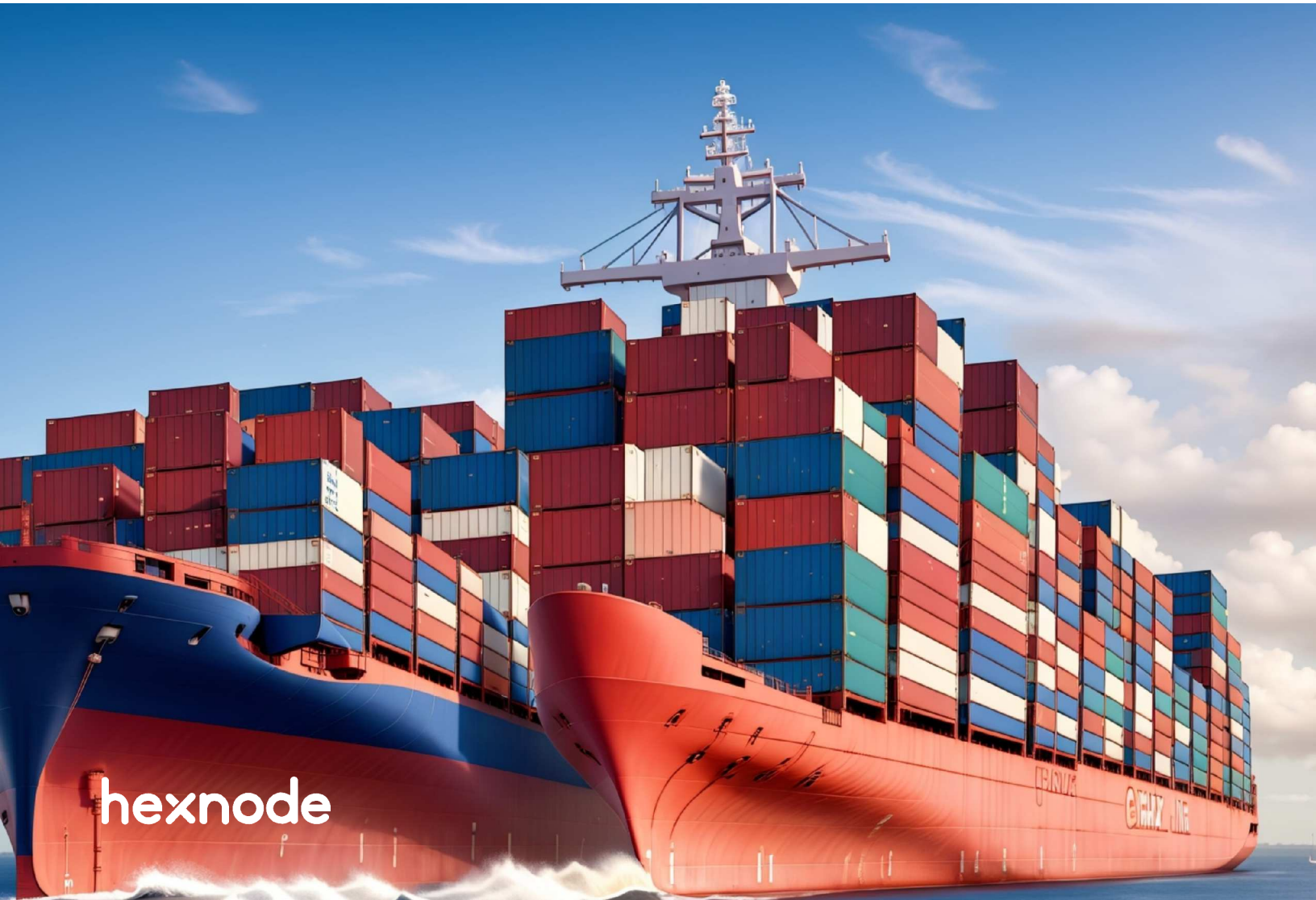
Securing the Supply Chain Sector

Analyzing Security Elements in the Supply Chain:
A Comprehensive Report



Introduction

In an age defined by the transformative power of digitalization across industries, the landscape of supply chain management stands as a prime example of this evolution. Gone are the days of isolated data and opaque processes. Digital tools such as cloud platforms and data analytics provide real-time visibility across the entire supply chain ecosystem. This empowers companies to track inventory levels, monitor every endpoint within the chain, and anticipate potential disruptions, ultimately leading to improved planning and informed decision-making.

