

**CYBER  
THREAT  
INTELLIGENCE  
REPORT**

**DIGITAL SUPPLY CHAIN  
COMPROMISE**

Cybersecurity Division  
Compiled by Sarah Hunt &  
Jocelyn Odorizzi

Date: 19 October 2023



# INTRODUCTION

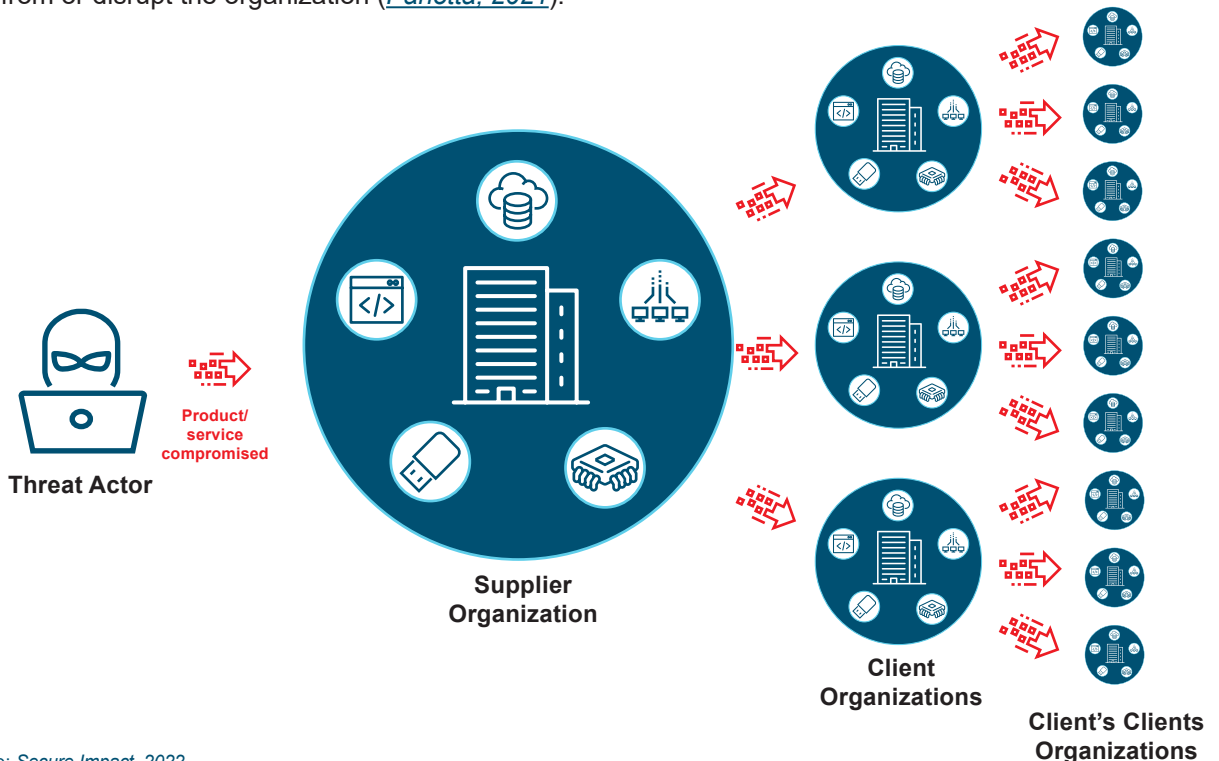
Amidst the intricate threads of our interconnected digital ecosystem, a sinister specter lurks – the insidious compromise of our supply chains. Integral to our organizations' continued existence—as the crucial elements needed to develop, create, and dispense products—supply chains have become ever more vital to protect. Digital supply chains—hereafter referred to as supply chains—though predominately ephemeral in nature, are part of this ecosystem that requires safeguarding (*ENISA, 2021*). In this report, we will unveil the clandestine maneuvers and unearth the threats associated with the compromise of these digital supply chains, illuminating the path to defend against this hard to detect menace.

In recent years, the landscape of cyber threats has witnessed a significant surge in supply chain compromises, demonstrating an alarming sophistication and breadth of tactics employed by threat actors. This report aims to provide a high-level analysis of the evolving threat landscape surrounding supply chain security, highlighting notable incidents as well as tactics, techniques, and procedures utilized by malicious actors. By examining well-documented incidents and emerging trends, this report offers actionable insights to empower organizations in proactively fortifying their supply chain defences and enhancing their cyber resilience against these ever-evolving threats. Considering the growing interconnectivity of global supply chains, a heightened level of vigilance and a strategic, multi-layered approach to security are imperative in safeguarding critical assets and preserving business continuity.



## WHAT IS SUPPLY CHAIN COMPROMISE?

A digital supply chain compromise is a type of one-to-many cyberattack targeting a trusted third-party vendor who offers services, software, or hardware vital to the supply chain. The attackers use this trusted connection to infiltrate an organization, distribute malicious software or hardware, or otherwise steal from or disrupt the organization (*Panetta, 2021*).



Source: *Secure Impact, 2022*

## WHY THE INCREASE IN SUPPLY CHAIN ATTACKS IN RECENT YEARS?

There are several factors contributing to the increase in supply chain attacks in recent years. One major factor is the growing complexity of global supply chains, which involve numerous interconnected parties. Cybercriminals may target software dependencies, third-party vendors, or weak links in the chain to gain access to valuable data or systems. This complexity breeds opportunity as there are more organizations with the same vulnerabilities that can be exploited. With this increased threat exposure, technology—such as malware generated or improved by artificial intelligence—is also advancing, making it easier for attackers to find and exploit weaknesses with more sophisticated tools ([Fadilpašić, 2023](#)). But it is not just the ease of access that is increasing the rate of supply chain attacks, as the potential payoff for attackers has also increased. Valuable information, such as customer data, intellectual property, or financial information, that used to be housed in hard to access on-premises systems can now be accessed through a successful digital supply chain attack, making them an attractive target for cybercriminals ([ENISA, 2021](#)).

The increasing reliance on digital systems is also expanding, increasing the attack surface as it becomes more challenging to secure every aspect of a supply chain due to the demands placed on it. It has become functionally impossible to maintain all parts of a supply chain within a single organization, which necessitates interactions with third parties or reliance on open-source software. This, combined with the prevalence of remote and hybrid work, has created new points of vulnerability that used to be contained to a single premise ([CrowdStrike, 2021](#)).

Human error and human ignorance are also responsible for the threat posed by supply chain compromise. Inadequate awareness of how an organization's supply chain is interconnected with third parties can lead to inadvertent insider threats, as security measures may be circumvented or not in place due to lack of training and knowledge ([Fadilpašić, 2023](#)).

## Threat Actor Profiles

### Nation-States

State-sponsored threat actors whose goal tends to be strategic in nature (e.g., intelligence gathering, espionage). Typically well-funded, with legal permission to act in their home nation.



### Cybercriminals & Organizations

Individuals or groups looking to profit from ransoming an organization or selling exfiltrated data. Typically profit driven, though may be hired by other threat actors with ulterior motives.



### Insider Threats

Individuals within a compromised organization. May be an unwitting insider, unintentionally introducing vulnerabilities into systems, or a malicious insider, who is compromising the organization intentionally.



Sources: [CCCS, 2023a](#); [Fadilpašić, 2023](#)



# DIFFERENT TYPES OF SUPPLY CHAIN COMPROMISES

## HARDWARE

The hardware supply chain attack vector has been overlooked by businesses and individuals alike but is an ingenious way of introducing vulnerabilities that can be manipulated by threat actors into an environment. Most often a compromised piece of hardware acts as a vessel for compromised software to enter a system; however, in cases of interdiction, hardware may be intercepted and have additional or different parts added allowing for the threat actor to monitor activity on the device. This tactic was one of the pieces of intelligence revealed by Edward Snowden about the National Security Agency [NSA], but has been completed by many different threat actors—predominately state-affiliated—around the world ([Snyder, 2014](#); [Leetaru, 2018](#)).

