

TOP CONCERNS WHILE

---

# Conducting Cybersecurity Due Diligence for Mergers and Acquisitions



## Cybersecurity should be central to the due diligence process during mergers and acquisitions (M&A) for businesses on both sides of the equation.

Acquirers need to ensure that:

- The M&A transaction won't result in an assumption of unnecessary risk due to the seller's current cybersecurity posture.
- They understand and are adequately prepared for the regulatory requirements of the environment they'll enter as a result of the transaction.
- They're ready to integrate systems with the seller in a secure manner.

For the selling company, it's important to consider:

- How they can get the people, processes and technology involved in their cybersecurity efforts up to a suitable industry standard to enable and justify valuation.
- Which remediation efforts they can prioritize that will have the greatest impact on the M&A process.



For a concise example of how this can all play out, consider the high-profile instance of the merger between Verizon and Yahoo in 2016. Reuters reported the following year that the deal had initially **been delayed** as the two sides came to an agreement over how to adjust the price following Yahoo's disclosure of two data breaches. Verizon ultimately received a discount totaling \$350 million.

If you're part of an acquirer or a seller that's currently involved in some phase of the M&A process, here are the top cybersecurity concerns you need to consider while conducting due diligence.



## Has the seller suffered a data breach?

The price reduction that occurred following the news of Yahoo's data breaches underscores the importance of identifying whether the seller has suffered a data breach.

Because, after all, these attacks do come with a hefty price tag.

IBM's latest report on the subject noted that the **average total cost** of such incidents reached \$4.24 million in 2021, the highest sum in the history of the organization's research on the topic.

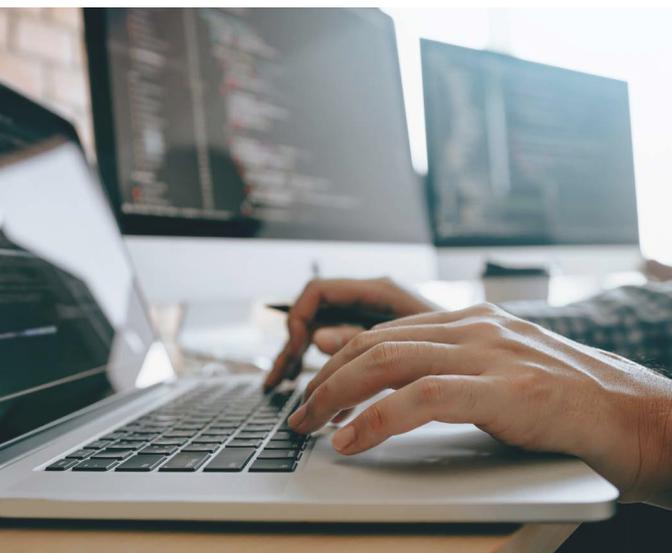
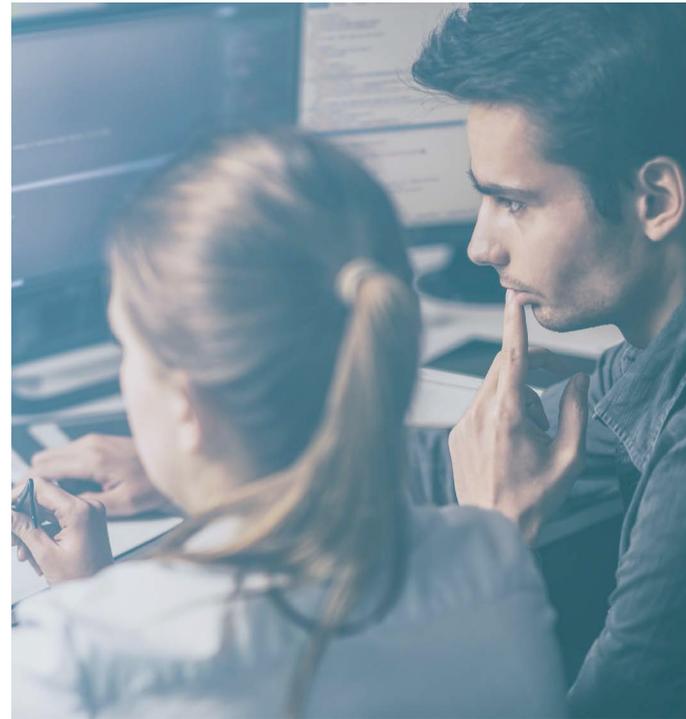
Data breaches may consist of:

- Internal company data that's been exposed to unauthorized parties and even, potentially, the public at large.
- Personal information related to the business's user base or customers, such as their login credentials, credit card numbers and more.

In general, data breaches can lead to reputational damage for the company that's been impacted. Clients and business partners may not feel that their data is secure in the hands of businesses that have been hit with this kind of incident.

This event could also point to an underlying problem with the company's overall cybersecurity posture. How did it happen in the first place? Has the business moved swiftly to contain the damage and elevate its defenses against future threats?

