HORNE

CYBERSECURITY CONSIDERATIONS FOR M&A

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

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 the financials, it is equally important to send in an experienced team to gain a clear picture of the organization's cybersecurity posture.

A BREACH CAN DESTROY THE VALUE OF THE ACQUISITION

Cybersecurity has become one of the biggest risks in business today. In 2015, security incidents increased 30% – with each breach exposing sensitive or strategic data, disrupting operations, incurring financial expenses and legal penalties, as well as damaging customer loyalty, brand and personal reputation. There is much at stake because any of these outcomes could impact a company's brand value and bottom line.

INVESTORS MUST PLACE A HIGHER VALUE ON THE CYBER RESILIENCE OF A POTENTIAL ACQUISITION.

Investors must place a higher value on the cyber resilience of a potential acquisition. How well an organization is protected from cyber threats should factor into its current valuation and could even destroy the long term value of the investment.

"If you are an investor or a company that is considering an acquisition," explains Josh Edwards, Senior Manager with HORNE's Public and Middle Market Transaction Services group, "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."

TripAdvisor faced this situation in 2014. Shortly after its $200 million acquisition of travel site Viator, attackers breached the information of 1.4 million customers. TripAdvisor did not uncover the breach themselves, but rather when its payment card service started receiving unauthorized charges on customer credit cards. This breach resulted in significant remediation costs for TripAdvisor and had immediate impact on its stock price and reputation.

MID-SIZED COMPANIES ARE PRIME TARGETS FOR HACKERS

Security breaches don't just hit large global corporations. Last year, 71% of cyberattacks struck businesses with less than 100 employees. "Many mid-sized companies think they are immune to the threats of cyber hackers," 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 do not devote the same resources to cybersecurity as large, public

companies do. So hackers often attack mid-size companies to find easy access into larger ones. This is what happened to Target in 2013. 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 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 solve the issue going forward without significant cost.

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

When exploring an acquisition, gaining a clear understanding of the target's cyber strength must be a key part of the due diligence process. The cybersecurity measures taken by an acquisition target to secure their systems should impact their valuation, risk profile and overall assessment of operational strength.

EXTERNAL PROTECTION ALONE IS NOT ADEQUATE

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

Companies must address internal threats such as human error – which is 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 system access or sharing sensitive data.

Phishing is just one method employed by cybercriminals in gaining access to sensitive data and systems. With ever evolving potential threats, identifying all security vulnerabilities during the due diligence process is often an unreasonable goal. However, reviewing the acquisition target's system security through advanced penetration testing, cyber education process and current policies and procedures can often identify vulnerabilities that significantly increase the likelihood of a past unknown or future penetration.

COMPLIANCE DOES NOT EQUAL SECURITY

Many companies face mandatory security regulations. A common mistake is assuming that a target's security 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.

In the quickly evolving world of cybersecurity, this environment results in regulatory guidelines being issued well after the threats have been first identified. Ensuring compliance is necessary to establish that baseline security features are in place and that no fines or penalties from regulators are imminent. Modern hackers are advanced and persistent. Being satisfied with minimum compliance can ultimately put the investment at risk.

THIRD-PARTIES MUST MEET CYBERSECURITY STANDARDS

In 2015, 63% of data breaches were linked to a third-party business partner. Weaknesses in business partner systems with direct connections into the acquisition target, can become an open door to hackers. When assessing the cyber resiliency of an acquisition target, remember to look at connected third parties, cloud applications and business partner integration to ensure they follow cybersecurity best practices.

HOW DO YOU KNOW?

The best way to gain true understanding of an acquisition target's cyber strength is to employ an outside, unbiased cyber team to test the external and internal protection and procedures.

There are many current assessment approaches and companies can get confused when considering the options and the costs. Vulnerability scans or assessments are low-cost tools for scanning systems against a list of known threats. They are automated, broad and shallow – and do not tell the whole story.

Instead, consider running an offensive, advanced penetration test. By attacking the network just as a real advanced threat group would – with human talent driving the decision making and execution – penetration testing will more exhaustively test the attack surface than an automated tool using a list of vulnerabilities.

Advanced penetration tests identify and intensively test a set of vulnerabilities in an organization that can lead to a compromise by a real attacker, in a real-world scenario. Partnering with a team of advanced penetration testers empowers IT teams with relevant, real-word solutions.

With the rise of the Internet of Things, there are an increasing number of systems that have web connections - security cameras, company conference systems, printers, HVAC systems, and more. Hackers can gain access into a company's internal system through any system connected to the internet. Imagine the risk of cybercriminals listening in to company meetings or reading every document printed. Advanced penetration tests will uncover these weak links and help you avoid an acquisition that is at high risk of breach.

PREPARE FOR POST-M&A

Mergers and acquisitions create new opportunities for hackers. As you acquire a new company or combine several entities, these corporate transactions change your IT infrastructure and processes, creating gaps in information security systems, policies, procedures and safeguards. The new combined organization is now vulnerable to new risk.

Also, these changes often come with headcount reductions or shifts which could activate disgruntled current or ex-employees that are familiar with the systems, processes and security measures to wreak havoc on the organization. We recommend that companies need to do their homework during the transaction process so that the best measures are in place to ensure smooth system integration while managing the human side to minimize internal security risk.

CONCLUSION

For investors and prospective acquiring parties, today's rise in cyber threats changes how you should value and assess an organization. Equally critical to sending in a diligence team to check the financials, is the need for sending in an experienced cyber team. A clear picture of an organization's cybersecurity posture must be obtained to ensure the value that is being purchased is protected.

M&A CHECKLIST TO ENSURE CYBER RESILIENCE

1. Understand how cyber resilience affects long-term value
2. Include cybersecurity audits in due diligence
3. Hire outside cyber expertise
4. Realize compliance is only baseline protection
5. Conduct advanced penetration tests – not just scan-based assessments
6. Test internal as well as external cyber resiliency
7. Look at the controls around the data
8. Run background checks on system administrators
9. Review cyber insurance policies and contracts
10. Audit cyber resiliency of all third-party business partners
11. Implement plans and procedures to ensure cybersecurity of new entity

---

ABOUT HORNE LLP

HORNE LLP goes beyond traditional accounting services to steer clients through the uncertainties and opportunities ahead. The HORNE Public and Middle Market Transaction Services practice helps clients navigate the transaction lifecycle by offering a comprehensive suite of valuation, due diligence and operational services.

Our HORNE Cyber Solutions team provides experienced guidance to ensure its clients' investments are well protected from security risks and retain their value for the long term. For more information, visit **www.hornecyber.com**.

JOIN THE CONVERSATION

Blog.HORNELLP.com/Waypoints

Blog.HORNELLP.com/Cyber

www.linkedin.com/company/HORNE-Public-&-Middle-Market

www.linkedin.com/company/HORNE-Cyber-Solutions

@HORNE_PMM

@HORNECyber

HORNE