This type of supply chain compromise—though hard to pull off—is often highly effective due to its complexity, which makes it less likely to be anticipated and harder to detect. There is also the human element to consider, as when the devices are counterfeited, they may be sold at a fraction of the cost which make them very enticing for buyers looking to save money. In 2012, the Senate Armed Services Committee released a report outlining the results of an investigation that discovered counterfeit parts, made in China, installed within critical defense systems, military equipment, the Navy Integrated Submarine Imaging System, Traffic Alert and Collision Avoidance Systems, cargo planes, Special Operations helicopters, and a Navy surveillance plan. “In just one example described in the report, the U.S. Air Force says that a single electronic parts supplier, Hong Dark Electronic Trade of Shenzhen, China, supplied approximately 84,000 suspect counterfeit electronic parts into the [Department of Defense] supply chain” ([United States Senate Committee on Armed Services, 2012](#)).

Since 2012, counterfeit hardware has become even more prevalent, being sold on sites such as Amazon and eBay. In 2022 a CEO, Onur Aksoy, was arrested for selling counterfeit Cisco devices, imported from China and Hong Kong, through e-commerce sites. Customers would experience their equipment failing or malfunctioning, which cost users tens of thousands of dollars due to severe damage to their networks and operations. In the end, Aksoy was able to sell the equipment from 2014 until 2020. Although customer complaints led Amazon and eBay to suspend/terminate the storefronts setup by Aksoy, he was able to evade these bans by creating new storefronts under different names. In total, Aksoy received over \$100 million USD in revenue before his arrest ([Kan, 2022](#)).

Other counterfeit hardware to be aware of are USB sticks which can result in less storage space than advertised, data loss due to sudden failure or data being written over, and even a full-blown cyber attack. One such attack is called BadUSB which uses the same security flaw as other USB attacks, such as Rubber Ducky. To understand the attack, you must first know how the computer communicates with peripheral devices such as keyboards, mice, headsets, external hard drives, and anything else that connects to the USB slot. When a new device is plugged in, a piece of software called a driver needs to be downloaded to the computer for the operating system to communicate with that device. This is how the user can move the mouse on the screen, use the keyboard, and save/open documents in a storage device. In this case, bad actors will install a malware package in the firmware on the USB stick, when the USB is inserted into the computer the malware is transferred to the computer during the driver installation, evading detection methods ([Cirelly, 2023](#)).

Without hardware security measures, intellectual property and customer data is at risk. Businesses can protect themselves against counterfeit hardware in four ways:

Only purchase devices from authorized sellers;

Create internal policies and processes that control the acquisition process;

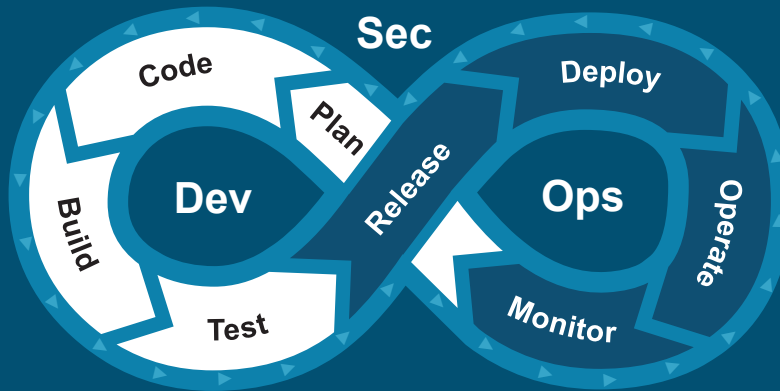
Keep all devices updated with the most recent software provided by the device vendors; and

Look for any physical differences between different units of the same product.

Without hardware security measures such as these, intellectual property and customer data are at risk ([Germain, 2020](#)).

A software supply chain compromise refers to the manipulation or tampering of a software package during its development, distribution, or deployment process. This can occur at various stages, such as when the software is being developed by a third-party vendor, during its distribution through a repository or marketplace, or even when it's installed on a user's system. The objective of a supply chain compromise typically involves introducing malicious code or vulnerabilities into a legitimate software package. This can lead to a range of security risks, including data breaches, unauthorized access, or the spread of malware ([CCCS, 2023b](#)).

An infamous example of a supply chain compromise is the SolarWinds incident in 2020, where attackers compromised the update process of a widely used network management software called Orion, allowing them to infiltrate numerous organizations using a trojan horse. This trojan horse, wearing the face of Orion, permitted cybercriminals to retain an access point, otherwise referred to as a backdoor, within affected organizations, enabling them to steal valuable information. The impacted organizations encompassed Fortune 500 corporations, Microsoft, and even governmental bodies such as the Cybersecurity and Infrastructure Security Agency [CISA], underscoring the far-reaching consequences of a supply chain breach ([Temple-Raston, 2021](#)).



- Plan:** This step involves setting objectives, defining requirements, and creating a roadmap for the development and operations process.
- Code:** Here, code is written, tested, and integrated to create the software or application.
- Build:** In this step, code from multiple developers is merged together to ensure compatibility and identify any conflicts.
- Test:** During this phase, the application is thoroughly tested for bugs, security vulnerabilities, and performance issues.
- Release:** This step involves preparing the software for deployment by finalizing configurations and ensuring all necessary resources and dependencies are in place.
- Deploy:** In this phase, the application is made available for users, either on-premises or through cloud platforms.
- Operate:** This stage involves managing and maintaining the deployed software or application in the production environment.
- Monitor:** This step is when continuous monitoring of the application's performance, security, and usage metrics is conducted.

Source: [Dhaduk, 2022](#)

Software supply chain compromises can occur through various methods, each targeting different stages of the software development and distribution process. Listed on the following page are some common methods that can be utilized at each stage of the software development lifecycle.

## Plan

**Improper Use of Third-Party Components:** Failing to fully assess and select secure third-party components with robust security track records may introduce vulnerabilities into the project.

**Inadequate Change Management Procedures:** Failing to plan for proper change control and versioning can lead to insecure deployments or the introduction of vulnerabilities during an update.

## Code

**Fake or Malicious Code Libraries:** Developers often use third-party libraries and dependencies. Attackers might create fake or malicious versions of popular libraries and upload them to repositories, hoping that developers will unknowingly use them in their projects.

**Malicious Code Injection:** Attackers may inject malicious code into the source code of a software package during development. This code can include backdoors, Trojans, or other forms of malware.

**Insider Threats:** Disgruntled employees or contractors with access to the software development process could intentionally introduce vulnerabilities or malicious code.

**Author Impersonation:** A malicious actor may impersonate a legitimate profile on information sharing sites and trick developers or system administrators into inadvertently introducing vulnerabilities or malicious code by exploiting their trust or manipulating them through phishing or other social engineering techniques.

## Build

**Compromised Build Tools:** Attackers may target the build process of a software project. They could replace legitimate build tools with malicious versions that inject vulnerabilities or backdoors into the final product.

**Credential Theft:** Compromising the credentials of a trusted developer or build system administrator could allow attackers to introduce malicious code during the build process.

**Social Engineering:** Tricking developers or system administrators into inadvertently introducing vulnerabilities or malicious code by exploiting their trust or manipulating them through phishing or other social engineering techniques.