Lastly, once information is leaked, it can persist in venues on the dark web and elsewhere, changing hands multiple times. In other words, a data breach isn't just a flash-in-the-pan event. The effects can linger for a long time.



## Is the seller compliant with the applicable regulations?

After a merger or acquisition, the buyer may be entering a new regulatory landscape. The seller could be in a jurisdiction where the acquirer has not previously operated, making the entity now subject to any data privacy laws that are relevant in that area.

If the seller does not have strong compliance standards and safeguards in place, the acquirer could assume an elevated level of risk, and the stakes are high.

Here are just a few of the pertinent regulatory and industry-standard requirements that should be a potential focus of cybersecurity due diligence:

- **The General Data Protection Regulation (GDPR):** This European Union law imposes specific guidelines on how companies can handle user data, and failure to maintain compliance can result in **large penalties**. As Reuters reported, Amazon recently received an \$886.6 million fine, which the company intends to appeal.
- **The California Consumer Privacy Act (CCPA):** According to the California attorney general's office, the organization started issuing "**notices of alleged noncompliance**" in July 2020. The agency's list of enforcement case examples includes remedies such as updating privacy policies, changing opt-out procedures and ceasing the practice of selling personal information.
- **The Health Insurance Portability and Accountability Act (HIPAA):** HIPAA guidelines cover issues related to privacy, security and breach notification in the medical field, among other concerns. Related to the **HIPAA rules**, the U.S. Department of Health and Human Services noted that, by the end of July 2021, the Office of Civil Rights had "settled or imposed a civil money penalty in 101 cases resulting in a total dollar amount of \$135,328,482.00."
- **Payment Card Industry Data Security Standard (PCI DSS):** These industry-standard guidelines apply to companies that process card payments. Incidents like the **2013 data breach** Target experienced highlight the importance of maintaining compliance with this standard.



## How does the seller manage third-party risk?

While a merger or acquisition may only directly involve two different businesses, the reality is that each company's technology environment likely entails interaction with a wide variety of outside entities.

In this sense, third parties include software as a service (SaaS) solutions and managed service providers as well as general vendors.

In addition to the risk posed by insider threats and external attackers, third parties can serve as the connection point for facilitating malicious activity. Threats range from ransomware to phishing attempts, data theft and more. Through a supply chain attack, bad actors leverage downstream vulnerabilities to work their way through the enterprise ecosystem. Once the two businesses in a merger or acquisition integrate key systems in their digital supply chains, the risk could grow exponentially.

Understanding the seller's approach to managing third-party risk is crucial for ensuring that existing vulnerabilities don't jeopardize the acquirer's new and existing systems. The M&A transaction could provide a prime opportunity, and a new incentive, for attackers to seize on previously discovered openings.





## Is the seller's data stored securely?

On the surface, it's such a simple question, but the answer carries immense weight.

If the seller's data is not stored securely, the potential risks include:

- Insufficient preparation for disaster recovery scenarios, including necessary backup precautions for retrieving data after a ransomware attack.
- Breached personal information for customers and users, including passwords, usernames, phone numbers and dates of birth.
- Theft of business data, potentially including intellectual property, trade secrets and login credentials.

The last point is a vital topic for mergers or acquisitions in which the acquirer has a strong interest in the seller's intellectual property. The threat is real and varied. While some intellectual property theft is motivated by a desire to gain an unfair advantage by stealing from competitors, businesses may also face blackmail attempts.



