



# SUPPLY CHAIN CYBERSECURITY REPORT 2022

**WHY CYBERSECURITY HAS NEVER BEEN MORE  
IMPORTANT FOR THE SUPPLY CHAIN SECTOR**

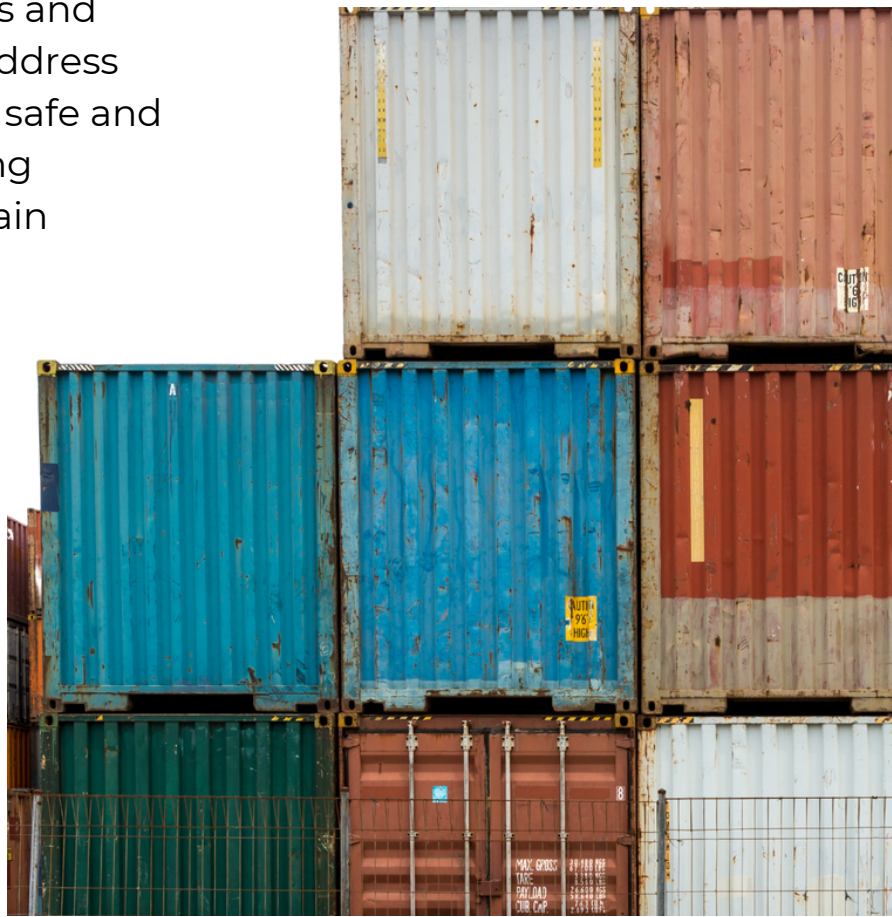
**BROUGHT TO YOU BY:**  
NINJIO Cybersecurity Awareness Training



## EXECUTIVE SUMMARY

Global supply chains have been under immense pressure over the past two years, from massive disruptions caused by the pandemic and war to high costs for raw materials and shipping. As if these crises weren't enough, cyberattacks on supply chains have been surging as well – a threat that will persist even as inflation cools and geopolitical tensions stabilize.

The digital transformation of the supply chain sector has opened a vast range of attack vectors for cyber criminals, hostile governments, and other threat actors to exploit. This is why companies in the supply chain sector have to establish proactive cybersecurity awareness platforms. Many of the largest supply chain cyberattacks in history involved a human element – from compromised credentials to malware downloaded onto a single device. When employees are informed about cyber threats and capable of taking action to address them, they'll keep the sector safe and help the world avoid the rising economic costs of supply chain disruptions.





Over the past two and a half years, global supply chains have faced a series of daunting challenges: snarled ports and empty warehouses, soaring freight costs, and economic turmoil have led to higher prices for goods, delivery delays, and significant tension between supply chain partners. These problems are compounded by the fact that supply chains are also attempting to navigate a uniquely dangerous threat landscape as cyber criminals, governments, and a wide range of other malign actors increasingly target the sector.