## Test

**Compromised Testing Tools:** Attackers may target the testing stage of a software project. They could replace legitimate testing tools with malicious versions that introduce vulnerabilities into the software or overlook existing vulnerabilities from the previous stages.

## Release

**Tampered Updates and Patches:** Attackers might intercept or tamper with software updates and patches during distribution. This can be done through techniques like man-in-the-middle attacks.

## Deploy

**Fake Software Repositories:** Attackers might create fake or malicious repositories that mimic legitimate ones. Users who unknowingly download software from these repositories could end up with compromised versions.

**Physical Access:** If physical copies of software are distributed, attackers could intercept, modify, and redistribute compromised versions.

**Continuous Integration/Continuous Deployment Attacks:** Manipulation of the code or pipeline for Continuous Integration/Continuous Deployment [CI/CD] scripts accessible by third parties, allowing for compromised code to be introduced into the project.

## Operate

**Intermediaries:** Third-party vendors or contractors involved in the development process could be compromised, allowing attackers to inject malicious code into the software before it reaches the end user.

## Monitor

**Zero-Day Exploits:** Using previously unknown vulnerabilities in software development tools, platforms, or processes to compromise the software supply chain.



Mitigating these risks involves implementing security best practices, such as using secure coding standards, code reviews, cryptographic signatures for software packages, and employing security measures at various stages of the development and deployment process. Additionally, monitoring for unusual or suspicious activities within the supply chain can help detect and respond to potential compromises ([CCCS, 2023b](#)).

## CLOUD

Including both elements of hardware and software supply chain compromise, a cloud supply chain compromise refers to a situation where an attacker gains unauthorized access to a cloud-based service or infrastructure by exploiting vulnerabilities within the supply chain of that service. This typically involves targeting third-party providers, vendors, or dependencies that the cloud service relies on. For instance, if a cloud service relies on various software components or services from different vendors, a compromise in one of those vendors' systems could potentially lead to a breach in the overall security of the cloud service. This could result in unauthorized access, data breaches, or other security incidents.

The ever-evolving nature of the cloud relies on a cycle of continuous integration and delivery, which introduces several opportunities in the development cycle for malicious actors to integrate themselves in the project, poisoning the well. For example, the reliance most cloud service providers have on open-source components, typically gained from public repositories, are another point where they introduce risk into their systems. While a lot of these repositories are well maintained, the ability for members of the public to post in them gives threat actors the ability to implant malicious code, potentially impacting the cloud service provider and their customers if proper reviews are not completed.

Such compromises highlight the importance of robust security measures not only within a cloud service itself but also across its entire supply chain, including third-party providers and their dependencies. It's essential for organizations to carefully vet and monitor their vendors and partners to minimize the risk of supply chain-related security breaches ([Osnat, 2021](#)).



# TACTICS, TECHNIQUES, & PROCEDURES

There are several different attack vectors that can be utilized to instigate a supply chain compromise. They break down into the following categories:



## Tool Manipulation

Modifying tools to serve as ingress points for malicious activity is one way threat actors can implement a supply chain compromise. On the software side, development tools used in the creation, debugging, management, support, or any other part of the development process can be manipulated to allow for malware to be inserted into the source code. In the context of hardware supply chain compromise, the tangible components used in production can be altered to install an alternative chip in a device, potentially facilitating the introduction of malware, backdoors, or the deliberate hindrance of efficient operation, thereby impacting the product's availability ([CCCS, 2023a](#)).

## Source Code Repository Manipulation



When developing code for software or cloud deployments developers often use either public or private source code repositories. These repositories act as libraries that developers can find code for previous solutions that they can use in their own projects. If an attacker infects code in the repository, and proper testing and validation is not completed, it is possible for developers to use this code with the malicious parts embedded, infecting the code of anyone who uses it. Private repositories can be impacted by disgruntled employees, while public repositories can be infected by outside actors, possibly using techniques—such as typosquatting to pretend to be a well-known code solution—or more direct code manipulation ([Kaczorowski, 2020](#)).



## Software Update Hijacking

A commonly seen tactic for supply chain compromise involves manipulating or otherwise hijacking an update for a piece of software. As there is already an established link between supplier and consumer, the update is often automatically trusted and given the same level of privilege as the software. If a threat actor can embed themselves in the update process and insert additional malicious code, the update may be distributed and installed without consumers realizing there is malware included, due to the trusted link ([CCCS, 2023a](#)).

## Product Bait-and-Switch



Replacing a product with a malicious version that appears legitimate is another attack vector for supply chain compromise. With software supply chain compromise, typosquatting is a common tactic used, where malicious actors will put up a product that is one letter off or very similarly named to the legitimate software (e.g., Microsoft vs. Micr0soft). They may also offer a cheaper or free version of what looks to be a popular paid piece of software on a service that is less regulated than the one the legitimate version is distributed on, a tactic common with mobile apps. With hardware supply chain compromise, legitimate distributors like Amazon may inadvertently list products they believe to be authentic but are, in fact, compromised, ostensibly allowing the threat actors to hide behind the legitimacy provided by the distributor. Another method of compromise involves the interception of legitimate hardware during the shipping process. This interdiction allows for the threat actor to manipulate the legitimate hardware or replace it entirely, allowing for easy distribution of the modified products ([Goodwin & Borenstein, 2020](#); [CCCS, 2023a](#)).



## Code Signing Manipulation

A commonly used method to ensure the authenticity and integrity of a piece of code is code signing. This is a mark that the code provided is assured to be coming from a specific source so that consumers can be sure the software they are using does what they are told it would do. If a threat actor manages to manipulate the code without invalidating the code signing, it could allow for a malicious piece of code to be viewed as legitimate due to the assumed trust of the signature. The two predominant approaches to manipulate code signing involve either compromising the certificate of authority that designates the code as trustworthy or unlawfully obtaining the private encryption key from a legitimate developer ([Encryption Consulting, n.d.](#); [CCCS, 2023a](#)).



# THREATS

While numerous supply chain compromise causes are rooted in technology, it's crucial to recognize that it's not solely a technological issue. It encompasses people, processes, and knowledge as well. Every vulnerability in the system ultimately traces back to human factors, as underscored by the various threats associated with supply chain compromise.

## ESPIONAGE & DATA EXFILTRATION

### WHAT IS IT?

Cyber espionage is when a malicious actor attempts to gain an advantage over competitors, seek out financial gains, or help advance a political agenda by illicitly accessing protected, sensitive, or classified data, systems, or intellectual property ([Baker, 2023](#)). Frequently in cyber espionage incidents, data exfiltration occurs. Data exfiltration, also known as data theft, involves the unauthorized transfer of information from a system and can occur as a component of espionage or other cyber attacks, such as ransomware incidents ([Joint Task Force, 2020](#)).

Supply chain compromise can aid in cyber espionage and data exfiltration as these threats are reliant on maintaining a sustained presence in the victim system, also referred to as an advanced persistent threat [APT]. If a threat actor gains access through a supply chain breach, the organization may not immediately detect it, as they might not have anticipated such a breach and, consequently, haven't prepared for it ([Baker, 2023](#)).

### EXAMPLE FROM THE REAL WORLD

In late 2020, FireEye, a cybersecurity company, released information about malicious activity that was impacting SolarWinds Orion, a service management platform. SolarWinds Orion is a product utilized across several organizations—ranging from governments to Fortune 500 companies. Exploiting this connection, the threat actor leveraged a vulnerability within the SolarWinds system to infiltrate it and deploy a file disguised as an update for the SolarWinds platform. Regrettably, for the platform's users, this turned out to be a Trojan Horse – a file that appears genuine but conceals malicious software. Consequently, when these organizations performed platform updates, they unwittingly created a backdoor for the threat actor, granting them access to gather information and conduct surveillance on all affected systems, as well as exfiltrate pertinent data ([Oladimeji & Kerner, 2023](#)).