## What technical security risks are present in the seller's IT environment?

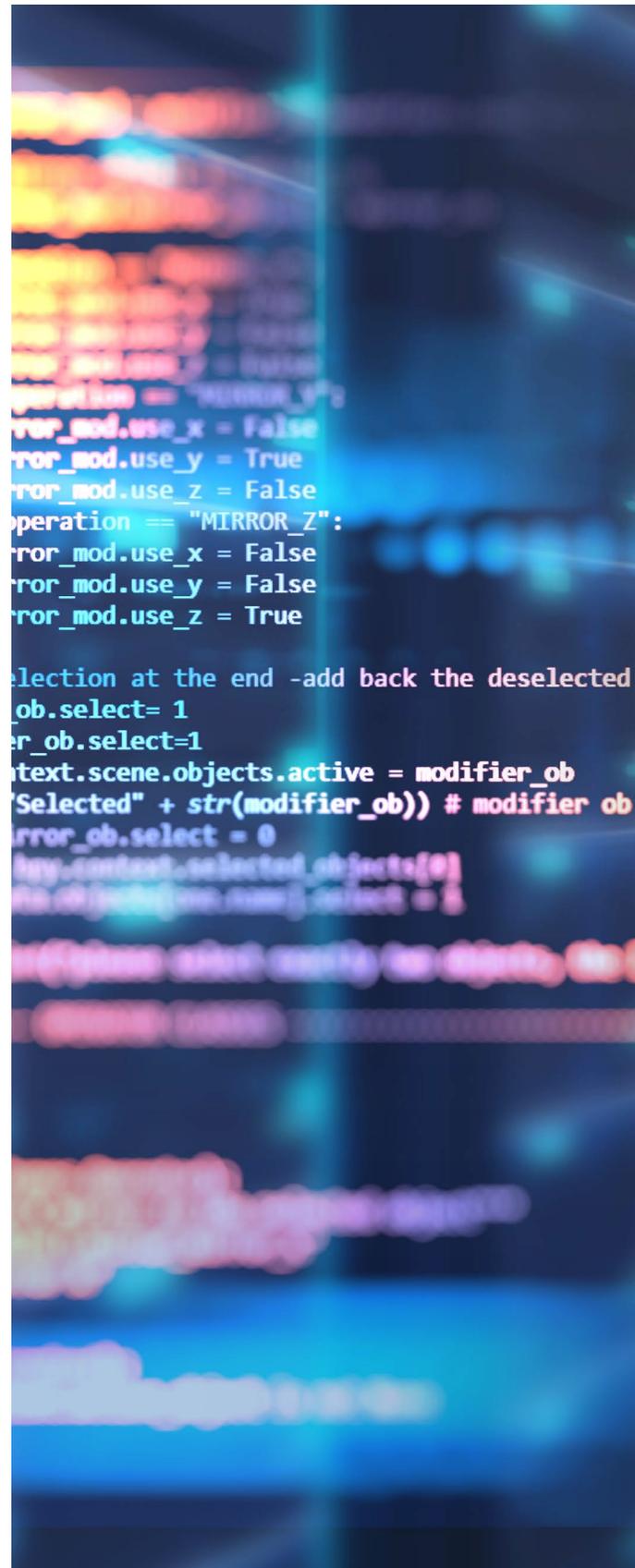
Ensuring that you can maintain and elevate your cybersecurity posture during a merger or acquisition is a crucial aspect of due diligence. Perhaps even more importantly, you have to verify that you won't be introducing new risks after the deal is done. This kind of negative impact may be much more common than you think.

Potential risks to watch for when assessing the seller's IT environment include:

- Data stored in locations that are currently under sanction.
- Unrestricted access to intellectual property.
- Previous data breaches.
- The presence of malware or viruses.
- Improper data classification.
- Weak cybersecurity foundation and protections.
- Absence of an IT security officer.
- Insufficient patent protections for proprietary data.
- Theft of product patents from departing workers.
- Lack of IT security documentation.

Additionally, it's important to ensure that the seller's organizational structure will be able to transition smoothly into the combined company's new state, specifically in regards to the security function.

Without deep insights into the technical security risks of a seller, you can't be sure that you aren't introducing unnecessary risk to the overall organization.



## Is the seller secure?

The answer to this question represents a culmination of all the points we've discussed so far. Security is a relative term, of course, and no company can ever rest on its laurels, but to earn an affirmative response to this essential question, it has to be clear that the seller knows how to manage risk, maintain compliance and secure its data, assets and more.

The seller's cybersecurity posture should provide sufficient assurance to the acquirer that:

- Intellectual property will be safeguarded.
- Systems are secure.
- The proper security controls and systems are in place for protecting day-to-day operations.



If you can't confidently say, "Yes, the seller is secure," this may be a reason for the acquirer to opt out of the acquisition or merger altogether.

Remember, immature security operations from the legacy businesses may impact the combined company somewhere down the road.

According to Reuters, a U.K. agency fined Marriott International Inc. almost \$24 million in October 2020 due to a **large data breach** that began in 2014. Interestingly, it was reported that the initial attack was against Starwood Hotels, which was later acquired by Marriott. After the acquisition, the breach remained undetected for some time. The penalty also only applied to the period following when the GDPR went into effect in 2018.

In this confluence of events, you can see how factors like cybersecurity risk from the seller and new regulations entering the compliance landscape amounted to significant consequences years after an M&A deal was closed.

Put simply, if you can't confidently say that the seller is secure, you have to make sure they can get there, and you must be prepared to assume all of the associated risks. Otherwise, as the potential acquirer, you have to walk away.

Keep in mind that the combined company may need to staff up, which can be difficult in the current climate. A recent report from the Information Systems Security Association (ISSA) found that 62% of cybersecurity professionals surveyed said the leading impact of the industry skills shortage was **growing workloads**. Additionally, more than one-third of respondents stated that burnout and unfilled job requisitions were challenges.



CFGI offers extensive due diligence services for mergers and acquisitions, including cybersecurity support. **Reach out** to our experts today for a 30-minute consultation.

---

# CFGI

## OFFICES

Boston	Washington, D.C.
New York	Stamford
Philadelphia	Charlotte
San Francisco	San Diego
Dallas	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](https://www.cfgi.com) | [in](#)