Cyberattacks on supply chains can bring economic activity to an abrupt halt, which is the last thing consumers and companies need when inflation remains high and recession fears persist. There are many reasons supply chain leaders are increasingly focused on cyber resilience – they recognize that the destructive capacity of cyberattacks has never been greater, while cyber criminals and hostile governments are especially focused on supply chains. This is because supply chains are vulnerable and lucrative targets due to their critical role in facilitating commerce and the growing number of attack vectors for hackers to exploit.

The supply chain sector is undergoing a sweeping digital transformation, which provides cyber criminals with ample opportunities to infiltrate companies through an expanding array of attack vectors. This is why supply chain cybersecurity platforms have to be agile and adaptive – they should be able to keep up with evolving cyber threats and ensure that all attack vectors are covered at all times. There's no better resource for building this type of resilience than a cyber-aware workforce. Every employee can do their part to keep your supply chain safe when they've been equipped to observe cybersecurity best practices, identify threats as they arise, and take action to neutralize those threats.

# CYBERSECURITY IS NECESSARY FOR SUPPLY CHAIN RESILIENCE

Supply chains around the world have confronted crisis after crisis over the past several years, exposing many fundamental weaknesses in how supply chains operate – so it's no surprise that resilience has become a key priority among leaders in the sector. According to a McKinsey survey of supply chain executives, 93 percent say they're taking steps to make their supply chains more resilient. Cybersecurity should be a core focus of this process, as cyberattacks have proven to be among the most disruptive forces supply chains face.

**"COMPANIES WILL NEED TO STEP UP INVESTMENT IN CYBERSECURITY TOOLS AND TEAMS."**

The McKinsey report argues that "cyberattacks are a growing concern" and observes that "companies will need to step up investment in cybersecurity tools and teams."

Researchers note that the increasing reliance on digital systems within the supply chain sector makes companies more vulnerable to cyberattacks, and they list this issue as one of the most pressing threats the sector needs to address. McKinsey explains that "hypothetical shocks like a global military conflict or a systemic cyberattack ... would dwarf the most severe shocks experienced to date."



Gartner reports that just 21 percent of supply chain leaders believe their networks are “highly resilient.” Companies can improve this status quo by ensuring that every link of the supply chain is protected from cyber threats, which means implementing a comprehensive cybersecurity awareness solution across the company – and working with partners to do the same. Many of the attack vectors hackers use to infiltrate supply chains fall under the purview of employee cybersecurity awareness, such as insecure networks (which employees are particularly reliant upon in the era of remote work), IoT devices with limited cybersecurity functionality, and malware in phishing emails. Because today’s supply chains are highly interconnected, a threat to one partner (a third-party vendor, for instance) constitutes a threat to the entire supply chain. This is one of the reasons 90 percent of supply chain professionals say visibility technology is a high priority – companies need to know what’s going on across the supply chain at all times, and this is particularly important when it comes to the state of their cybersecurity.



# 60% OF SUPPLY CHAIN LEADERS CONSIDER INABILITY TO RESPOND TO TECHNOLOGICAL CHALLENGES A MODERATE OR MAJOR RISK

Cybersecurity is a prerequisite for supply chain resilience, and it's only going to become more important as the (long overdue) digital transformation in the sector picks up momentum. As a recent BDO report explains: "Digital transformation is breaking down the traditional barriers that can stymie innovation and collaboration, but in doing so, it creates more opportunities for threat actors to break in, thus exponentially increasing supply chain cyber risks." PwC recently found that 60 percent of supply chain leaders consider the "inability of suppliers to respond to technological challenges" a moderate (41 percent) or major (19 percent) risk. A central technological challenge is how to keep supply chains safe at a time when cyber criminals have more reasons than ever to attack them.

