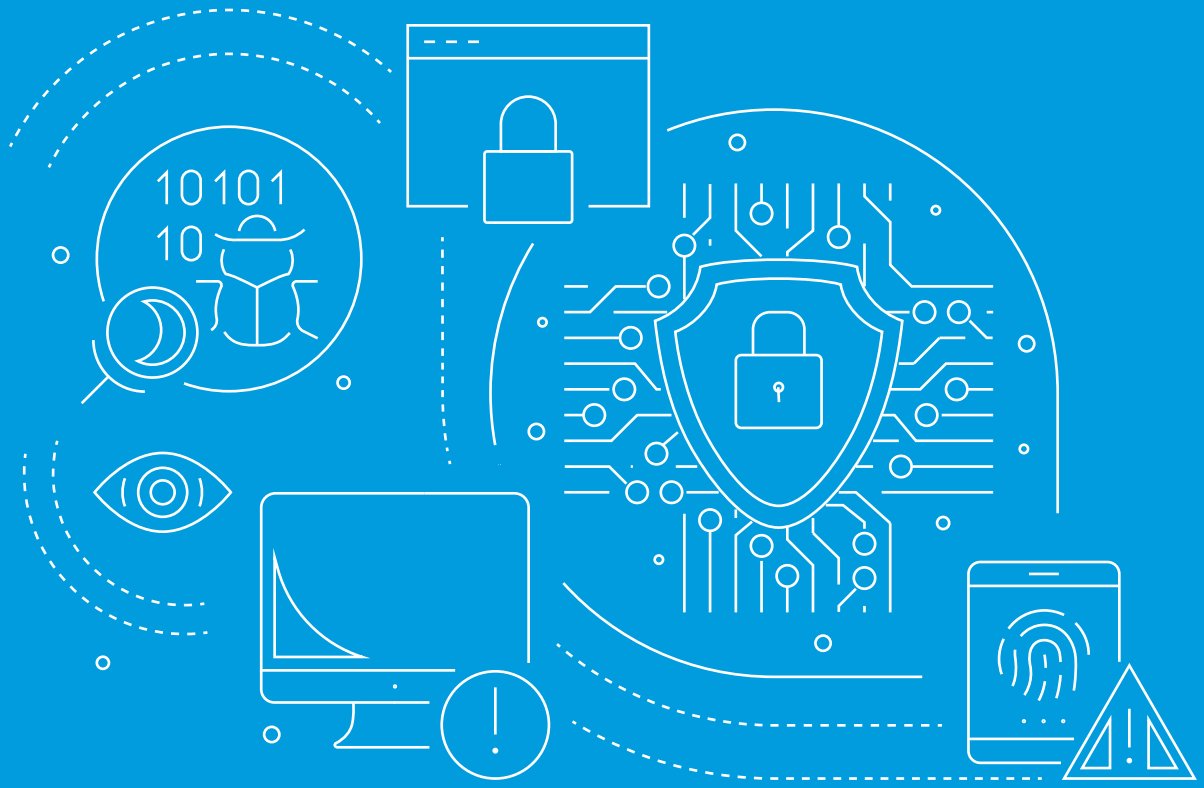


THE IMPORTANCE OF CYBER DUE DILIGENCE

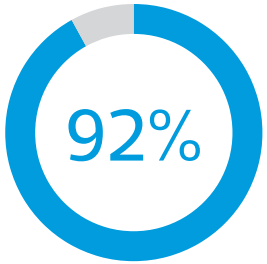
AVOID INHERITING CYBERATTACKS FROM AN M&A TRANSACTION

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

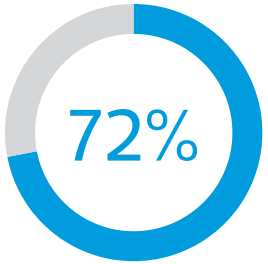
RSM

While the media focuses on high-profile data breaches at large corporations, middle market organizations are not immune to cyber warfare. In fact, the middle market is a prime target for cyberattackers, who understand that businesses in this segment possess valuable data, yet often lack the controls and security teams to protect it.