## RANSOM & EXTORTION

### WHAT IS IT?

Supply chain compromise was listed by the CISA as a primary factor contributing to the rise in ransomware reports in 2021 ([CISA, 2022](#)). This occurs because supply chain compromise allows threat actors to effectively scale their attack surface, with the initially compromised target serving as a “gateway” to gain access to multiple other systems, demanding minimal additional effort from the cybercriminal. A ransomware attack could result in some or all links in a supply chain having their critical files encrypted and being extorted for decryption keys ([The Associated Press, 2021](#)).

Ransomware is not the only form of extortion that leverages supply chain compromises. In 2023, there has been a rise in cybercriminals utilizing vulnerabilities in systems to exfiltrate data, followed by threats to post this information online unless the victim organization pays them not to. Like with ransomware, a supply chain compromise exacerbates the impact of this extortion, as it allows cybercriminals to extort several organizations by using a single vulnerability. Many cybercriminal groups engage in the practice of both encrypting systems and issuing threats to expose an organization's data simultaneously, a strategy commonly known as double extortion ([Coker, 2023](#)).

### EXAMPLE FROM THE REAL WORLD

Disclosed in the first half of 2023, the cyber attack on the MOVEit file transfer management program—used for secure file transfers—showcases the devastating scope a supply chain compromise can have. Unfortunately, MOVEit had a zero-day vulnerability, one that was unknown to its developers. The vulnerability enabled the CIOp ransomware group to breach the systems of MOVEit clients, allowing them to exfiltrate data and potentially expose the information unless the affected company paid the ransom ([Satter & Siddiqui, 2023](#)).

As of mid-October 2023, at least 2,275 organizations have been victimized by the MOVEit attack, resulting in the information of approximately 62-67 million individuals having been impacted ([Kondruss, 2023](#)). The extent of this attack highlights the destructive effect a supply chain attack can have, since several of the impacted companies were not direct users of MOVEit but rather had a vendor who utilized the service, creating an ever-growing snowball of effected organizations.



### WHAT IS IT?

Disruption of operations due to a supply chain compromise is a critical concern for organizations. When a component or service within the supply chain is compromised, it can lead to significant disruptions in the normal functioning of a system, network, or entire organization. This disruption can manifest in various ways, such as system outages, financial loss, delays in production or service delivery, and stoppages in key business processes.

These disturbances can have cascading effects across an organization and its ecosystem. Suppliers, partners, and customers who rely on the affected organization may also experience delays and setbacks. More frighteningly, if the compromised element is part of critical infrastructure—such as in healthcare or transportation—the consequences can be even more severe, potentially jeopardizing public safety ([HackerOne, n.d.](#)).

### EXAMPLE FROM THE REAL WORLD

Labelled as the most devastating cyberattack in history by cybersecurity and technology journalist Andy Greenberg, the NotPetya attack occurred in June 2017 and saw the operations of organizations in over 60 countries paralyzed due to a supply chain compromise. The attack started with the compromise of a single, small software company in the Ukraine but brought giant, multinational organizations to a standstill. Maersk, a global shipping company, faced days of business disruption, which, in turn, caused organizations and vendors dependent on them to also experience work stoppages. An entire shipping terminal was shut down when they were unable to receive directions on the cargo on certain ships, having the knock-on effect of the land shipping crews being unable to work, and customers not receiving their cargo. Maersk was not the sole major company impacted by this attack; it also affected other significant entities like the pharmaceutical giant Merck and the snack food company Mondelez, as well as the supply chains they are integral parts of ([Greenberg, 2018](#)).

## REPUTATIONAL DAMAGE

### WHAT IS IT?

A supply chain compromise has the potential to diminish customer trust and confidence in the affected organization. This erosion of trust can stem from perceptions of vulnerability as a victim of such an attack, the harm experienced by customers due to data exposure, or the compromise of their own systems. The consequences of this lost trust can be enduring, impacting a company's reputation and customer loyalty over the long term ([HackerOne, n.d.](#)).

A compromised supply chain can not only immediately harm a company's brand reputation but, depending on the industry and location, it may also lead to legal and regulatory consequences. Organizations may face fines, penalties, or other legal actions for failing to adequately protect sensitive information, all of which continue to reflect poorly on the organization over time ([von Berlepsch, Lemke, & Gorton, 2022](#)).

### EXAMPLE FROM THE REAL WORLD

In 2013 the retail company Target experienced a data breach when a third-party vendor was compromised, resulting in the personal information of over 100 million of their customers being exposed. The public responded unfavorably to the extended duration it took Target to both identify the breach and subsequently notify the public. This perceived delay in action resulted in a significant decline in Target's public perception. In BrandIndex surveys conducted between 2013 and 2019, consumer's perception of the Target brand dropped by over 10% immediately after the breach and by 2019, despite trending more positive over the years, had not returned to pre-breach standings ([Black Kite, 2022](#)).

## FINANCIAL IMPACT

### WHAT IS IT?

Responding to any cyber incident can be resource-intensive to handle, but a supply chain compromise can blindside an organization, primarily because it arises from an unexpected vector and involves multiple complex facets. When a component or service within the supply chain is compromised, it can lead to a range of direct and indirect costs for all affected organizations. For example, a data breach associated with a supply chain compromise costs an organization 8.3% more than the cost of other data breaches, averaging around \$4.63 million USD per incident ([IBM, 2023](#)).

Direct costs may include expenses related to things such as identifying and mitigating the breach. This can include engaging cybersecurity experts to investigate the incident, conducting forensic analyses, implementing measures to contain and eradicate the threat, and providing credit monitoring services for impacted customers. There may also be costs associated with notifying affected parties, ranging from customers, partners, vendors, and regulatory authorities, as required by the organization's standards and data protection regulations.



While these direct costs can be significant, the indirect costs can be equally or more devastating financially. These may involve the loss of revenue due to operational disruptions such as downtime or reduced productivity, lost sales or customers due to reputational damage, the costs associated with paying regulatory penalties or fines, or the cost of legal fees needed to defend against potential lawsuits. In addition, the now apparent need for more enhanced security measures and technologies to prevent future incidents and strengthen the supply chain's resilience can also be costly to implement (*Summerfield, 2017*).

### EXAMPLE FROM THE REAL WORLD

\$10 billion USD. That is the estimated cost of the 2017 NotPetya cyber attack discussed in the *Disruption of Operations* section (*Greenberg, 2018*). Impacting over 300 organizations, including banks, power companies, hospitals, and multinational corporations, this attack was financially devastating for several of the affected groups. FedEx was heavily impacted by the attack, as they had recently acquired TNT Express, another delivery and logistics company, who was hit by NotPetya. The expenditure for FedEx to recuperate from the TNT Express incident totaled \$400 million USD. This cost was divided between the revenue loss resulting from the inability to operate and the expenses associated with restoring the affected systems following the attack (*Nash, Castellanos, & Janofsky, 2018*). Merck, a pharmaceutical company, suffered the most substantial financial loss during the attack, amounting to a staggering \$870 million USD. They were even compelled to borrow specific pharmaceutical doses from the U.S. Centers for Disease Control and Prevention, leading to increased scrutiny and negative publicity from the House Energy and Commerce committee (*Greenberg, 2018; Nash, Castellanos, & Janofsky, 2018*).