However, the increased interconnectedness inherent in this digital age presents a host of challenges. Many businesses still rely on legacy systems, and the process of integrating them with modern digital tools proves to be both complex and financially demanding, requiring substantial investments in infrastructure upgrades and software development. Compounding this challenge is the reluctance of legacy industries to embrace change and the scarcity of skilled professionals capable of driving such transformative initiatives.

Nevertheless, the most critical challenge of all is undoubtedly cybersecurity. As connectivity expands, so do vulnerabilities in security. Every node in the supply chain, reliant on digital systems, becomes a potential entry point for cyber threats, data breaches, and operational disruptions. Consider the case of the Colonial Pipeline hack[1], where assailants exploited a compromised (VPN) password to shut down operations for several days. The attack serves as a reminder that despite having a robust security strategy, the involvement of third-party vendors significantly amplifies risks. Furthermore, the repercussions of these vulnerabilities echo throughout the entire supply chain, impacting production schedules, delivery timelines, and eroding customer trust.

While these challenges are formidable, businesses can unlock the full potential of digitalization within their supply chains by addressing them head-on. Through a combination of technological innovation, strategic investments, and a steadfast commitment to cybersecurity best practices, companies can chart a path toward a future where digitalization not only enhances efficiency and agility but also ensures the integrity and security of the entire supply chain ecosystem.

(1) https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Table of Contents

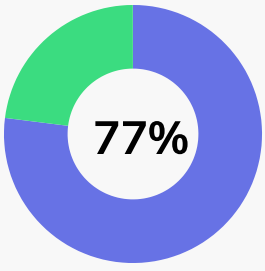
Methodology

Hexnode conducted an independent, vendor-agnostic survey targeting 1000 IT professionals working across small and mid-sized organizations with employee counts ranging from 50 to over 1000 individuals. The respondents, aged 18 years and older, represented various levels of management, including top, mid, and front-line positions. A total of 1000 participants were included in the study, spanning 11 different industry verticals: Automotive, Consumer Packaged Goods, Energy/Utilities/Oil and Gas, Engineering, Healthcare, Manufacturing, Pharmaceuticals, Retail/Wholesale trade, Shipping/Distribution, Transportation, and Food/Beverage. Conducted in December 2023, the survey sought responses based on the respondents' professional experiences.

Key Findings

Employees express skepticism towards their organizations' existing security systems and processes.

- 77% of employees harbour apprehensions regarding cybersecurity threats within their organizations' supply chains, raising concerns over preparedness.
- 42% of organizations remain ill-prepared for cyberattacks due to the lack of a clearly delineated or effective incident response plan.
- 28% of respondents voice reservations regarding the adequacy of their cybersecurity budget.



Employees are concerned about cybersecurity threats in their organizations' supply chains.

Employees lack necessary skills in operating organization's tools and technology effectively.

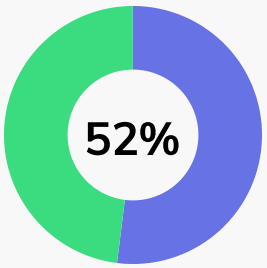
- 41% of employees perceive themselves as only moderately proficient in utilizing the tools and technology within their organizations.

Organizations need to strengthen their third-party risk management programs to safeguard against disruptions in the supply chain caused by attacks on these entities.

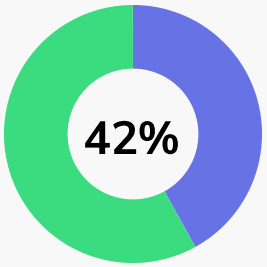
- 52% of organizations have encountered cybersecurity incidents on at least one occasion due to third-party vendors.

Employees report that organizations are exploring investments in emerging technologies like AI and automation; however, challenges persist in implementing these technologies.

- 42% of organizations are planning substantial investments in emerging technologies for streamlined supply chain processes.
- Skills and expertise gaps represent a major challenge impeding the adoption of emerging technologies.



Organizations faced cybersecurity incidents at least once due to third-party vendors.



Organizations plan significant investments in emerging technologies.

Understanding the Supply Chain Landscape

At its core, the supply chain is a dynamic ecosystem comprised of suppliers, manufacturers, distributors, logistics providers, retailers, and consumers. However, the interdependencies within this ecosystem extend far beyond traditional business relationships- they encompass a multitude of interconnected networks and endpoints that collaborate in real time to facilitate the seamless flow of goods, information, and capital across geographical boundaries and time zones.