According to Check Point Software Technologies, cyberattacks increased 40% globally year-over-year in 2021.[1] With cyberattacks on the rise, cybersecurity should be a priority when considering a business acquisition. Ensuring that the target business's data is secure and uncompromised should be a mandatory part of the due diligence process.



Percentage of data breaches in the first 3 months of 2022 that were the result of cyberattacks[2]



Percentage of middle market executives who believe unauthorized users will attempt to access data or systems in 2022[3]

[1] CIO&Leader, "Cyberattacks Increase 40% Globally in 2021: Study," October 11, 2021.

[2] ITRC, "Q1 2022 Data Breach Analysis"

[3] RSM, "2022 Cybersecurity Special Report"

If the target company were to become the victim of a cyberattack, the time, effort and expense required to restore the business can be extensive.

It is important to note that the size of a company does not necessarily have a positive correlation with the potential cybersecurity risk it assumes. In fact, the opposite may be true when looking at the cost of an attack as a percentage of revenue. For companies of any size, the cost of recovering from a cyberattack can run into six figures. For a company with $9 million or less in revenue, potentially 10% of its revenue could be unexpectedly consumed by insufficient cybersecurity protection.

For small and middle market businesses, crisis services between 2016 and 2020 ranged from less than $100 to upward of $120 million.[4]

The average incident cost of a cyberattack in 2020 was $898,000.[5]

The average time to identify and contain an attack in 2020 was 280 days.[6]

[4] NetDiligence, "Cyber Claims Study," 2021 Report

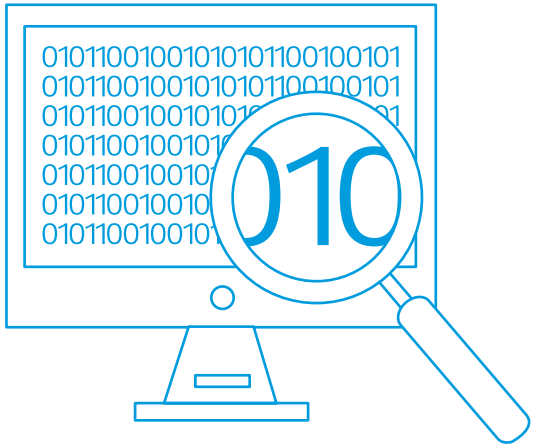
[5] RSM/NetDiligence, "Cyber Claims Study, 2021 Report"

[6] IBM Security, "Cost of a Data Breach Report," 2020

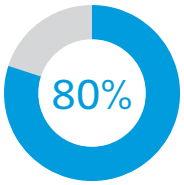
In addition to verifying that a target company is sufficiently protected to guard against future attacks, it is also critical to determine whether that target company's data has already been compromised. One type of data that is a particularly attractive target for hackers is intellectual property.

If obtaining unique intellectual property is a key part of an acquisition plan but that intellectual property has been compromised prior to purchase, then the company's market value is already diminished before the acquisition is complete. Losses like this can add up to millions of dollars, and it is possible that the deal thesis may not be realized.

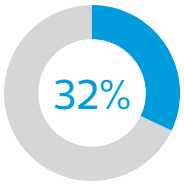
To accurately evaluate the assets and potential revenue that a target company can bring to the table, it is essential to uncover intellectual property impropriety or a breach during the due diligence process when options for recourse are still available.