Companies in the supply chain sector have never been more cognizant of their vulnerabilities. While this is an unnerving time for supply chain professionals, it should also be a moment of clarity. Despite the scale of the disruptions supply chains have experienced over the past several years, future disruptions could be even more crippling. One of the primary reasons for this alarming state of affairs is the fact that cyberattacks on supply chains are becoming more frequent and damaging. This is why companies should build cybersecurity into every link of their supply chains to make their operations as resilient as possible.



# SUPPLY CHAINS FACE MORE CYBER RISKS THAN EVER

---

Many factors have come together to increase the likelihood of a cyberattack on your supply chain. As the number of attack vectors has risen dramatically, cyber criminals, belligerent governments, and other threat actors have been targeting supply chains more actively. These cyber threats are becoming more severe when supply chains are already in crisis – a May 2022 report published by Accenture found that supply chain disruptions have led to a loss of €112 billion (0.9 percent of GDP) in the eurozone alone. Depending on the effects of the war in Ukraine, these losses could climb to €920 billion (7.7 percent of GDP) next year.







# SUPPLY CHAIN CYBERATTACKS INCREASED BY 51% BETWEEN JULY AND DECEMBER 2021

A recent [report](#) from NCC Group found that supply chain cyberattacks increased by 51 percent between July and December 2021, while less than a third of cybersecurity decision-makers said they were “very confident” that they could respond to one of these attacks quickly and effectively. Companies are clearly aware that this is an unacceptable level of risk – respondents said they were planning to increase their cybersecurity budgets by an average of 10 percent in 2022. According to the 2022 Verizon Data Breach Investigations [Report](#) (DBIR), supply chain attacks “increased dramatically” over the preceding year. “From very well publicized critical infrastructure attacks to massive supply chain breaches,” the report states, “the financially motivated criminals and nefarious nation-state actors have rarely, if ever, come out swinging the way they did over the last 12 months.”



The global integration of supply chains has introduced an extremely high level of third-party risk. As the National Institute of Standards and Technology (NIST) [explains](#), among the top supply chain risks are “Third party service providers or vendors – from janitorial services to software engineering – with physical or virtual access to information systems, software code, or IP.” NIST also cites “third party data storage or data aggregators” as potential attack vectors. One of the reasons [90 percent](#) of supply chain leaders say they’re pursuing regionalization over the next three years is the fact that they’re concerned about third-party risks posed by geographically distributed partners. DBIR researchers emphasize the “interconnected nature of real-world environments when discussing Supply Chain and third-party breaches.”

## TOP SUPPLY CHAIN RISKS



SERVICE  
PROVIDERS/VENDORS



PARTNERING  
COMPANIES



DATA STORAGE/  
AGGREGATORS

One of the most significant supply chain disruptions on record was caused by the [NotPetya](#) ransomware attack in 2017. NotPetya was part of a Russian cyber assault on Ukraine – part of a long-running online conflict between the two countries that continues now, as Russia [continues](#) to launch cyberattacks on its neighbor since invading in early 2022. Supply chains are especially vulnerable in an era of cyberwarfare, as they’re essential for sustaining critical infrastructure – a key target for governments and state-affiliated actors that are trying to inflict as much damage as possible with a cyberattack.

FOR MORE INFORMATION ABOUT HOW TO KEEP YOUR  
COMPANY SAFE FROM STATE-SPONSORED CYBERATTACKS, SEE  
[HERE](#) AND [HERE](#).

Supply chain monitoring and logistics operations are heavily dependent on digital systems that can be shut down or disrupted. Ninety-five percent of supply chain leaders say they have formal supply chain risk management processes in place, while 59 percent adopted new processes over the preceding year. Cybersecurity should be an integral part of any supply chain's risk management strategy, but this strategy can't be constrained within the four walls of your company. It isn't just vital to generate stakeholder support for the development of a robust cybersecurity platform among your own employees – you have to do the same with your partners. As the DBIR observes:



**“ONE KEY SUPPLY CHAIN BREACH CAN LEAD TO WIDE-RANGING CONSEQUENCES.”**


However, over one-third of companies say they don't regularly monitor their suppliers' cybersecurity arrangements.

