The Next Big Breach

How to Protect Against Supply Chain Cybersecurity Threats

Today's cybersecurity breach looks a lot different than those encountered just a few years ago. As cybercriminals expand their range of tricks to include phishing, AI-enabled attacks like deepfakes, and insider threats, many supply chain businesses struggle to keep up.

One of the biggest and potentially most dangerous blind spots for supply chain organizations is third-party providers and partners. From 3PLs to software vendors, a typical company may have its systems connected to dozens of external tools and platforms, each with its own potential for a devastating data breach.

And since per-breach costs in the U.S. have soared to more than **$10 million**, closing those security gaps is critical. Getting there may feel like an impossible task, but the good news is that a little extra vetting before you sign a contract with a new third-party provider can save you massive costs down the line.

In this white paper, we'll discuss:

1. Third-Party Data Breaches: A Rising Threat for Supply Chain Businesses
2. The Top 5 Cybersecurity Mistakes in Supply Chain
3. Best Practices to Protect Your Business
4. Security Certification: What to Look For and Why It Matters
5. Questions to Ask a Vendor to Prevent Them from Supplying a Data Breach
6. Internal Best Practices

Third-Party Data Breaches:

A Rising Threat for Supply Chain

While many people think of a data breach as something that happens to an internal system, the truth is a breach at a third-party vendor or partner can just as easily wreak havoc. And in today's supply chain environment, where an organization is typically connected to dozens of external tools and platforms, there are more opportunities than ever for malicious actors to get ahold of business, customer, and partner information.

For example, when Progress Software's MOVEit file transfer tool was targeted by a cyberattack spree, it exposed sensitive information from a wide variety of businesses using the tool. Even businesses whose internal security was solid had their data revealed. The breach highlighted a critical blind spot for many businesses throughout the supply chain: vendor and other third-party security.

According to cybersecurity firm SOCRadar, **breaches linked to third parties made up more than 35%** of all cybersecurity incidents in 2024. "Your partners' security practices become part of your world, whether you want them to or not," OneRail Chief Information Security Officer Julius Tubbs says.

While not as high as the aforementioned breaches in the U.S., where regulations are often tighter, IBM reports the global average cost of a data breach in 2025 was **$4.4 million**.

Insider Incidents:

A Costly Blind Spot

Insider incidents are breaches in which an employee, contractor or inside partner exposes the company to a cyberattack.

And according to data privacy research firm Ponemon, the cost of insider incidents is on the rise. Their research has found:

The total average annual cost of insider security incidents reached **$17.4 million** in 2024.

Insiders don't have to be malicious to cause significant damage to a business. **55%** of those 2024 incidents were due to carelessness or mistakes, and another **20%** were outsmarted (for example, through successful phishing attempts).

The good news is, companies who implement an internal risk management program saw their time to containment drop, which also reduced their overall breach containment costs.

So how can you avoid a devastating attack like these? It's not a single-action solution; you have to tighten up both your internal security practices and carefully vet any third party who will have access to your data (or that your data will travel through, as in the case of MOVEit).

Top 5 Cybersecurity Mistakes in Supply Chain

Securing your business starts with identifying common mistakes and ensuring you're not making them. While every business environment is different (and comes with its own unique risks and potential challenges/problems), there are five mistakes that pop up most often:

- **Lack of proper vetting for third-party supply chain data storage providers**
- **Lack of oversight of your vendors and partners**
- **Inadequate internal risk management** (such as employee training and policies)
- **Compromised software or hardware**
- **Failure to meet compliance standards for regulations like GDPR and CCPA**

Cybersecurity Mistake 1: Not vetting third-party providers

The moment you integrate with other organizations, whether partners, customers or vendors, you accept the level of security with which those third parties operate. With the average supply chain business connecting to many different vendor and partner systems, it only takes one weak link to cause a massive problem. And if you don't have a strong third-party risk management program, you're relying on guessing their security is strong enough to protect both their business and yours.

"The biggest mistake is assuming your partners operate at the same security level you do. Most of the time, they do not."

