CFGI

VISION AND VALUE:

What You Need To Know To Manage Third-Party Risk

No company is an island.

Businesses have always relied on a variety of third-party partners to help carry out vital functions. From suppliers and distributors to outsourced operational support and more, more and more organizations leverage third-party partners to support their business operations.

In an increasingly online world, this produces complicated digital ecosystems in which organizations need to be very intentional about managing cybersecurity risk among all of these different entities. In this context, third parties include a wide variety of organizations, such as:

- Direct vendors.
- Various "as a service" (XaaS) providers, such as software, platforms or infrastructure.
- Managed service providers (e.g., suppliers installing hardware in data centers).

The core similarity among these various parties is that they're all connected to your current IT systems, meaning their vulnerabilities have an impact on your overall cybersecurity posture.

To execute a comprehensive Third-Party Risk Management program, your business needs to prioritize:

- **Visibility:** You have to gain visibility into security risks across your third-party landscape.
- **Risk:** You must be able to quantify risk levels for each third-party entity so you can make strategic decisions.

We're here to help you bolster your overall vision by providing a window into the threat landscape. We'll also help you learn how to define and interpret the level of risk you need to manage among your third-party partners.

Gaining visibility: Security risks in the third-party landscape

Third-Party Risk Management entails understanding that attackers won't always approach your business directly. Instead, they may compromise individual partners of yours and use that leverage to attack associated entities, including your company.

The kinds of threats you may face through insufficient Third-Party Risk Management are not new. The difference is that outside parties provide attackers with an opportunity to circumvent some of the security precautions you've likely put in place.

In particular, attackers may find weak links among your third-party partners and use them to:

- Compromise your data (e.g. intellectual property) and hold it for ransom against your company.
- Gain unauthorized access to your company's data and systems by implementing targeted and highly effective phishing attacks.
- Exfiltrate and sell data for which your business is responsible.

Fortunately, you can take proactive measures that mitigate your potential exposure to such threats. By working with CFGI and SecurityScorecard, you can benefit from expert research and external technical scans conducted by dedicated cybersecurity experts. We can help you identify risk factors that may leave you vulnerable to these types of attacks.

THREAT 1:

vetting third-party vendors

upward of 1,500 organizations

THREAT 2:

experienced a breach

THREAT 3: Data exposure

Leaked personal information belonging to customers and exposed login credentials are an ever-present reality. Businesses have also been subject to targeted attacks that exposed internal communications and more. In addition to attacking primary targets for specific reasons, a lucrative secondary black market exists for selling passwords and other forms of information, often in bulk. If a user recycles passwords across multiple accounts, this can compound the consequences of having data from an individual account leaked.

From the perspective of Third-Party Risk Management, if one of your vendors or other partners experiences a data breach, the attackers could gain access to your credentials for that specific entity through your third-party provider. If the breached entity housed data for you, that information could be compromised as well. Even in a best-case scenario, the mere fact of having been attached to a high-profile data breach can damage your reputation.

Putting a number to it: Using metrics to assess relative risk

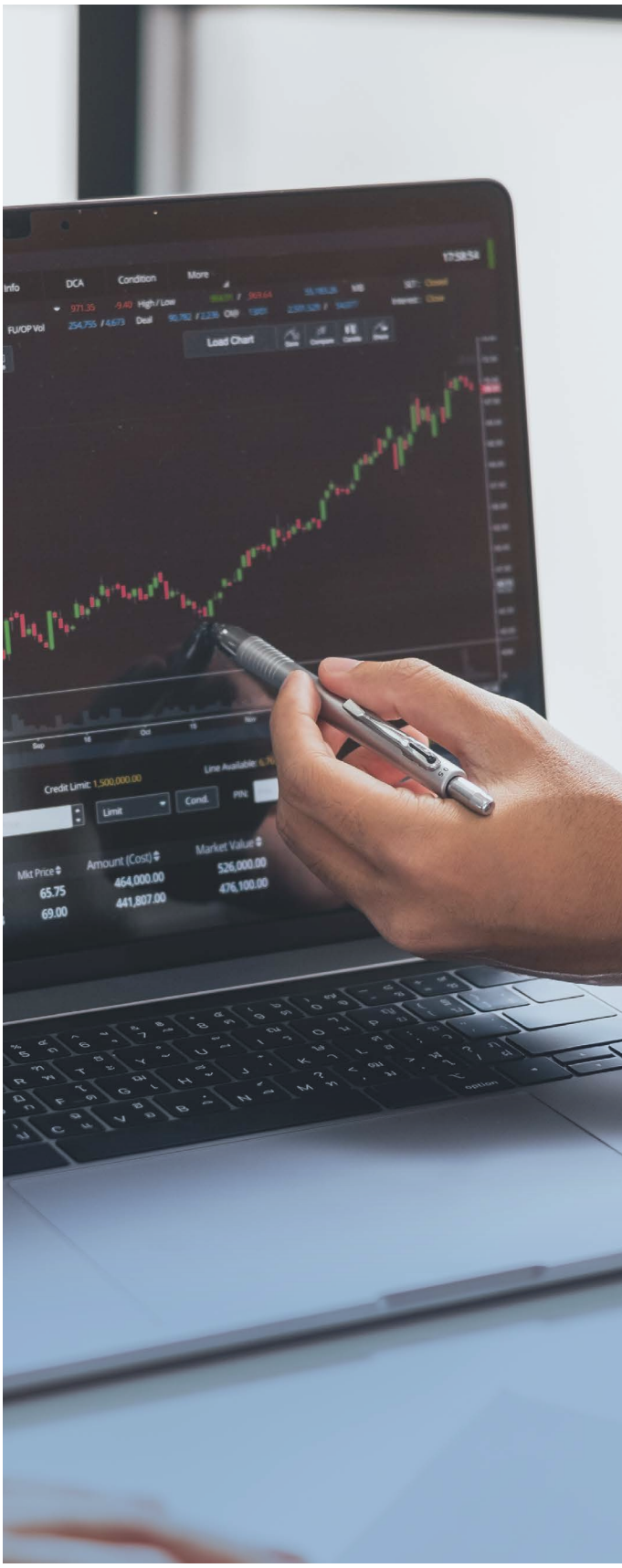
Today's threat landscape demands a mature cybersecurity posture for businesses of all sizes. Small businesses and major corporations alike are susceptible to attacks that are launched using vulnerable third-party entities.