The digitalization of the supply network has metamorphosized the way the chain operates, enabling stakeholders to leverage tools such as sensors embedded in shipping containers for real-time monitoring of goods' location, temperature, and condition. This industry 4.0 approach empowers businesses to address potential issues such as delays, spoilage, or theft before they escalate. Additionally, cloud-based supply chain management systems offer a centralized platform for coordinating activities among multiple stakeholders, synchronizing communication, while enhancing efficiency, and transparency.

While this interconnectedness offers unprecedented opportunities for efficiency, innovation, and growth, it also presents significant challenges capable of spanning across multiple organizations, systems, and geographies. Shockingly, over 33% of organizations with active supply chains fell victim to cyber-attacks in the past year, with a staggering 62% of these attacks classified as serious. Compounding the issue, nearly 26% of organizations took one to three months to detect these security breaches, underscoring the urgent need for heightened vigilance and proactive security measures.

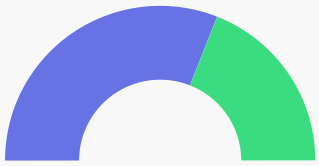
33%

Organizations fell victim to cyberattacks in the past year.

In light of these escalating threats, businesses must strive to gain a deeper understanding of their security landscape and take decisive action to fortify their defenses. It is imperative for organizations to invest in the right mix of internal and third-party technologies and provide comprehensive training to employees to navigate the ever-evolving cybersecurity landscape effectively. Rather than waiting for clients or customers to discover breaches, firms must proactively equip themselves with the necessary tools or enlist the services of third-party security firms to detect and address security incidents swiftly.

> **Encouragingly, employees reported that their internal teams are adept at identifying threats when attacked, with nearly 70% of the security breaches identified by their respective IT departments.**

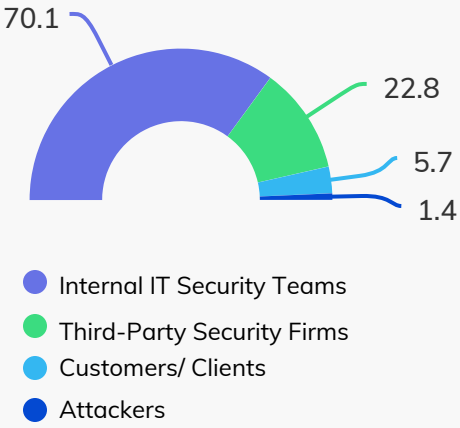
This highlights the importance of cultivating a culture of cybersecurity awareness within organizations. By embracing solutions tailored to their specific technical challenges, businesses can not only mitigate risks and reduce long-term costs but also deliver a tangible return on investment. Furthermore, prioritizing customer satisfaction and loyalty through robust cybersecurity measures can help businesses retain clientele and foster repeat investments.



62%

Attacked organizations faced serious security breaches.

Who identified the attack?



Benchmarking Enterprise IT and Security Dynamics

Traditionally, supply chain management relied heavily on manual processes and fragmented systems, leading to inefficiencies, delays, and increased operational costs. However, the integration of technology within the supply chain has revolutionized the way businesses operate today. From streamlined logistics to enhanced inventory management, sophisticated software solutions have become paramount for enterprises seeking to stay competitive.

Regrettably, these advancements come with their own set of inherent risks and vulnerabilities. In an era where hackers possess the capability to compromise even the most robust security measures, the reliance on technology exposes organizations to potential threats. For instance, in 2023, three vulnerabilities were uncovered in MOVEit, a managed file transfer (MFT) software used for secure data transfer. Exploiting this zero-day vulnerability in MOVEit Transfer, attackers gained unauthorized access to Norton's network, compromising personal information and demanding ransom[2].

Cyber Incident Response Plan (CIRP), also known as Computer Incident Response Plan is formulated by an enterprise to respond to potentially catastrophic, computer-related incidents, such as viruses or hacker attacks. The CIRP should include steps to determine whether the incident originated from a malicious source — and, if so, to contain the threat and isolate the enterprise from the attacker[3].