—Julius Tubbs, CISM, CRISC, CCSP

OneRail Chief Information Security Officer & Data Protection Officer

Cybersecurity Mistake 2: Not enough visibility into third-party security practices

The ugly truth is, if you don't know how your vendors store data, manage access, patch systems or handle incidents, your business is exposed. Even if your internal security practices are top notch, lack of visibility into your vendor and partner security leaves you open to breaches.

Unfortunately, many businesses assume a focus on cybersecurity is a given in today's tech-savvy world. That assumption is costly, with supply chain vendors who should know how to lock down their clients' data still falling victim to outdated or badly designed security protocols.

Cybersecurity Mistake 3: Inadequate internal risk management

Most security mistakes happen because people are busy, distracted, or have processes in place that make it too easy to slip up.

"There's a common misconception that the purpose of training is to teach people cybersecurity," Tubbs says. "It's not. The real purpose of training is to change behavior."

If your cybersecurity training program is either lacking or not fully aligned with how your business works day to day (and how employee workflows are designed), it won't influence behavior. And if employee behavior doesn't change, your risk remains high.

Just one example of a small behavior change making a big difference is preventing phishing attempts. Here's how such an attack may play out:

+ One of your trusted suppliers gets hit with a cyber attack, but because their tech stack isn't as sophisticated as yours, they don't notice the breach right away.
+ Using the opening created by this attack, the cyber criminal sends an email to you from the compromised supplier with a document (often a PDF) attached. The document contains a link to log in to the employee's email account, perhaps to view a quote or invoice.
+ Because it's from a trusted supplier and the from: email address is legit, your procurement manager who receives the email doesn't think twice about opening the attachment or clicking the link.
+ The link takes the procurement manager to a login page that looks like the real thing, and enters their login information.
+ The cyber criminal now has access to your employee's email, from which they can send phishing emails to your other employees, along with any vendors or customers your employee is in contact with.

By teaching employees how to spot phishing attacks like this one (and to confirm any requests for logins sent via email), you can prevent massive damage to your business, your partners and your reputation.

Cybersecurity Mistake 4: Allowing compromised software or hardware into your tech stack

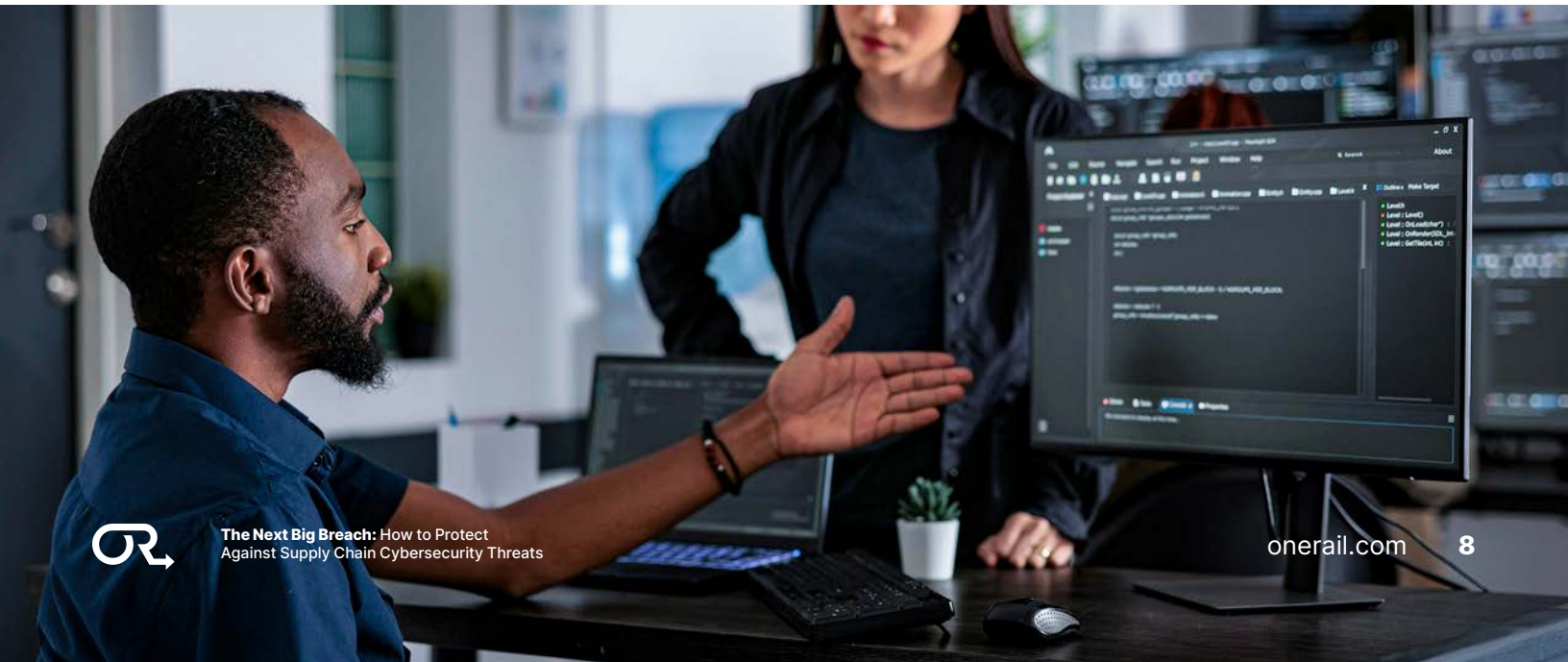
Purchasing software or hardware outside the official information security or technology process can lead to compromised or counterfeit technology entering your system.