Developing a strategy for assessing risk and working with your partners to mitigate the underlying issues requires a thorough understanding of all the parties within your organization's digital ecosystem.

In partnership with SecurityScorecard, CFGI can help you quantify your partner's cybersecurity health by analyzing **10 different risk factors**. These separate scores are weighted by importance to inform the third party's overall grade.

We'll explore some of these factors below, including one of the most heavily weighted categories, internet protocol (IP) reputation. The other risk factors we'll highlight here are network security, domain name system (DNS) health, patching cadence and information leaks.

Remember, these are just a few of the risk factors that you have to consider when assessing and managing third-party risk. Crucially, putting a number to these values, backed by data and analytics, can help you move from a gut feeling to an elevated cybersecurity posture. With the right approach, you can help protect your organization and safeguard sensitive data.



RISK FACTOR 1: *IP reputation*

Assessing the IP reputation of third-party organizations can help you steer clear of interactions with networks that have been significantly compromised in the past or that may currently be hijacked and used for malware, spam, botnets and other illegitimate purposes.

RISK FACTOR 2: *Network security*

A high number of misconfigured open ports could represent a vulnerability and pose an opportunity for interested criminals. If there's a way in, and there's something valuable on the network, it may only be a matter of time before this risk is exploited.

RISK FACTOR 3: *DNS health*

Even without compromising an email account associated with a third party, attackers may be able to spoof the targeted domain when sending emails to execute a spear-phishing campaign against your business. This is one of the many reasons that companies need to proactively monitor the DNS health of their third-party partners. Confirming that your partner has the proper configurations in place can help boost your own security.

RISK FACTOR 4: *Patching cadence*

Once a particular vulnerability is discovered, vendors will often attempt to release a patch as quickly as possible. Not every system takes advantage of these updates as frequently as it should. When an attacker sizes up a new target, they'll probe for known security shortcomings and exploit any opening they can. Your third-party partner has a responsibility to stay on top of known vulnerabilities with a reliable, and speedy, patching cadence.

RISK FACTOR 5: *Information leaks*

Just as having your own data exposed in a breach can damage your reputation, you should also be aware of any company information from your third-party partners that has been leaked online. Massive breaches and small-scale operations are both potential problem signs. It's important to monitor for these issues at all levels. Discuss with your partner how previous breaches occurred and what's been done about them to prevent the possibility of future incidents.

Objectivity, analysis and strategy

Wherever possible, a robust Third-Party Risk Management program should use objective criteria for measuring these risk factors, both individually and in the aggregate. We've provided a quick overview of some of the important risk factors that influence an assessment of the third-party partner's overall security posture, especially as it pertains to your business.

However, there are still additional risk categories that can affect your partner's overarching score. If the company is repeatedly mentioned in hacker forums, it could indicate that the business is an emerging target, for instance. The third party should also have strong procedures in place for educating users about how to be responsible stewards of organizational data.

Ultimately, the objective of a Third-Party Risk Management operation is to develop security standards and monitor against them to determine the viability of a continued partnership with the outside entity. Proactive outreach can help the two organizations work together to mitigate risk and elevate their cybersecurity operations.

As we've seen, the threats are too numerous, and too consequential, to not prioritize this important component of your overall security posture.

Conclusion

Today's headlines provide a glimpse into the wide and varied threat landscape that's emerging before us. Ransomware targets range from powerful companies that operate vital infrastructure to smaller businesses that were unfortunate enough to be downstream from a successful supply chain attack. With powerful incentives on the line — including a large secondary market for stolen login credentials — there's a strong motivation for attackers to keep scouring for new ways to exploit a variety of different targets. Altogether, this means that you need robust cybersecurity strategies in place to analyze and manage third-party risk.

Vision and value are the two keys to enhancing your cybersecurity posture. You need to see the threat landscape for all that is, and you have to be able to measure the risk you're taking on through third-party partnerships. With these two elements in mind, you can more successfully vet new suppliers while working with your existing partners to help mitigate risk.

It's going to take a joint effort to succeed in this climate.

We've developed a new solution for Third-Party Risk Management. **Contact us today** for a free 30-minute consultation to find out what it's all about.

CFGI

OFFICES

Boston
New York
Philadelphia
San Francisco
Dallas
Washington, D.C.
Stamford
Charlotte
San Diego
Los Angeles

We currently work with clients throughout the US and internationally. Our offices are conveniently located in Boston, New York, Philadelphia, San Francisco, Washington D.C., Dallas, Charlotte, Stamford, San Diego and Los Angeles.

Call or email us today to begin a dialogue. We'll show you how a consulting relationship with CFGI can provide both immediate benefits and lasting effects.

cfgi.com | in