### WHAT IS IT?

A compromised supply chain can serve as a vehicle for distributing malware to a broader spectrum of individuals and entities. It enables attackers to breach trusted providers and utilize them as a trustworthy front for disseminating malware. This malicious software might be inserted into authentic software or firmware updates. When installed, it could grant unauthorized access or control to the attackers. Similarly, a USB manufacturer could be compromised, leading to malware being pre-loaded onto their products before distribution, with the same potential consequences.

Malware distributed through a supply chain compromise can be more challenging to identify since it may carry a digital signature from a trusted entity, creating an illusion of authenticity. This veneer of legitimacy, in turn, could delay the discovery of the malware, consequently amplifying the harm within impacted organizations or enabling the malware to travel further through the supply chain (*Greenberg, 2019*).













### EXAMPLE FROM THE REAL WORLD

In March 2017, cybercriminals compromised Piriform Software, a UK-based company known for developing digital cleaning and optimization tools. They accomplished this by using stolen credentials and subsequently moving within Piriform's systems to install various malicious tools and software. A few months later, Piriform was acquired by the security juggernaut firm Avast, which garnered a larger audience for Piriform's tools. Unfortunately for Avast, this increased exposure for these new tools also led to a serious supply chain compromise.

One of Piriform's popular tools, CCleaner, which had been developed before the acquisition, was compromised by the attackers in March. The cybercriminals infected CCleaner with malicious code, affecting all 2.27 million users who downloaded the tool from Avast's website. Of these compromised users, the attackers chose to target 40 with a second stage attack, similar to the one used against Piriform. While the attack was detected relatively quickly, the potential for the supply chain attack to persist, utilizing the products of the 40 affected companies in much in the same way Piriform's tools had been used to spread malware (*Hay Newman, 2018*).

# MITIGATIONS

Mitigating supply chain compromise is crucial to maintaining the security and integrity of products and services. Here are some strategies and best practices to consider:

 <h3>Vendor Risk Assessment</h3> <p>Conduct thorough due diligence before onboarding any new vendors or suppliers. This includes assessing their security practices, compliance with industry standards, and track record (<a href="#">CCCS, 2022</a>; <a href="#">CCCS, 2023b</a>).</p>	 <h3>Third-Party Audits &amp; Certifications</h3> <p>Require vendors to undergo regular security audits and obtain relevant certifications, such as ISO 27001 compliance, PCI compliance, ISAE 3402 report, or a SOC 1 or 2 report (<a href="#">JCAEW Insights, 2023</a>).</p>	 <h3>Contractual Obligations</h3> <p>Clearly define security requirements and expectations in contracts, requests for proposals, and service level agreements [SLAs]. Specify responsibilities for security measures, incident reporting, and compliance with industry regulations (<a href="#">NIST, n.d.</a>).</p>
 <h3>Continuous Monitoring</h3> <p>Implement continuous monitoring of vendor activities and systems, including their security posture, to identify any anomalies or suspicious behaviour (<a href="#">CISA, 2021</a>).</p>	 <h3>Multi-Factor Authentication [MFA]</h3> <p>Mandate the use of multi-factor authentication for accessing sensitive systems or data, both within your organization and for your vendors tasks (<a href="#">Kost, 2023</a>).</p>	 <h3>Data Encryption</h3> <p>Require the encryption of sensitive data during transit and at rest. This helps protect information from being intercepted or accessed by unauthorized parties (<a href="#">Kost, 2023</a>).</p>
 <h3>Secure Software Development Lifecycle</h3> <p>Encourage or require vendors to follow secure development practices, such as regular security testing, code reviews, and vulnerability scanning (<a href="#">Katz, 2023</a>).</p>	 <h3>Patch Management</h3> <p>Ensure vendors have a robust process for promptly applying security patches and updates to their software and systems (<a href="#">Olsson, 2021</a>).</p>	 <h3>Incident Response Planning</h3> <p>Require vendors to have a well-defined incident response plan in place, and establish procedures for timely reporting of any security incidents (<a href="#">Boyens et al., 2022</a>).</p>
 <h3>Incident Testing &amp; Simulation</h3> <p>Conduct simulated exercises to test your and your vendors' incident response capabilities (<a href="#">Cymulate, 2019</a>).</p>	 <h3>Business Continuity Planning</h3> <p>Establish redundancy and backup plans for critical components of your supply chain to ensure continuity in case of an incident or disruption (<a href="#">Boyens et al., 2022</a>).</p>	 <h3>Access Controls &amp; Least Privilege</h3> <p>Enforce the principle of least privilege, ensuring that individuals and systems only have access to the resources and information necessary to perform their tasks (<a href="#">Kost, 2023</a>).</p>





### Supply Chain Visibility

Gain visibility into your vendor's supply chain, including subcontractors and their security practices ([Pagnotta, 2023](#)).



### Cybersecurity Training & Awareness

Provide training and resources to employees and vendors on cybersecurity best practices, including phishing awareness and social engineering prevention ([CCCS, 2020a](#)).



### Regulatory Compliance

Ensure that vendors adhere to relevant industry-specific regulations and compliance standards ([Biniyaz, 2023](#)).



### Regular Security Assessments & Audits

Conduct periodic security assessments and audits, including penetration testing and vulnerability scanning, of your vendors' systems and applications ([Paterson, 2017](#)).



### Supplier Diversity

Consider diversifying your supplier base to reduce dependency on a single vendor, which can help spread risk ([Basom, 2023](#)).



### Transparency & Communication

Foster open communication channels with your vendors to facilitate the sharing of security-related information and concerns ([Wyatt, 2023](#)).

## CONCLUSION

In conclusion, the threat to our digital supply chains is not a hypothetical scenario, but a stark reality demanding our vigilant attention. As this report has revealed, the adversaries' tactics are becoming increasingly sophisticated, exploiting vulnerabilities in our interconnected systems. However, armed with comprehensive knowledge and a proactive stance, we have the power to fortify our defenses and mitigate the risks. By fostering a culture of awareness, continuous monitoring, rigorous testing, and swift response, we can help safeguard our digital supply chains, better ensuring the integrity and resilience of our critical operations. The battle is ongoing, but with strategic awareness and concerted efforts, we stand poised to rail against this pervasive threat.

# DEFINITION GUIDE

TERM	DEFINITION
<b>Advanced Persistent Threat [APT]</b>	<p>A sophisticated and targeted cyberattack strategy involving prolonged and stealthy intrusion into a specific target's network or systems with the intent of gaining unauthorized access, extracting sensitive information, or maintaining long-term covert access for other malicious activities.</p>
<b>Breach</b>	<p>Refers to the unauthorised access, acquisition, or disclosure of sensitive or confidential information. This can include personal data, financial information, intellectual property, or other data that an organization or individual aims to keep private.</p>
<b>Business Continuity</b>	<p>Refers to an organization's ability to maintain essential operations and functions during and after a disruptive event. This could be caused by a range of factors, including natural disasters cyber attacks or other unforeseen incidents.</p>
<b>Encryption</b>	<p>The process of converting information or data into code to prevent unauthorized access. It involves using an algorithm and an encryption key to transform plaintext (readable data) into ciphertext (encoded data).</p>
<b>Exfiltration</b>	<p>Refers to the unauthorized extraction, copying, or theft of data from a computer system, network, or organization. It typically involves a malicious actor gaining access to sensitive information and then transferring it out of the affected environment without detection.</p>
<b>Incident Response</b>	<p>Refers to the structured approach and coordinated actions taken by an organization to manage and mitigate the impact of a security incident. This can include events like data breaches, cyberattacks, system vulnerabilities, or other disruptions to normal operations.</p>
<b>Multi-Factor Authentication [MFA]</b>	<p>A security practice that requires users to provide multiple forms of identification before granting them access to a system application or account.</p>
<b>Secure Software Development Lifecycle [SDLC]</b>	<p>A structured framework used by software developers and organizations to plan, design, build, test, deploy, and maintain software applications. The process helps ensure that software projects are developed systematically meeting quality standards and user requirements while managing resources effectively.</p>
<b>Typosquatting</b>	<p>A malicious practice where cyber attackers registers a domain name that is intentionally similar to a legitimate website's domain. The goal of typosquatting is to trick users into visiting the malicious site where they may be subjected to various scams, phishing attacks, malware downloads, or attempts to steal their login credentials. Also known as URL hijacking.</p>
<b>Zero-Trust</b>	<p>A security model which requires all individuals regardless of role to be authenticated and authorized before being granted or keeping access to networks, systems, assets, applications, information, etc.</p>