While it can be tempting to find cheaper products online or bypass the normal tech vetting process in order to speed things up, going around your information security (IS) or information technology (IT) team means you might make purchases without firmware integrity, approved distributors and authenticity in mind.

One more issue: if that software isn't designed with supply chain business needs in mind, it may also provide ineffective solutions while leaving your organization's data exposed.

Cybersecurity Mistake 5: Falling out of compliance

Failing to comply with SOC audits or regulations like GDPR and CCPA can result in massive fines – but that's not the only risk of compliance issues. Investigations, legal proceedings, remediation, loss of customer trust — all of these have ramifications that reach far beyond the fines you'll have to pay.



Best Practices to Protect Your Business

Avoiding the mistakes above starts with assessing your own risk management practices, especially those surrounding third-party vendor vetting and monitoring.

Unfortunately, one of the biggest issues businesses face is teams bringing in new tools, signing contracts or onboarding vendors without looping in the security team. Stakeholders may think bringing IS or IT into the decision will slow things down, or they make the mistake of assuming the risk is small. But keeping security departments out of these decisions eliminates checks that protect business value. Security can't evaluate the vendor, legal can't negotiate the right protections and procurement can't make sure terms align with the company's standards.

"The fix is straightforward. Standardize the workflow. Involve security early in the conversation. Build security requirements into contracts. Build vendor onboarding into a repeatable process instead of letting each team figure it out on their own."

—Julius Tubbs, CISM, CRISC, CCSP

OneRail Chief Information Security Officer & Data Protection Officer

Security Certification:

What to Look for & Why It Matters

Proper vendor vetting starts with a SOC 2 Type II report. What does that mean, and how does it ensure best cybersecurity practices for a vendor organization?

A SOC 2 is an independent audit conducted by a licensed CPA firm that evaluates the quality of an organization's internal controls over a defined period of time, typically six to 12 months. The purpose is to determine whether a company consistently protects its customer data according to the American Institute of CPAs (AICPA) Trust Services Criteria. Those criteria are:

1. Security (protection against unauthorized access)
2. Availability (systems are operational and reliable)
3. Processing integrity (data is processed accurately and completely)
4. Confidentiality (protection and restriction of access to information)
5. Privacy (personal data is collected, used, retained and disposed of properly)

Most companies have their systems evaluated against just one or two of these criteria. Looking for vendors who have achieved all five ensures mature governance and end-to-end protection of your customers' information — and ultimately, your business health.

