HORNECYBER

CYBERSECURITY CONSIDERATIONS FOR MERGERS & ACQUISITIONS

Address cybersecurity in due diligence to ensure the long-term value of your investment

For growth-oriented companies and investors looking at potential acquisitions, the process of valuation and due diligence has become increasingly complex. While investors understand the importance of sending in a due diligence team to check financials, it is equally important to send in an experienced cybersecurity team to gain a clear picture of the organization's security posture.

A BREACH CAN DESTROY THE VALUE OF AN ACQUISITION

Cybersecurity has become one of the biggest risks in business today. In 2017 alone, there were 1,579 data breaches reported by organizations - with each breach exposing sensitive or strategic data, disrupting operations, causing financial expenses and legal penalties, as well as damaging customer loyalty and brand reputation.

As data generation increases, so will data breaches. According to Digital Guardian, experts estimate a 4,300 percent increase in annual data generation by 2020, with more than one-third of all data living in or passing through the cloud. ***With such high stakes, investors must place a higher value on the cyber-resilience of a potential acquisition.*** An organization's security posture should be a major factor in its current valuation, as poor cybersecurity has the potential to destroy the long term value of an investment.

A DATA BREACH FOUND AFTER CLOSING COULD EVAPORATE THE VALUE OF THE ACQUISITION.

"If you are an investor or company that is considering an acquisition," explains Josh Edwards, Partner with HORNE's Public and Middle Market team, "consider the damage a security breach could cause to a company's value. If your systems are breached and sensitive data is leaked a day after closing, ***the acquisition value could evaporate."***

Yahoo faced this situation in 2017. After disclosing two massive data breaches, some of the largest in history, Verizon acquired the web services provider for $350 million less than originally agreed upon. While Verizon completed the acquisition, the two data breaches could have cost Yahoo the entire transaction, a deal worth much more than the lost $350 million.

MID-SIZED COMPANIES ARE PRIME TARGETS FOR HACKERS

Security breaches don't just hit large global corporations like Yahoo and Under Armour. Verizon's Data Breach Investigations Report found that 58% of all cyber attacks target small to mid-size businesses. "Many mid-sized companies think they are immune to real world threats," continues Edwards, "but what they may not realize is that they are a prime target."

Today's hackers are organized and persistent. They know that small and mid-sized companies are often not able to devote the same resources to cybersecurity as large, public companies. Hackers often target mid-sized companies as an avenue to larger companies, as exemplified by the Target breach a few years ago. Credit and debit card access for 40 million Target customers was compromised through a data connection between Target and an HVAC contractor.

MAKE CYBERSECURITY PART OF DUE DILIGENCE

When reviewing a potential merger or acquisition target, good financial and operational due diligence is important. Although items missed during this process can be irritating, many times the investor can either be made whole based on purchase contract provisions or can solve the issue going forward without significant cost.

The opposite is true with cybersecurity. Cyber-resilience is critical. Attacks occurring after the close of a transaction, or unknown attacks committed prior to the close of the transaction, are costly to resolve and typically hard to include under indemnity provisions.

EXTERNAL PROTECTION ALONE IS NOT ENOUGH

When assessing an organization's security posture, do not assume that having protection from external attackers is enough to provide security. "Many companies believe that having security solutions in place is enough to ward off attackers. However, it only takes one weak link to grant a cybercriminal access to the internal systems," says Edwards.

Companies must address insider threats, such as human error - a frequent cause of security breaches. ***A prime time for hackers to strike is immediately after an acquisition or merger.*** New organizations, employee names and titles often cause uncertainty and confusion, which creates an easier environment to trick employees into providing credentials or sharing sensitive data.

Phishing is just one method employed by cybercriminals to gain access to sensitive data and network systems. With ever evolving attack methods, identifying all security vulnerabilities during the due diligence process is often an unreasonable goal. However, reviewing the acquisition target's system security posture through Advanced Penetration Testing, cyber education, and current policies and procedures can often identify vulnerabilities and significantly reduce the likelihood of a future attack.

COMPLIANCE DOES NOT EQUAL SECURITY

Many companies face mandatory security regulations. A common mistake is assuming that a target's compliance provides ample security against threats. The regulatory environment for most industries moves at a slow pace. The formation and approval of new regulatory requirements can take months, if not years.

