Breaking Up With Third-Party and Supply Chain Risk

Breaking Up With Third-Party and Supply Chain Risk

No business is an island. Every business is connected to other businesses like vendors, service providers, distributors, manufacturers, utilities, government organizations and more. Every time you form a relationship with a new entity, you have to provide them with information about your business — sometimes extremely sensitive financial or proprietary information — and every time you provide your new ally with sensitive business information, you open up another channel of risk.

In 2020, over 90 percent of U.S. businesses experienced a cybersecurity incident, like a data breach, because of a third-party or supply chain fault.

Since it isn't really possible to do business without forming new relationships, that risk is never going to go away. That means it's in your company's best interest to find ways to secure your data and systems against the dangers that can come to your door through third-party or supply chain cybersecurity disasters. Fortunately, we offer an award-winning array of effective and cost-effective security solutions to help you mitigate the danger of third-party or supply chain risk.

I Just Haven't Met You Yet

You've probably heard people use third-party risk and supply chain risk somewhat interchangeably. That may leave you wondering if there's a difference between the two, and if so, how can you tell one from the other?

Well, here's the deal. Third-party and supply chain risks may be similar threats but they have slightly different personalities. However, what they have in common is that they are both major dangers to your business.

Meet Third-Party Risk

This is a broad category that includes risks created by entities that you are not directly purchasing from or selling to. Some examples include:

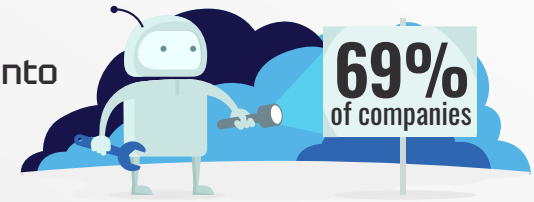
- Government agencies
- Your accountant's MSP
- A charitable organization

Meet Supply Chain Risk

This includes everything that directly impacts your ability to conduct operations, make a product or supply a service. Some examples include:

- The manufacturer of a component you need to make your product
- A business service provider like a payroll processor
- Distributors and vendors

69 percent of companies don't have visibility into their vendors' cybersecurity practices.

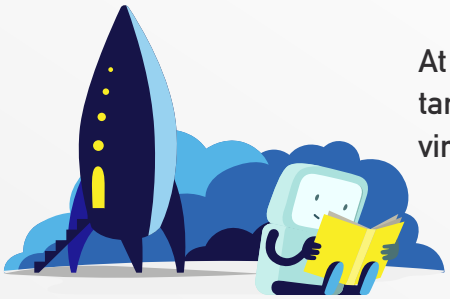


I Knew You Were Trouble When You Walked In

Your risk of trouble from a third-party or supply chain data breach constantly changes based on data supply and demand. If a major world event or development results in increased risk of a cyberattack for one of your vendors, suppliers or business partners, you are also at risk.

We reported extensively on pandemic-related breaches in the newsletter "The Week in Breach". It is easy to follow the pattern and see that as the COVID-19 pandemic evolved and changed, so did cybercrime risk. Bad actors quickly changed targets to industries under pressure by deploying ransomware to shut down operations and stealing data.

From the initial outbreak of the virus to the development of treatments and through the discovery, manufacture and distribution of vaccines, every industry that has been part of the pandemic supply chain has been in danger.



At the beginning of the pandemic, hospitals were at the top of the cybercriminal target list as they sought to steal data to sell about treatments for the virus or score a quick payday by disrupting operations.

As the search for a cure progressed, bad actors shifted their focus to attacking research institutions, like university medical schools and laboratories, in order to acquire the new hot commodity: data about the virus itself.

When the potential for a vaccine entered the picture, cybercriminals turned their eyes to drug companies to steal research and formula data.

Finally, after vaccines started to hit the market, bad actors squeezed one more payday out of the crisis by attacking the specialized cold storage and transport companies that were needed for distribution.

Don't Fall Dangerously in Love – Be Smart About Relationship Risk

The world is in the midst of an unprecedented surge in cybercrime – 80 percent of businesses reported facing an increased number of cyberattacks in 2020. Every attack at every entity that you have a business relationship with opens your organization up to risk that you need to mitigate.

More than 60 percent of data breaches are a result of exposure through third-party or supply chain risk.

Supply chain cybersecurity risk warnings increased by 80 percent in the second quarter of 2020 alone.

In a 2020 survey, 63 percent of companies said their data was potentially compromised within the last twelve months due to a hardware- or silicon-level security breach.

Experts estimate that 17 percent of companies have all of their sensitive files accessible to all of their employees.

Of all data breaches, 30 percent involve internal actors with ill intent, including employees moonlighting by selling data or access on the Dark Web.

Is Your New Partner a Heartbreaker?