One of the most important security best practices is to fully review a third-party provider's SOC 2 Type II report. It's not enough to confirm they have this report; you need to look at the scope, exceptions, trust service criteria and consistency of their reports over multiple years. That last point is important: Consistency is the biggest indication that their controls work in everyday operations, not just on paper.

The same goes for ISO certification. It only matters to your business if the scope covers the specific systems and services your organization will rely on. A provider may have ISO certification that doesn't apply to the part of their environment that stores your data, making it irrelevant to your business needs.

That said, ISO certification that highlights a provider's robust processes and measures to protect sensitive data IS an important indicator of that provider's suitability to partner with your business. For example, a vendor with ISO 27001:2022 certification shows a commitment to safeguarding supply chain continuity and customer trust.

Supply chain networks are becoming more data-driven every year. The ISO 27001:2022 certification ensures that every order, customer record and operational insight is protected within a globally recognized security framework.

Carefully reviewing a potential vendor for ISO and SOC 2 certification is no longer optional in today's cybersecurity landscape.

"The goal is not to collect documents. The goal is to understand what those documents say about how that provider approaches security, privacy and risk."

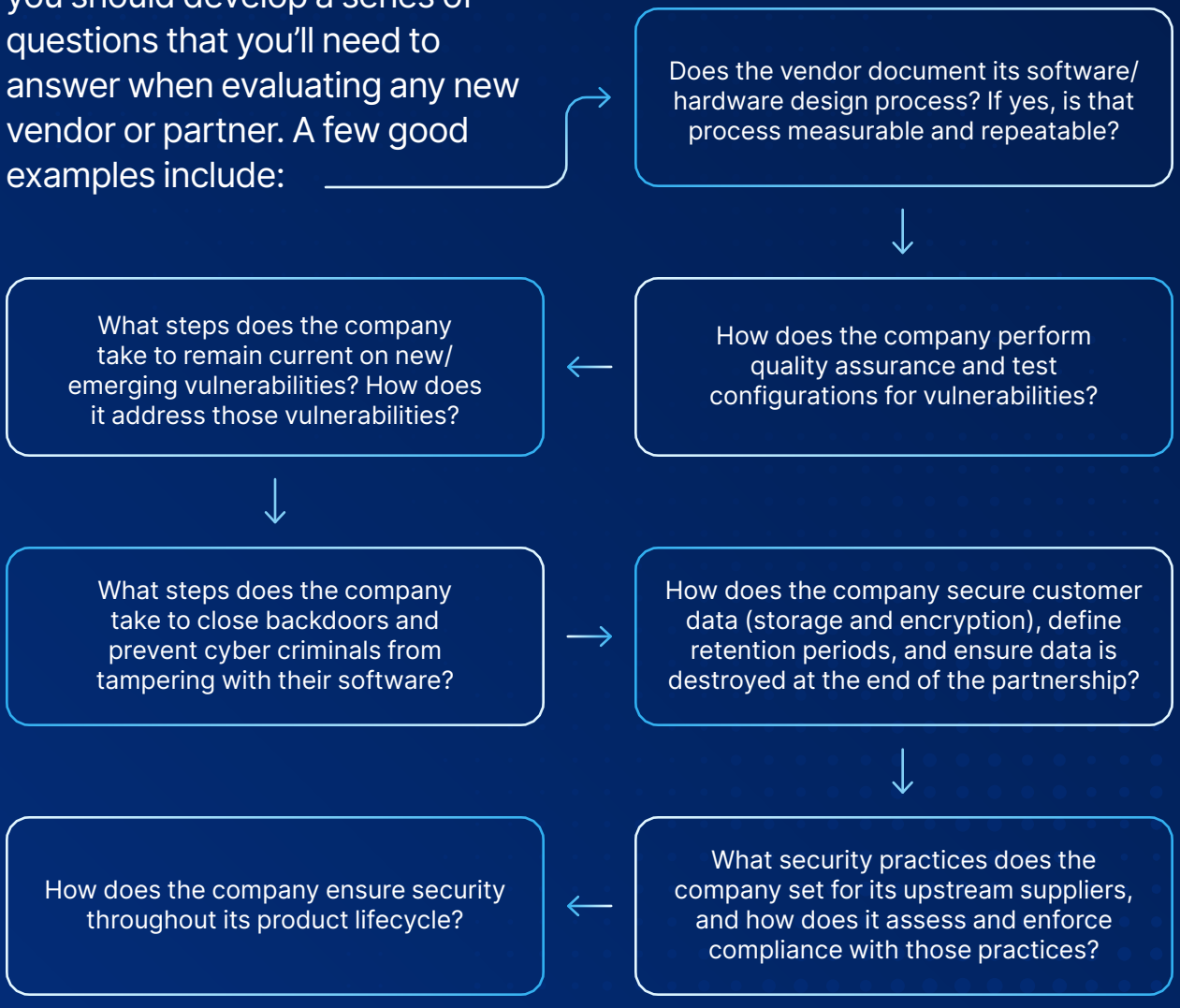
—Julius Tubbs, CISM, CRISC, CCSP

OneRail Chief Information Security Officer & Data Protection Officer

Questions to Ask

Do Your Due Diligence to Prevent Vendors from Triggering Data Breaches

Beyond these certifications, you should develop a series of questions that you'll need to answer when evaluating any new vendor or partner. A few good examples include:



Internal Best Practices

With third-party providers properly assessed, you can focus on more internal-facing best practices to protect your business. These include:

+ Encrypting data and requiring multi-factor authentication to ensure protected access to sensitive data and systems.
+ Performing regular updates and patches to ensure your system remains protected against new or emerging threats.
+ Implementing strict monitoring and logging practices to detect malicious activity and intrusion attempts faster.
+ Performing penetration and vulnerability testing and regularly review and update your security policies to stay ahead of threats.
+ Performing regular backups in case of a breach or incursion.
+ Putting a recovery plan into place so all stakeholders know what to do in the event of a cyberattack or breach.