The fast paced world of cybersecurity often results in regulatory guidelines being issued well after specific threats have been identified. Compliance is necessary to establish baseline security features and ensure no fines or penalties from regulators are imminent. However, being satisfied with bare-minimum compliance can jeopardize the investment of a merger or acquisition.

THIRD PARTIES MUST MEET CYBERSECURITY STANDARDS

According to Opus and Ponemon Institute's 2018 study, 61 percent of organizations have experienced a data breach caused by a vendor or third party. Weaknesses in business partners' systems with direct connection to the acquisition target serve as open doors to hackers. When assessing the cyber-resilience of an acquisition target, remember to look at connected vendors, third parties, cloud applications, and business partners to ensure they follow cybersecurity best practices.

HOW DO YOU KNOW?

The best way to gain true understanding of a merger or acquisition target's security posture is to employ an outside cybersecurity firm to conduct an assessment.

There are many current security assessment approaches. Companies can get confused and overwhelmed when considering the options and associated costs. Vulnerability scans are low-cost tools for quickly checking systems against a public list of known threats. However, scans are automated, broad, and shallow - and do not tell the whole story.

Instead, consider running an offensive, Advanced Penetration Test. By emulating the attack methods of real attackers - with human talent driving the decision making and execution - Advanced Penetration Testing provides a comprehensive look at an organization's unique vulnerabilities through the lens of a hacker. Partnering with a team of Advanced Penetration Testers helps ensure the investment of your transaction.

TODAY'S THREAT LANDSCAPE

Today's cyber risks threaten more than customer data. Hackers no attack security cameras, door locks, copiers, scanners, HVAC systems, and physical assets to leverage them for access to valuable corporate data. Advanced Penetration Testing finds risks "below the surface", allowing organization's to strengthen security around data, operations, physical assets, and most importantly - brand reputation.

PREPARE FOR POST M&A

Mergers and acquisitions create new opportunities for hackers. Corporate transactions change your IT infrastructure and processes, creating gaps in information security systems, policies, procedures, and safeguards. The newly combined organization is now vulnerable to new cyber risks.

These changes often come with headcount reductions or shifts which could activate disgruntled employees familiar with the acquired organization's systems, processes, and security measures to wreak havoc. We recommend companies do their due diligence during the transaction process so that the best measures are in place to ensure smooth system integration and mitigation of internal security risks.

CONCLUSION

Today's threat landscape changes how investors and prospective acquiring parties should value and assess an organization being considered for a merger or acquisition. It is equally critical to send in an experienced cybersecurity team to uncover vulnerabilities, past breaches, and hidden risks as it is to send in a due diligence team to check financials prior to a transaction. ***A clear picture of an organization's security posture must be obtained to ensure the value of the purchase is protected.***

M&A CHECKLIST TO ENSURE CYBER-RESILIENCE

1. **Understand how cyber-resilience affects long-term value of an investment**
2. **Include cybersecurity audits in due diligence**
3. **Hire outside cyber expertise for guidance and advisory**
4. **Conduct Advanced Penetration Testing - not just scan-based assessments**
5. **Test internal and external security posture**
6. **Assess the IT controls around sensitive data**
7. **Run background checks on system administrators**
8. **Review cyber insurance policies and contracts**
9. **Audit all vendors and third-party business partners to assess security posture**
10. **Implement policies and procedures to ensure proper security within new entity**

ABOUT HORNE CYBER

At HORNE, our greatest strength is our people. As an accounting firm, our assurance team consists of CPAs and cybersecurity experts with more than 10 years of experience in providing IT assurance and security services to our clients. Our team's unique composition marries financial and information technology expertise with an offense-oriented approach to cybersecurity. HORNE Cyber's offense-oriented approach to cybersecurity uncovers hidden cyber risks and significantly reduces exposure to security threats, allowing clients to stay compliant with ever-changing regulations and use technology as a lever for growth.

For more information, visit www.HORNECyber.com.

HEAR IT FROM OUR CLIENTS

"HORNE Cyber's team exceeded our expectations. HORNE's passion for information security, and their knowledge of cybersecurity, truly enhanced our experience. We look forward to working with HORNE Cyber on future cybersecurity engagements. We would recommend HORNE Cyber for any organization looking to test their preparedness and enhance their cybersecurity."

- Dave Stende, CEO/Managing Partner, Eide Bailly

HORNECYBER

HORNECYBER.COM