# REFERENCES & FURTHER READING

- Arampatzis, A. (2023, August 1). Supply chain attacks: One of the biggest cybersecurity threats of 2023. *Supply Chain Brain*. <https://www.supplychainbrain.com/blogs/1-think-tank/post/37813-supply-chain-attacks-one-of-the-biggest-cybersecurity-threats-of-2023>
- Barker, K. (2023, February 28). What is cyber espionage?. *CrowdStrike*. <https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/>
- Basom, A. (2023, August 25). Affirmative action is out — But supplier diversity is here to stay. *Supply Chain Brain*. <https://www.supplychainbrain.com/blogs/1-think-tank/post/37848-affirmative-action-is-out-but-supplier-diversity-is-here-to-stay>
- Bates, E. (2021, February 11). Understanding the third-party impact on cybersecurity risk. *Forbes*. <https://www.forbes.com/sites/forbestechcouncil/2021/02/11/understanding-the-third-party-impact-on-cybersecurity-risk/?sh=502238fb7089>
- Biniyaz, J.K. (2023, July 7). How to mitigate cybersecurity risks associated with supply chain partners and vendors. *Entrepreneur*. <https://www.entrepreneur.com/science-technology/how-to-mitigate-cybersecurity-risks-within-supply-chain/454758>
- Black Hat. (2020, January 15). *The Enemy Within: Modern Supply Chain Attacks* [Video]. YouTube. <https://www.youtube.com/watch?v=vno8xm--K44>
- Black Kite. (2022, January 13). Reputational cyber risk – How to avoid business loss. *Black Kite*. <https://blackkite.com/blog/reputational-cyber-risk-how-to-avoid-business-lost/>
- Bonderud, D. (2021, September 28). Supply chain attack: What it is (and what to do about it). *Security Intelligence*. <https://securityintelligence.com/articles/supply-chain-attack-what-it-is-what-to-do/>
- Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). Cybersecurity supply chain risk management practices for systems and organizations. *National Institute of Standards and Technology*. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf>
- Brooks, C. (2022, August 30). The urgency of cybersecurity for hardware devices. *Security Infowatch*. <https://www.securityinfowatch.com/cybersecurity/information-security/computer-and-network-security-hardware/article/21279199/the-urgency-of-cybersecurity-for-hardware-devices>
- Canadian Centre for Cyber Security. (2018, December 6). Supply chain threats and commercial espionage. *Government of Canada*. <https://www.cyber.gc.ca/en/guidance/supply-chain-threats-and-commercial-espionage>
- Canadian Centre for Cyber Security. (2019, March 29). Supply chain security for small and medium-sized organizations (ITSAP.00.070). *Government of Canada*. <https://www.cyber.gc.ca/en/guidance/supply-chain-security-small-and-medium-sized-organizations-itsap00070>
- Canadian Centre for Cyber Security. (2020a, February 20). Top 10 IT security actions: #6 provide tailored cyber security training (ITSM.10.093). *Government of Canada*. <https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-6-provide-tailored-cyber-security-training-itsm10093>
- Canadian Centre for Cyber Security. (2020b, December 30). Alert - Recommendations for SolarWinds Supply-Chain Compromise - update 1. *Government of Canada*. <https://www.cyber.gc.ca/en/alerts-advisories/recommendations-solarwinds-supply-chain-compromise>
- Canadian Centre for Cyber Security. (2022, July 28). Cyber supply chain: An approach to assessing risk - ITSAP.10.070. *Government of Canada*. <https://www.cyber.gc.ca/en/guidance/cyber-supply-chain-approach-assessing-risk-itsap10070>
- Canadian Centre for Cyber Security. (2023a, February 8). The cyber threat from supply chains. *Government of Canada*. <https://www.cyber.gc.ca/en/guidance/cyber-threat-supply-chains>
- Canadian Centre for Cyber Security. (2023b, February 8). Protecting your organization from software supply chain threats – ITSM.10.071. *Government of Canada*. <https://www.cyber.gc.ca/en/guidance/protecting-your-organization-software-supply-chain-threats-itsm10071>

- Canadian Centre for Cyber Security. (2023c, March 30). Alert - Supply chain compromise impacting 3CXDesktopApp. *Government of Canada*. <https://www.cyber.gc.ca/en/alerts-advisories/supply-chain-compromise-impacting-3cxdesktopapp>
- Canadian Centre for Cyber Security. (2023d, April 11). Defending against data exfiltration threats - ITSM.40.110. *Government of Canada*. <https://www.cyber.gc.ca/en/guidance/defending-against-data-exfiltration-threats-itsm40110>
- Center for Internet Security. (2021, March 15). The SolarWinds cyber-attack: What you need to know. *Center for Internet Security*. <https://www.cisecurity.org/solarwinds>
- Cirelly, J. (2023, January 10). What is BadUSB? and how to avoid it?. *Comparitech*. <https://www.comparitech.com/net-admin/what-is-badusb/>
- Coker, J. (2023, July 26). Ransomware attacks skyrocket in 2023. *Infosecurity Magazine*. <https://www.infosecurity-magazine.com/news/ransomware-attacks-skyrocket-q2/>
- CrowdStrike. (2021, December 8). What is a supply chain attack?. *CrowdStrike*. <https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/>
- CrowdStrike. (2023, March 31). CrowdStrike Falcon Platform detects and prevents active intrusion campaign targeting 3CXDesktopApp customers. *CrowdStrike Blog*. <https://www.crowdstrike.com/blog/crowdstrike-detects-and-prevents-active-intrusion-campaign-targeting-3cxdesktopapp-customers/>
- Cybersecurity & Infrastructure Security Agency. (2021). Defending against software supply chain attacks. *Cybersecurity & Infrastructure Security Agency*. [https://www.cisa.gov/sites/default/files/publications/defending\\_against\\_software\\_supply\\_chain\\_attacks\\_508\\_1.pdf](https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf)
- Cybersecurity & Infrastructure Security Agency. (2022, February 10). 2021 Trends Show Increased Globalized Threat of Ransomware. *Cybersecurity & Infrastructure Security Agency*. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a>
- Cymulate. (2019, May 6). How BAS optimizes defense against supply chain attacks. *Cymulate*. <https://cymulate.com/blog/how-breach-attack-simulation-optimizes-defense-against-supply-chain-attacks/>
- Dhaduk, H. (2022, January 13). DevOps lifecycle: 7 phases explained in detail with examples. *Simform*. <https://www.simform.com/blog/devops-lifecycle/>
- Encryption Consulting. (n.d.). What is code signing? How does code signing work?. *Encryption Consulting*. <https://www.encryptionconsulting.com/education-center/what-is-code-signing/>
- ENISA. (2017, August 29). Supply chain attacks. *European Union Agency for Cybersecurity*. <https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks>
- ENISA. (2021, July 29). Understanding the increase in supply chain security attacks. *European Union Agency for Cybersecurity*. <https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks>
- Fadilpašić, S. (2023, May 8). 6 reasons why supply chain attacks are on the rise. *Make Use Of\_*. <https://www.makeuseof.com/reasons-why-supply-chain-attacks-are-on-the-rise/>
- Fischbein, J. (2022, September 27). Mitigating the risk of supply chain attacks in the age of cloud computing. *Forbes*. <https://www.forbes.com/sites/forbestechcouncil/2022/09/27/mitigating-the-risk-of-supply-chain-attacks-in-the-age-of-cloud-computing/?sh=61f21a58d313>
- Fortinet. (n.d.). Supply chain attacks: Examples and countermeasures. *Fortinet*. <https://www.fortinet.com/resources/cyberglossary/supply-chain-attacks>
- Fortra's Alert Logic Staff. (2023, March 14). Supply chain compromise: The risks you need to know. *Fortra*. <https://www.alertlogic.com/blog/supply-chain-compromise/>
- Gatlan, S. (2019, March 26). ASUS admits its Live Update Utility was backdoored by APT group. *Bleeping-Computer*. <https://www.bleepingcomputer.com/news/security/asus-admits-its-live-update-utility-was-backdoored-by-apt-group/>