Supply chain and third-party risk can be tricky to get a handle on because they are created by circumstances that are beyond your control. Your company's risk for information exposure is dependent on your partner's cybersecurity culture – like how strictly they enforce access controls or if they're using best-practice mitigations, like multifactor authentication, to protect their data.

How easily can one of your service providers or vendors suffer a cybersecurity incident, like a data breach, that puts your company at risk? According to trend-watchers, very easily.

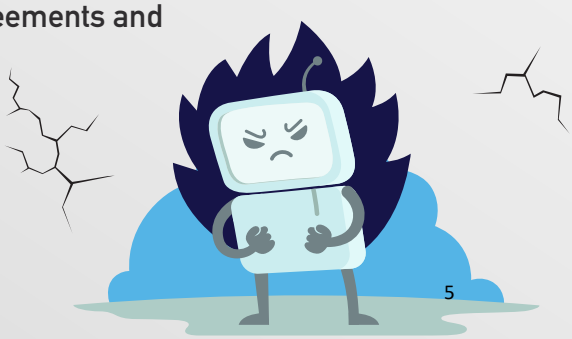
- On average, only 5 percent of company folders are properly protected.
- Data breaches exposed 36 billion records in the first half of 2020.
- About 60 percent of companies have over 500 accounts with non-expiring passwords.
- Of all U.S companies, 41 percent allow employees unrestricted access to sensitive data.
- A new cyberattack is launched every 39 seconds.
- Worse still, your partners aren't always required to tell you if they've had an incident, leaving you wide open to unpleasant surprises.

Anyone Can Have a Bad Romance With a Supplier or Service Provider

A cybersecurity nightmare that results from a third-party or supply chain data breach can happen to any organization – from massive corporations to small businesses – through no fault of your own. Every week, we report on those incidents in "The Week in Breach". As these examples drawn from our reporting demonstrate, it's essential that every organization be prepared for unexpected risk and develop cyber resilience to blunt the impact of another company's data breach.

Tesla & Visser

When the DoppelPaymer ransomware gang launched a successful attack against precision aerospace parts manufacturer Visser, they didn't just get that company's sensitive data. The gang also scored sensitive data about Visser's clients, including Tesla, Space X, Boeing and Lockheed Martin. The stolen records contained correspondence, non-disclosure agreements and even partial schematics.



The National Trust (UK) & Blackbaud

In a breach that reverberated around the world, more than 170 foundations, charitable organizations, schools and medical systems, including the UK National Trust, were impacted by a data theft incident that occurred as part of a repelled ransomware attack at cloud computing provider Blackbaud. In some cases, sensitive information was exposed, like donor lists and records, leading to a ripple effect of trouble across many organizations.

Expedia & Prestige Software

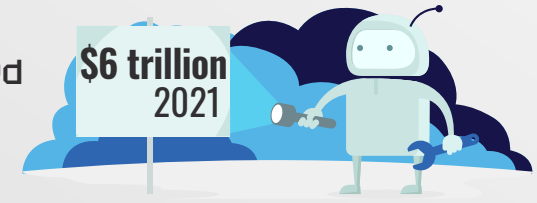
Travel giant Expedia experienced a data breach after Spanish hotel channel manager Prestige Software, a leading travel industry software developer, left over 10 million records from their large hotel booking website clients in an exposed Amazon Web Services S3 data bucket. The 10 million-plus log files dated as far back as 2013 and included names, credit card details, ID numbers and reservation details for clients who booked travel through Expedia as well as other travel sites like Hotels.com and Booking.com

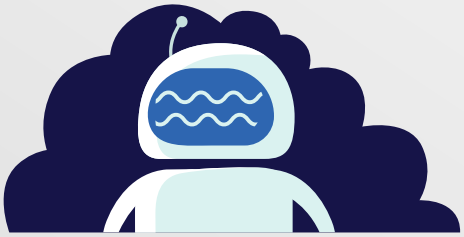
You Can't Buy Love but You Can Buy Great Security for Less

Securing your systems and data against supply chain and third-party risk is vital for your company's success. But you don't have to spend a fortune to do it. Our solutions include many features that provide strong bulwarks against cyberattacks, including mitigations recommended by authorities like the U.S. Cybersecurity & Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST).

- Multifactor authentication (MFA)
- Single sign-on
- Secure identity and access management
- Threat intelligence and reporting
- Security awareness and phishing resistance training

Damage caused by cybercrime is expected to reach $6 trillion in 2021.





Breaking Up With This Risk Isn't Really Hard to Do

Are you ready to break up with third-party and supply chain risk? Not only will we give you a shoulder to cry on, we'll also help you choose the right combination of solutions to kick it to the curb and secure your systems and data.

IntegraMSP
PARTNERSHIPS BUILT ON INTEGRITY