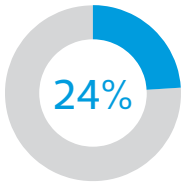
Including intellectual property, these are the five most common data types being breached:[7]



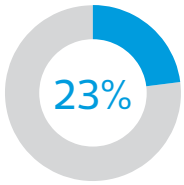
Customers' personally identifiable information



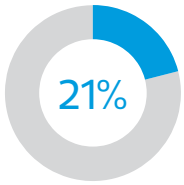
Intellectual property



Anonymized customer data



Other corporate data



Employees' personally identifiable information

[7] IBM Security, "Cost of a Data Breach Report," 2020

One mistake companies can make is assuming that insurance will cover cyber-related losses. At one time, it was relatively easy for businesses to secure cyber liability insurance (CLI), but securing that insurance has become more challenging.

Insurance providers, having incurred significant losses from companies that were victims of cyberattacks (especially ransomware breaches), are now hesitant to take on the excess risk. Businesses that do not already have some type of viable cybersecurity coverage in place are either being denied coverage altogether or are being forced to pay higher premiums.

NEARLY
40%

of middle market organizations fail to carry a cyber insurance policy.[8]

99%

of CLI claims in 2021 were from middle market businesses with less than $2 billion in annual revenue.[9]

[8] RSM, "2022 Cybersecurity Special Report"

[9] RSM/NetDiligence, "Cyber Claims Study, 2021 Report"

Along with increased cybersecurity risk, the data privacy regulatory landscape continues to shift. As a result, middle market businesses are facing additional compliance demands. This may be a particular concern if the target company is based outside the United States.

The European Union's General Data Protection Regulation (GDPR), for example, provided a new standard for how E.U. resident data is collected and stored. This new regulation has prompted a dozen U.S. states to establish some form of data privacy regulations, including the California Consumer Privacy Act (CCPA). It is critical to confirm that the target company is in compliance with any applicable regulations prior to closing the deal.

Only 58% of middle market business executives surveyed were familiar with GDPR requirements.

Of those familiar with GDPR requirements, 96% of middle market executives said they were preparing for emerging privacy legislation.

[10] RSM, "2022 Cybersecurity Special Report"

[11] Ibid

A primary part of cybersecurity due diligence should be a security assessment of the target business. The goal? To understand its current security posture and to identify gaps in its security program.

An assessment can help determine whether there are appropriate security standards in place, including but not limited to the following:

- ISO 27001
- Sarbanes-Oxley Act of 2002 (SOX)
- Federal Information Security Management Act (FISMA)

The assessment can also uncover vulnerable attack vectors. During the review, confirm that all networks and systems have rigorous cybersecurity protocols in place, including protocols for third-party access.

In addition, it is important to determine whether the target company will need major funding to become security-compliant. When a company is preparing to be acquired, it will frequently cut spending to make its financials more desirable to a buyer. This often includes cuts to IT security and maintenance. If the new owner does not realize this until post-sale, it could take years to complete the upgrade and assure proper security strategies and tactics are in place.

In addition to conducting a proper security assessment, another pre-purchase best practice is to answer critical questions regarding the viability of the potential acquisition in terms of security and compliance. These questions include:

- What is it about the business that gives it value, and what is the investment thesis?
- Is that valuable feature well protected and something that cannot be stolen or copied?
- How can you tell if that value has been compromised before you buy the company? After you buy it?
- How can you continually monitor this risk?
- If the business has vulnerabilities or gaps in its security, what will it take to fill the gaps? Is that worth the investment?
- Is the business regulatory-compliant? If not, is it worth bringing it up to compliance? Are there potential penalties for not doing so?
- Is the business in an industry facing potential new regulatory oversight? If not directly, what about its primary partners or customers?

Take action before it's too late

Once the target company's current security posture and threats are exposed, a targeted information security spend can mitigate the potential for a security breach. The benefits of this effort are twofold: The target company will be less attractive to potential cyberattackers, and the deal will be more attractive for the acquiring company.

RSM can help. Through our *M&A360*™ framework, we take a holistic approach across all stages of the investment life cycle. Our team can provide end-to-end deal support and delivery, including comprehensive due diligence.

LEARN MORE

+1 800 274 3978
rsmus.com

eb-nt-rc-all-0822-cybersecurity due diligence

RSM