- Germain, J.M. (2020, July 24). Beware of counterfeit network equipment. *Tech News World*. <https://www.technewsworld.com/story/beware-of-counterfeit-network-equipment-86770.html>
- Get Cyber Safe. (2023, February 20). What is typosquatting? *Government of Canada*. <https://www.getcyber-safe.gc.ca/en/blogs/what-typosquatting>
- Global Affairs Canada. (2021, April 15). SolarWinds cyber compromise. *Government of Canada*. <https://www.canada.ca/en/global-affairs/news/2021/04/solarwinds-cyber-compromise.html>
- Goodwin, C., & Borenstein, J. (2020, February 3). Guarding against supply chain attacks—Part 2: Hardware risks. *Microsoft*. <https://www.microsoft.com/en-us/security/blog/2020/02/03/guarding-against-supply-chain-attacks-part-2-hardware-risks/>
- Gorin, Z. (2022, January 4). 2022 trends: Supply chains' impact on corporate reputation. *ICR*. <https://icrinc.com/insights/2022-trends-supply-chains-impact-on-corporate-reputation/>
- Greenberg, A. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>
- Greenberg, A. (2019, May 3). A mysterious hacker group is on a supply chain hijacking spree. *Wired*. <https://www.wired.com/story/barium-supply-chain-hackers/>
- Greenberg, A. (2021, May 31). Hacker lexicon: What is a supply chain attack?. *Wired*. <https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/>
- Greig, J. (2023, August 22). Legitimate software tainted in attacks on Hong Kong organizations, report says. *The Record*. <https://tinyurl.com/bdh48khf>
- HackerOne. (n.d.). Supply chain attacks: Impact, examples, and 6 preventive measures. *HackerOne*. <https://www.hackerone.com/knowledge-center/supply-chain-attacks-impact-examples-and-6-preventive-measures>
- Hay Newman, L. (2018, April 17). Inside the unnerving supply chain attack that corrupted CCleaner. *Wired*. <https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/>
- Hay Newman, L. (2018, October 4). There's no good fix if the supply chain gets hacked. *Wired*. <https://www.wired.com/story/supply-chain-hacks-cybersecurity-worst-case-scenario/>
- Heinbockel, W., Laderman, E., & Serrao, G. (2018, May 8). Supply chain attacks and resiliency mitigations. MITRE. <https://www.mitre.org/news-insights/publication/supply-chain-attacks-and-resiliency-mitigations>
- Hill, M. (2021, November 19). The Kaseya ransomware attack: A timeline. CSO. <https://www.csoonline.com/article/571081/the-kaseya-ransomware-attack-a-timeline.html>
- Huang, K., Wang, X., Wei, W., & Madnick, S. (2023, May 4). The devastating business impacts of a cyber breach. *Harvard Business Review*. <https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach>
- IBM. (2023). Cost of a data breach report 2023. *IBM*. <https://www.ibm.com/reports/data-breach>
- ICAEW Insights. (2023, June 27). What the MOVEit hack tells us about supply chain risks. *ICAEW*. <https://www.icaew.com/insights/viewpoints-on-the-news/2023/jun-2023/What-the-MOVEit-hack-tells-us-about-supply-chain-risks>
- InfoSec. (2023, August 10). *MOVEit file transfer vulnerability: What you should know* | *Hacker Headlines* [Video]. YouTube. <https://www.youtube.com/watch?v=Nv3nwJ-uVDU>
- Infused Innovations. (2020, December 21). *What is a Supply Chain Attack?* [Video]. YouTube. <https://www.youtube.com/watch?v=ljT4AcCza9Q>
- International Organization for Standardization. (2021). *Cybersecurity — Supplier relationships — Part 1: Overview and concepts* (ISO Standard No. 27036-1:2021). <https://www.iso.org/standard/82905.html>

- International Organization for Standardization. (2022). *Security and resilience — Security management systems — Requirements* (ISO Standard No. 28000:2022). <https://www.iso.org/standard/79612.html>
- ISACA. (2021, July 28). State of cybersecurity: Reputational damage from attacks tops list of concerns. *ISACA*. <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-23/state-of-cybersecurity-reputational-damage-from-attacks-tops-list-of-concerns>
- Joint Task Force. (2018). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy. *National Institute of Standards and Technology*. <https://doi.org/10.6028/NIST.SP.800-37r2>
- Joint Task Force. (2020). Security and Privacy Controls for Information Systems and Organizations. *National Institute of Standards and Technology*. <https://doi.org/10.6028/NIST.SP.800-53r5>
- Kaczorowski, M. (2020, September 2). Secure at every step: What is software supply chain security and why does it matter?. *GitHub Blog*. <https://github.blog/2020-09-02-secure-your-software-supply-chain-and-protect-against-supply-chain-threats-github-blog/>
- Kan, M. (2022, July 8). CEO arrested for selling \$1 billion in fake Cisco hardware on Amazon, eBay. *PCMag*. <https://www.pcmag.com/news/ceo-arrested-for-selling-1-billion-in-fake-cisco-hardware-on-amazon-ebay>
- Katz, E. (2023, September 13). 5 types of software supply chain attacks developers should know. *Spectral*. <https://spectralops.io/blog/5-types-of-software-supply-chain-attacks-developers-should-know/>
- Kelley, A. (2023, August 16). New CISA guidance looks to guard against supply chain hacks. *Next Gov FCW*. <https://www.nextgov.com/cybersecurity/2023/08/new-cisa-guidance-looks-guard-against-supply-chain-hacks/389480/>
- Kondruss, B. (2023, September 20). MOVEit hack victim list: Progress Software MOVEit vulnerability cyber incident. *Kon Briefing*. <https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html>
- Kost, E. (2023, July 13). 11 ways to prevent supply chain attacks in 2023 (highly effective). *UpGuard*. <https://www.upguard.com/blog/how-to-prevent-supply-chain-attacks>
- Leaders, K. (2023, July 18). 5 common cybersecurity attacks on open-source software. *Anaconda*. <https://www.anaconda.com/blog/5-common-cybersecurity-attacks-on-open-source-software>
- Leetaru, K. (2018, October 4). The Chinese ‘Spy Chip’ Story Is A Reminder Of How Insecure Our Digital World Really Is. *Forbes*. <https://www.forbes.com/sites/kalevleetaru/2018/10/04/the-chinese-spy-chip-story-is-a-reminder-of-how-insecure-our-digital-world-really-is/?sh=58bf900f7e13>
- Lennon, M. (2020, December 14). Global espionage campaign used software supply chain hack to compromise targets, including US Gov. *SecurityWeek*. <https://www.securityweek.com/global-espionage-campaign-used-software-supply-chain-hack-compromise-targets-including-us-gov/>
- Lord, N. (2020, August 7). The cost of a malware infection? For Maersk, \$300 million. *Fortra*. <https://www.digitalguardian.com/blog/cost-malware-infection-maersk-300-million>
- Lyons Hardcastle, J. (2023, July 20). MOVEit body count closes in on 400 orgs, 20M+ individuals. *The Register*. [https://www.theregister.com/2023/07/20/moveit\\_victim\\_count/](https://www.theregister.com/2023/07/20/moveit_victim_count/)
- Montalbano, E. (2023, August 9). OWASP lead flags gaping hole in software supply chain security. *DarkReading*. <https://www.darkreading.com/application-security/owasp-lead-gaping-hole-software-supply-chain-security>
- Nash, K.S., Castellanos, S., & Janofsky, A. (2018, June 27). One year after NotPetya cyberattack, firms wrestle with recovery costs. *WSJ Pro Cybersecurity*. <https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906>
- National Institute of Standards and Technology. (n.d.). Best practices in cyber supply chain risk management conference materials. *National Institute of Standards and Technology*. <https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf>