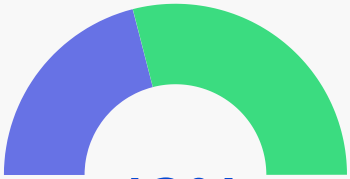
(2) https://securityintelligence.com/news/the-moveit-breach-impact-and-fallout-how-can-you-respond/

(3) https://www.gartner.com/en/information-technology/glossary/cirp-cyber-incident-response-plan

While attacks on supply chains have often been associated with nation-state-sponsored groups aiming for cyber espionage or critical infrastructure disruption, recent incidents underscore a broader risk landscape. Despite the increasing prevalence of supply chain attacks, the survey revealed that 42% of organizations still lack a well-defined or effective incident response plan.

The modern supply chain relies heavily on advanced technologies and digital infrastructure, ranging from RFID tags and GPS tracking systems to cloud-based platforms and blockchain technology. This interconnected web of networks and devices operates on a global scale, facilitating the monitoring, tracking, and optimization of goods throughout the supply chain. On a good note, while 58% of organizations have diligently implemented firewalls and intrusion detection/prevention systems to safeguard their networks, a concerning 4% overlook the importance of regularly auditing their endpoints. Furthermore, 33% of organizations lack strict endpoint policies, with over 4.2% lacking endpoint policies altogether.

The supply chain sector is in a constant state of flux, blurring the lines between physical and digital channels. The proliferation of e-commerce and omnichannel retailing further complicates the threat landscape. While these developments present both challenges and opportunities, businesses must innovate and adapt to meet evolving demands. The fact that 77% of employees still express concerns about the cybersecurity measures implemented by their organizations cannot be overlooked.



42%

Organizations lack effective or well-defined Incident Response Plan (IRP).

33% Organizations lack strict endpoint policies.

77%

Employees express concerns about cybersecurity measures implemented by their organizations.

A Study on Staff Sentiments

Amid the backdrop where technology and automation are increasingly prevalent, the human element remains an indispensable driver that demands more attention than ever before. While technology presents a wealth of advantages, skilled professionals provide adaptability and creativity that machines cannot replicate. As it goes, the role of employees in upholding robust cybersecurity measures cannot be overstated.

> **Through negligence or lack of awareness, human error can inadvertently expose organizations to vulnerabilities, rendering them susceptible to cyber attacks.**

Whether succumbing to phishing scams, clicking on malicious links, or unwittingly divulging sensitive information, employees can inadvertently become weak links in the cybersecurity chain. Hence, fostering a culture that actively engages employees in the cybersecurity management process is imperative. Regrettably, nearly 30% of employees encounter challenges in receiving adequate IT assistance when issues arise.

While ensuring employee commitment to best security practices is paramount, it is equally imperative for organizations to exhibit adherence to cybersecurity protocols.

30%

Employees encounter challenges in receiving adequate IT assistance.

> **Alarmingly, 40% of respondents report that their organizations are not diligent in regularly updating or patching their systems. Furthermore, 35% of employees observe that their organizations only adhere to basic password policies for convenience, with approximately 6% lacking a password policy altogether.**

While these figures may appear insignificant, neglecting fundamental protocols can have far-reaching consequences. A single compromised password can grant malicious actors unrestricted access, from data theft to compromising critical business systems. In fact, close to half (49%) of incidents documented in Verizon's 2023 Data Breach Investigations Report[4] were linked to compromised passwords.

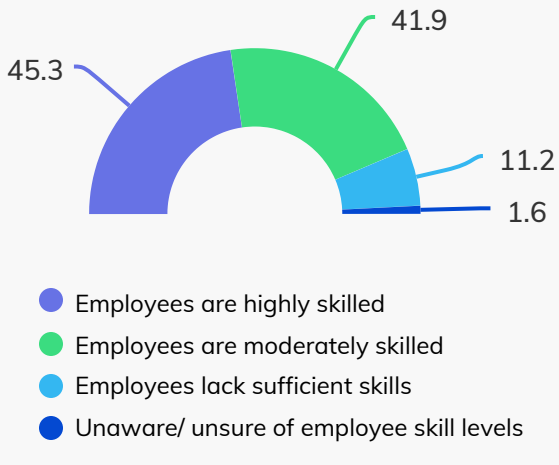
In addition to upholding cybersecurity protocols, it is essential to ensure that employees have a comprehensive understanding of their organization's security architecture. Despite 84% of employees acknowledging the high importance placed on endpoint security, a disappointing 33% of organizations, in fact, lack strict endpoint compliance policies. With a diverse array of endpoints permeating the supply chain ecosystem, including handheld barcode scanners, RFID readers, and GPS-enabled tablets, organizations must develop robust strategies to address non-compliant devices. Encouragingly, some employees have highlighted the implementation of endpoint management technologies by their organizations. These technologies ensure that configurations are promptly updated when devices fall out of compliance, and compromised devices are isolated and wiped as needed.

