Courtesy of
SCS Agency Inc

CYBERRISKS&LIABILITIES_

Best Practices for Cyber Risk Management During Mergers and Acquisitions

In the modern business world, where technology and digital integration play a crucial role, managing cyber risks during mergers and acquisitions (M&A) is of utmost importance. Undetected or undisclosed cyberthreats can pose significant dangers to the seamless integration of two entities, but the excitement of new opportunities can often overshadow the potential cybersecurity threats that exist.

This article provides information on common cyber risks during an M&A and offers best practices for managing them before, during and after the process.

Understanding Cyber Risk Landscape in M&A
As organizations engage in M&A, it is crucial to have a comprehensive understanding of the various threats that can impact the success of a deal. For example, data security should be a top priority, as it must be ensured that integrating different information systems does not pose a risk of exposing sensitive data to potential breaches. Regulatory compliance is equally critical to avoid severe legal consequences and financial penalties.

As assets are transferred, intellectual property (IP) protection takes on greater importance, and measures must be taken to safeguard proprietary information from compromise. Furthermore, third-party risks arising from the extended network of suppliers, partners and service providers can introduce vulnerabilities that may be exploited during an M&A transition.

M&A cyber incidents can cause financial and reputational harm. Breaches can erode trust and attract fines and legal liabilities. To avoid these risks, a comprehensive approach to cyber risk assessment and mitigation is crucial. It ensures the financial viability and reputation of the entities involved.

Pre-M&A Cybersecurity Best Practices
Cybersecurity risk mitigation strategies should be utilized during all phases of an M&A. Best practices for the acquiring business to consider before the M&A process begins include:

- **Conducting a comprehensive cyber risk assessment of the target company.** Such an assessment can help identify existing vulnerabilities and weaknesses and provide an opportunity to evaluate the target company's cybersecurity policies and practices.
- **Reviewing applicable laws and regulations.** This can help ensure compliance with data protection laws and assist in avoiding legal issues regarding intellectual property rights concerning copyrights, trademarks and patents. It can also help the acquiring business avoid noncompliance penalties and fines.
- **Assessing the cost of cyber risk mitigation.** Knowing the cost can help a business determine the expenses and time associated with addressing the cybersecurity issues that impact the M&A. That information can be useful in negotiating the M&A price or deciding if the deal should ultimately go through.
- **Involving cyber risk experts in due diligence while utilizing passive threat hunting.** Engaging with experts can help an organization detect additional exposures in a timely manner and calculate the probability of cybersecurity incidents occurring.

SCS AGENCY INSURANCE

Cybersecurity Best Practices During the M&A
Once the M&A process begins, the acquiring company should take additional steps to mitigate cyber risks. These include:

- **Involving the cybersecurity team from the outset**—Including the cybersecurity team from the start of the M&A process allows individuals with the proper tools and knowledge to be engaged from the start, allowing them the opportunity to gather information needed to detect and mitigate threats.
- **Considering the kind of integration occurring**—Knowing the type of integration enables the acquiring firm to tailor their risk management strategies to the different cyber risks surrounding a full, hybrid or soft integration.
- **Standardizing the information security procedures of the two companies and establishing agreed-upon roles**—This can help improve risk management efficiencies and effectiveness as the two entities come together.
- **Creating an asset inventory**—Having such an inventory can make it easier to keep track of and monitor hardware, software and data vulnerabilities.
- **Analyzing vendor risks**—Knowing these risks can help the acquiring business gain a more complete picture of the cybersecurity posture of third-party partners, helping mitigate potential threats and vulnerabilities that may be inherited.
- **Identifying specific attack risks and potential vulnerabilities**—Being aware of potential exposures allows the acquiring firm to assess the risk profile and security posture of the target firm.

It is also essential to communicate the cyber risks to stakeholders and to maintain transparency with shareholders, employees and customers during an M&A. Developing a communication plan for post-merger cyber incidents is also necessary.

Post-M&A Cybersecurity Best Practices
Once an M&A deal has been signed, the acquiring company should be able to search more thoroughly for cyber risks associated with the target company. Potential actions the acquiring firm could take include engaging in active threat hunting or looking for exploitable security vulnerabilities through penetration testing. It is also important to constantly monitor for cyberthreats, utilize endpoint detection and response strategies, and establish policies to continuously handle incidents as they arise.

As with the other stages of an M&A, communication remains key; it is crucial to educate and train employees on any new or updated cybersecurity policies and procedures.

Conclusion
An M&A can present a business with several cybersecurity risks. By implementing cybersecurity best practices before, during and after the transaction, a business can mitigate its cyber exposures and build systems that can help detect and prevent future issues.

For more information on managing cyber risk, contact us today.