- Ng, A. (2017, October 25). How Kaspersky Lab got on the US government's bad side. *CNET*. <https://www.cnet.com/news/privacy/kaspersky-lab-russian-hacking-us-government-national-security-faq/>
- Oladimeji, S., & Kerner, S.M. (2023, June 27). SolarWinds hack explained: Everything you need to know. *WhatIs.Com*. <https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>
- Olsson, S. (2021, January 6). Avoid supply chain attacks similar to SolarWinds Orion. *TruSec*. <https://www.truSec.com/hub/blog/avoiding-supply-chain-attacks-similar-to-solarwinds-orions-sunburst>
- Osnat, R. (2021, May 10). Supply chain attacks and cloud native: What you need to know. *The New Stack*. <https://thenewstack.io/supply-chain-attacks-and-cloud-native-what-you-need-to-know/>
- Pagnotta, S. (2023, May 2). How to mitigate supply chain attacks. *Bitsight*. <https://www.bitsight.com/blog/how-mitigate-supply-chain-attacks>
- Palmer, D. (2019, April 29). Ransomware: The key lesson Maersk learned from battling the NotPetya attack. *ZD Net*. <https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/>
- Panetta, K. (2021, January 11). How to respond to a supply chain attack. *Gartner*. <https://www.gartner.com/smarterwithgartner/how-to-respond-to-a-supply-chain-attack>
- Pangilinan, M. (2023, July 12). Nova Scotia announces action for MOVEit data breach victims. *Insurance News*. <https://www.insurancebusinessmag.com/ca/news/breaking-news/nova-scotia-announces-action-for-moveit-data-breach-victims-452425.aspx>
- Patel, V. (2023, March 30). Supply chain compromise. *MITRE ATT&CK*. <https://attack.mitre.org/techniques/T1195/>
- Paterson, A. (2017, November 9). Mitigating risk of supply chain attacks. *SecurityWeek*. <https://www.security-week.com/mitigating-risk-supply-chain-attacks/>
- RSA Conference. (2020, February 27). *Supply Chain Security in the Software Era* [Video]. YouTube. <https://www.youtube.com/watch?v=SgqkbCKp8kE>
- RSA Conference. (2021, February 5). *Webcast: Supply Chain Security: A New Kind of Halting Problem* [Video]. YouTube. <https://www.youtube.com/watch?v=QlvJs-vrJzo>
- RSA Conference. (2022, August 22). *Linked-Out: Security Principles to Break Software Supply Chain Attacks* [Video]. YouTube. <https://www.youtube.com/watch?v=KpvHL4cwFTI>
- Satter, R., & Siddiqui, Z. (2023, August 8). Analysis: MOVEit hack spawned over 600 breaches but is not done yet -cyber analysts. *Reuters*. <https://www.reuters.com/technology/moveit-hack-spawned-around-600-breaches-isnt-done-yet-cyber-analysts-2023-08-08/>
- Schram, G. (2021, June 14). NotPetya: Its Consequences. *Cybrary*. <https://www.cybrary.it/blog/notpetya-its-consequences>
- Secure Impact. (2022, March 14). Cyber security trends in 2022 - Supply chain attacks are rapidly increasing. *Secure Impact*. <https://www.secure-impact.com/post/cyber-security-trends-in-2022-supply-chain-attacks>
- Sheridan, K. (2020, May 28). GitHub supply chain attack uses Octopus Scanner malware. *DarkReading*. <https://www.darkreading.com/vulnerabilities-threats/github-supply-chain-attack-uses-octopus-scanner-malware>
- Summerfield, R. (2017). Dealing with cyber breaches in the supply chain. *Financier Worldwide*. <https://www.financierworldwide.com/dealing-with-cyber-breaches-in-the-supply-chain>
- Snyder, B. (2014, May 15). Snowden: The NSA planted backdoors in Cisco products. *InfoWorld*. <https://www.infoworld.com/article/2608141/snowden—the-nsa-planted-backdoors-in-cisco-products.html>

- Temple-Raston, D. (2021, April 16). A 'worst nightmare' cyberattack: The untold story of the SolarWinds hack. *NPR*. <https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack>
- Temple-Raston, D., & Jarvis, W. (2023, August 30). How did Clop get its hands on the MOVEit zero day?. *The Record*. <https://therecord.media/clop-moveit-zero-day-dustin-childs-interview>
- Tenable. (n.d.). Supply chain compromise: Compromise software supply chain. *Tenable*. [https://www.tenable.com/attack-path-techniques/T1195.002\\_Windows](https://www.tenable.com/attack-path-techniques/T1195.002_Windows)
- The Associated Press. (2021, July 3). Explainer: Ransomware and its role in supply chain attacks. *CTV News*. <https://www.ctvnews.ca/sci-tech/explainer-ransomware-and-its-role-in-supply-chain-attacks-1.5495662>
- Thompson, K. (1984). Reflections on trusting trust. *Turing Award Lecture*. [https://www.cs.cmu.edu/~rdri-ley/487/papers/Thompson\\_1984\\_ReflectionsonTrustingTrust.pdf](https://www.cs.cmu.edu/~rdri-ley/487/papers/Thompson_1984_ReflectionsonTrustingTrust.pdf)
- Trend Micro. (2022, July 17). *Explaining supply chain cyber risk* [Video]. YouTube. <https://www.youtube.com/watch?v=8Yiy9vZLlyg&t=13s>
- United States Senate Committee on Armed Services. (2012, May 21). Senate Armed Services Committee releases report on counterfeit electronic parts. *United States Senate Committee on Armed Services*. <https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts>
- vGics Global. (2022, August 26). Different types of hardware attacks. *LinkedIn*. <https://www.linkedin.com/pulse/different-types-hardware-attacks-vgics-global/>
- von Berlepsch, D., Lemke, F., & Gorton, M. (2022, October 13). The importance of corporate reputation for sustainable supply chains: A systematic literature review, bibliometric mapping, and research agenda. *Springer Link*. <https://link.springer.com/article/10.1007/s10551-022-05268-x>
- Woods, B., & Bochman, A. (2018, May 30). Supply chain in the software era. *Atlantic Council*. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/supply-chain-in-the-software-era/>
- Wyatt, K. (2023, August 24). Understanding the risks and mitigation strategies for supply chain attacks. *Ozark Technology*. <https://www.ozarktechnology.com/blog/understanding-the-risks-and-mitigation-strategies-for-supply-chain-attacks>