To attain the desired level of threat mitigation, organizations must foster a culture of cybersecurity awareness and employee engagement. This involves delivering comprehensive training and education programs to augment employees' comprehension of cybersecurity threats, best practices, and their pivotal role in safeguarding sensitive data. However, with 28% of employees deeming the cybersecurity budget insufficient and 41% expressing only moderate proficiency in utilizing assigned tools and technology, there is a pressing need to empower employees with the knowledge and skills to identify and address potential threats effectively. As employees reach the required expertise, organizations will be able to diminish the likelihood of security breaches substantially.

28.2%

Employees deem cybersecurity budget insufficient.

Employee Skillset with Tools and Technology



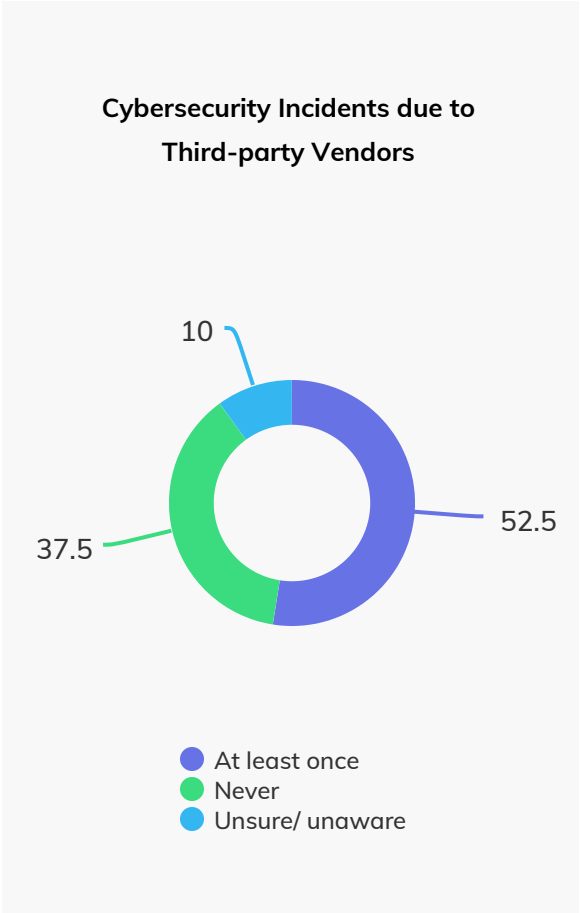
(4) https://www.verizon.com/business/en-nl/resources/reports/dbir/

Significance of third-party vendor risks

Supply chain attacks are compounded by the intricate network of relationships between organizations and their third-party service providers. A significant portion, at least 52% of organizations, has encountered cybersecurity incidents stemming from third-party vendors on at least one occasion. Malicious actors can infiltrate the target organization by exploiting a trusted component or software within the supply chain, circumventing traditional security measures, and catching victims off guard. The recent Okta breach of 2023[5] is a glaring example of third-party risk. In this instance, a hacking group executed a supply chain attack targeting Okta's customers rather than Okta itself, exposing several financial institutions, including Western Union, Ally, and Amalgamated Bank, to potential threats.

Given the potential for lax cybersecurity frameworks and controls among third-party vendors, which can pose significant risks to organizations, what can be done to minimize that risk?

A critical step is to comprehensively understand your company's relationship with third-party vendors through robust third-party risk management (TPRM) programs.



(5) https://techcrunch.com/2023/11/29/okta-admits-hackers-accessed-data-on-all-customers-during-recent-breach/

This entails analyzing the potential risk that might be introduced to your organization when utilizingthird-party services, engaging with vendors to assess their security posture, and remediating any identified risks. It may be necessary to withhold deployment until security issues are remediated. Following remediation efforts, your organization can determine whether to onboard the vendor or seek alternative options based on your risk tolerance, vendor criticality, and compliance requirements. If anything, keeping an eye on your vendor after onboarding is even more important, as they will have access to internal systems and sensitive data to deliver their services. Alarmingly, over 15% of businesses bypass the TPRM process, indirectly exposing themselves to potential organizational threats.

