ecosystem-first/?sh=6f1aa4075407

14 *CEO's guide to generative AI: Cybersecurity.* IBM Institute for Business Value. October 2023. https://ibm.co/ceo-generative-ai-cybersecurity

15 Warren, Tom. "Microsoft and OpenAI say hackers are using ChatGPT to improve cyberattacks." *The Verge*. February 14, 2024. https://www.theverge.com/2024/2/14/24072706/microsoft-openai-cyberattack-tools-ai-chatgpt

16 "A coding boost from AI." McKinsey. July 21, 2023. https://www.mckinsey.com/featured-insights/sustainable-inclusive-growth/chart-of-the-day/a-coding-boost-from-ai

17 *X-Force Threat Intelligence Index 2024*. IBM Security. February 2024. https://www.ibm.com/reports/threat-intelligence

18 *RiskN: The Era of Exponential Risk*. Moody's. 2023. https://www.moodys.com/web/en/us/insights/exponential-risk.html

19 Ibid.

20 Karimi, Kaivan. "The security cultural transformation of the automotive industry." Microsoft blog. October 31, 2023. https://www.microsoft.com/en-us/industry/blog/manufacturing-and-mobility/automotive/2023/10/31/the-security-cultural-transformation-of-the-automotive-industry/

21 "What is ASPICE?" APTIV. August 11, 2022. https://www.aptiv.com/en/insights/article/what-is-aspice; "GM Secures Supplier Ecosystem with Coding Standards." *EPSNews*. September 7, 2018. https://epsnews.com/2018/09/07/gm-secures-supplier-ecosystem-with-coding-standards/

22 "Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order." NIST. 2021. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity; "Software Cybersecurity for Producers and Purchasers." NIST. 2022. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-cybersecurity-producers-and

## About Research Insights

Research Insights are fact-based strategic insights for business executives on critical public- and private-sector issues. They are based on findings from analysis of our own primary research studies. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

## The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research, and technology to give them a distinct advantage in today's rapidly changing environment.



IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | May 2024



PNKRGA15-USEN-03