There's no question that we will continue to see devastating cyberattacks on global supply chains in the coming years. Now that companies are well aware of this trend, they have to take immediate action to build up their defenses – and this begins with the creation of a cyber-aware workforce.




# HOW CYBERSECURITY AWARENESS CAN PROTECT SUPPLY CHAINS


One of the most persistent trends in cybersecurity is the role of human beings in keeping organizations safe. The 2022 DBIR [reports](#) that 82 percent of breaches involve a human element: “Whether it is the use of stolen credentials, phishing, misuse, or simply an error,” the researchers write, “people continue to play a very large role in incidents and breaches alike.” There are constant reminders of the importance of cybersecurity awareness in preventing major supply chain attacks. Consider these examples:



NotPetya [infiltrated](#) the shipping giant Maersk’s systems through a single infected computer. As a *Wired* [article](#) about the attack explained, a “finance executive for Maersk’s Ukraine operation had asked IT administrators to install the accounting software M.E.Doc [the vehicle for the NotPetya malware] on a single computer. That gave NotPetya the only foothold it needed.”



Hackers [breached](#) Colonial Pipeline with a single compromised password. According to the DBIR, the use of stolen credentials and ransomware were the top two “action varieties in third-party incidents.”



SolarWinds [blamed](#) a “compromise of credentials and/or access through a third-party application” for the major cyberattack it suffered in late 2020.



In all these cases – which represent several of the largest cyberattacks in history – human behavior had a direct impact on cyber criminals' ability to infiltrate secure systems. While this is a reminder that employee negligence and error are among the most significant cybersecurity liabilities for companies in the supply chain sector, it also demonstrates that their most effective cybersecurity asset is employee awareness. With this fact in mind, consider how companies can empower employees to defend supply chains around the world.

## 1. Establish a proactive cybersecurity awareness program.

When so many cyberattacks are the result of human behavior, it's clear that educating employees should be at the top of any company's list of cybersecurity priorities. Companies often realize this fact too late – 90 percent, for instance, say they provided employees with cybersecurity awareness training after a ransomware attack. There's no reason you should wait to educate employees about cyber threats once you've already suffered the immense financial and reputational consequences of a cyberattack.

## 2. Ensure that your TRAINING content is engaging and relevant.

The biggest mistake companies make when they try to educate their employees about cyber threats is failing to recognize how busy adults learn. It's necessary to keep employees engaged with compelling, narrative-driven content about the latest cyber threats, leverage effective learning techniques like gamification, and give them brief (but consistent) episodes and exercises that won't overload learners with unnecessary information. Cybersecurity awareness content should focus on the specific threats employees face, such as third-party risk.

## 3. Give employees the resources and information they need.

Recall the three major supply chain cyberattacks cited in this report. NotPetya infected the entire Maersk system because one employee downloaded malware onto a single device. This demonstrates the importance of training content that teaches employees how to identify various forms of malware. The attack was also a reminder that physical device security is crucial – especially in an era of remote work, when more employees will be using coffee shops and airport terminals as makeshift offices. Compromised credentials were implicated in the Colonial Pipeline and SolarWinds attacks, and the 2022 DBIR reports that the use of stolen credentials is the top action variety in breaches. Companies can cite these facts to emphasize the importance of using tools like password managers and VPNs, while highlighting the dangers of sharing credentials or failing to update them.



# NOW IS THE TIME TO MAKE CYBER RESILIENCE A CORE PRIORITY AT EVERY LEVEL OF YOUR ORGANIZATION

These are just a few of the ways companies can build cybersecurity awareness into their supply chains. While the supply chain sector will face even more relentless and destructive cyberattacks in the coming years, business leaders have never been more aware of this threat. If you're a supply chain leader, now is the time to make cyber resilience a core priority at every level of your organization. When employees learn how to identify and prevent supply chain cyberattacks, they won't just keep the company safe – they'll help the entire economy avoid the calamitous disruptions we've experienced over the past several years.



[www.ninjio.com](http://www.ninjio.com) | 805.864.1999 | [info@ninjio.com](mailto:info@ninjio.com)