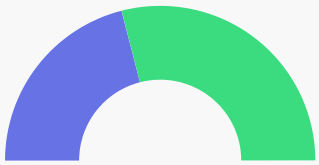
15%

Businesses bypass TPRM processes

Embracing Supply Chain 2.0

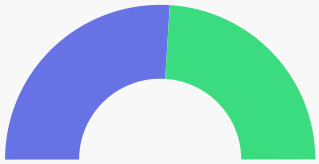
Transitioning from a linear model reliant on disjointed systems, Supply Chain 2.0 embodies a paradigm shift towards a more interconnected, data-driven, and customer-centric approach. With evolving customer expectations driving the need for greater agility, efficiency, and resilience, Supply Chain 2.0 embraces digital technologies like IoT devices, blockchain, and artificial intelligence to create a cohesive network of systems and stakeholders. This digitization enables real-time visibility, data-driven decision-making, and seamless collaboration across the entire supply chain ecosystem. Currently, more than 32% of organizations are extensively leveraging IoT devices such as GPS trackers, sensors, and barcode scanners for supply chain tracking, with an additional 42% planning significant investments in emerging technologies to streamline supply chain processes.

However, as businesses strive to gain a competitive edge in today's dynamic market environment by adopting new technologies, challenges abound. Approximately 52% of organizations encounter obstacles when integrating advanced technologies. Skill shortages in critical areas like data analytics, AI, and digital literacy, alongside budget constraints, pose significant hurdles to effectively embracing newer technology. Of particular concern are data security and privacy issues, which stand out as primary challenges. As supply chain networks become increasingly interconnected and data flows across multiple touchpoints, the risk of cyber threats, data breaches, and unauthorized access escalates.



42%

Organizations plan significant investments in emerging technologies.