+ Building security practices into contracts and RFPs.
+ Developing and implementing a comprehensive internal risk management plan that ensures employees are not only educated on security risks, but know how and why they should adjust their behavior to protect sensitive data.

A final note for organizations trying to balance the need for better third-party vetting and security practices against tight schedules:

"The biggest challenge to achieving these best practices is speed. Businesses want to move fast, and may try to skip steps like reviews, testing, approvals, and documentation. That is exactly how issues get introduced."

—Julius Tubbs, CISM, CRISC, CCSP

OneRail Chief Information Security Officer & Data Protection Officer

OneRail Delivers on Cybersecurity Promises

Reinforcing its commitment to compliance and security, OneRail recently achieved SOC Type II compliance across all five Trust Services Criteria: security, availability, processing integrity, confidentiality and privacy.

In addition, OneRail achieved ISO 27001:2022 certification to ensure our approach also aligns with global standards.

Even more significant: OneRail has maintained SOC 2 Type II compliance for five consecutive years, demonstrating consistency in controls, compliance and documentation. Many companies fail to maintain continuous, year-over-year SOC 2 compliance. Our focus on constant monitoring, risk management and evidence-gathering has kept us in line with SOC 2 criteria.

OneRail also built up a three-year record of zero exceptions (a control not operating as designed). This is a rare achievement that OneRail is proud to have managed.

Putting all of that security expertise to work for its partners, OneRail created a Trust Center to put relevant, real-time security control documentation in clients' hands. This information portal delivers a level of transparency to help companies ensure their business is secure in OneRail's system.

What does all of this mean for you? If you're looking for a partner who takes business security seriously and has the track record and processes to back up that claim, get in touch today to find out how we can help.

OneRail is a last mile delivery orchestration solution providing dependability and speed to help enterprise retailers and distributors meet their delivery promise. Unlike fragmented carrier networks, OneRail brings software and execution together in a single solution, supported by 24/7 operational oversight and a seamlessly integrated managed courier network, enabling brands to lower expenses, increase delivery capabilities and rapidly scale.

Let's talk

Scan the code to contact OneRail

GDPR Compliant

ISO 27001:2022

AICPA SOC 2

HIPPA Compliant

CCPA Compliant