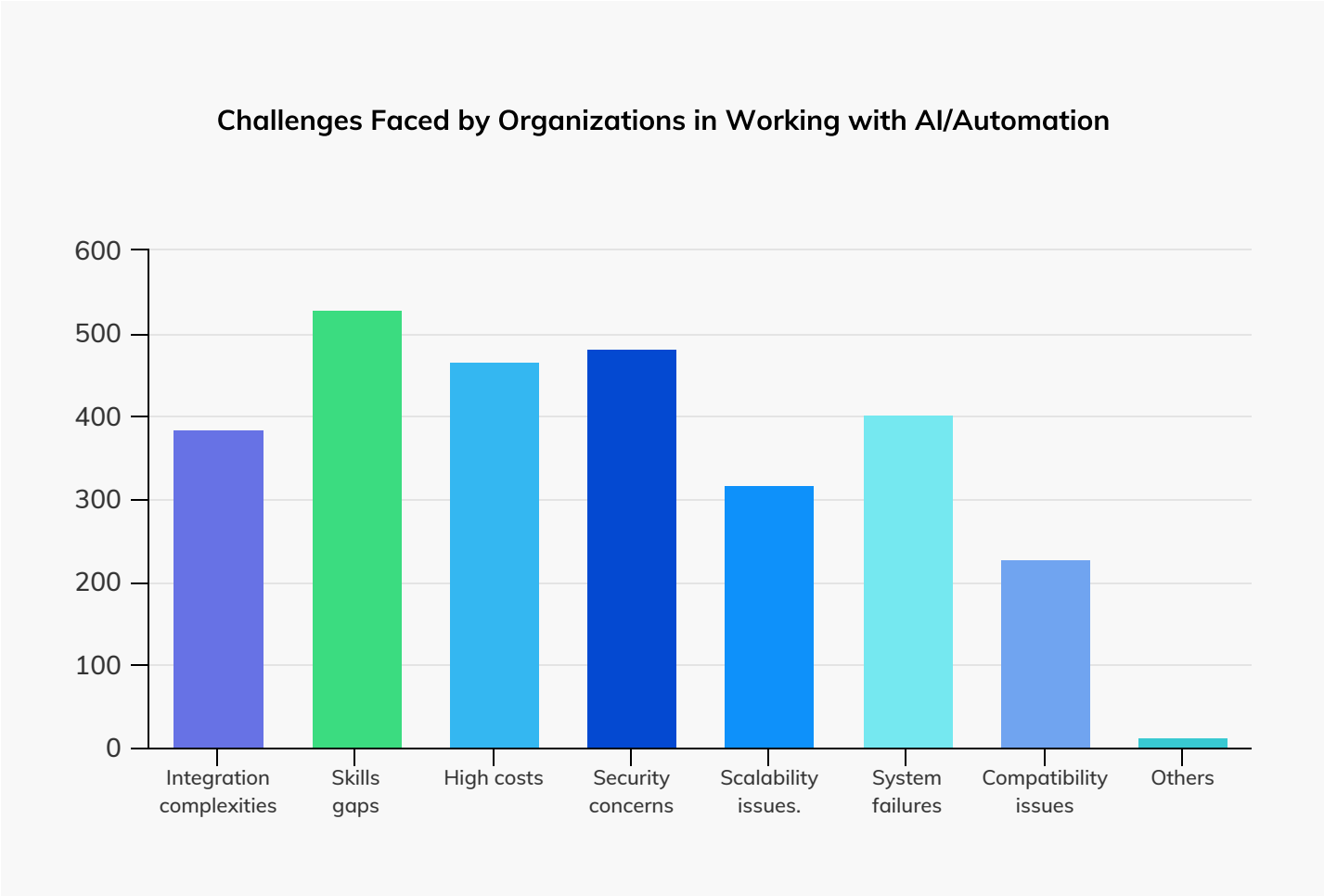


52%

Organizations encounter obstacles when integrating advanced technologies.

Protecting sensitive information, ensuring compliance with regulations such as the General Data Protection Regulation (GDPR), and safeguarding against cyber attacks demand robust cybersecurity measures, comprehensive employee training, and vigilant risk mitigation strategies.

Despite these challenges, the promise of Supply Chain 2.0 for transforming logistics operations and driving competitive advantage remains substantial. Through strategic planning, investment, and proactive measures, organizations can overcome hurdles and unlock their full potential.



Next Steps

Investments in technology have surged in recent decades, surpassing other areas of investment. However, despite this significant influx of capital, the returns have remained relatively stagnant. This underscores the importance of reassessing investment strategies. Instead of simply pouring funds into technology solutions, investing in the right technology that aligns with the evolving demands of the supply chain landscape is imperative.

Chief Supply Chain Officers (CSCO) on a global scale should develop a strategic roadmap with the future of supply chain in mind. As businesses increasingly embrace new technologies and delegate decision-making authority to technology-driven processes, they face a parallel challenge in navigating potential threats.

> **By investing in appropriate technology solutions, organizations can better position themselves to address future challenges effectively.**

Along with the necessity of investing in the right technology, the survey highlights the importance of acquiring the necessary skills and expertise to leverage technology effectively. Even in an era of hyper-automation, the human element remains indispensable for its inherent creativity and cannot be overlooked.

Additionally, organizations must prioritize technology solutions that offer scalability and flexibility. For instance, those who previously invested in endpoint management technology capable of IoT management would have been well-prepared when IoT emerged as a dominant force in the supply chain industry. With these insights, organizations can adopt agile supply chain strategies to swiftly respond to market fluctuations, meet evolving customer demands, and navigate unforeseen disruptions.

Hexnode stands as a prominent vendor in the realm of unified endpoint management, offering expertise in deploying tailored technology solutions to meet diverse business needs. To explore how Hexnode can empower your organization to deliver optimal experiences while ensuring maximum resilience, contact our expert team today.

About Hexnode

Hexnode, the enterprise software division of Mitsogo Inc., was developed with the mission of helping enterprises manage their device fleet. Recognizing the value of corporate data and witnessing the emergence of BYODs, COPEs, and COBOs, the award-winning Unified Endpoint Management (UEM) solution has been in an endeavor of introducing intelligent technologies to safeguard devices against threats and thefts. It offers full mobility management software compatible with all major platforms, including Android, Windows, iOS, macOS, Fire OS, and Apple TVs.

Disclaimer

This survey report is based on responses collected from participants and is intended solely for informational purposes. The accuracy and reliability of the information rely on the honesty of the respondents. The results of this survey may also not be fully representative of the entire population due to factors such as sample size, demographics, and respondent self-selection. This report does not constitute professional advice, readers should consult with relevant experts or conduct further research before making decisions based on the content presented.

To Learn More:

For additional information on how Hexnode can help organizations secure their supply chain, click here.

For Hexnode's resources, click here.

To find out how Hexnode can help you with your endpoint management investment, contact us at sales@hexnode.com.

hexnode

Mitsogo Inc., United States (HQ), 111 Pine St #1225,

San Francisco, CA 94111

Tel: +1-415-636-7555 (Intl.), Fax: +1-415-646-4151(Intl.)