KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Digital Assets: Cybersecurity Considerations in an Acquisition

By Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE, Principal,
Cyber Risk Management

In today's business environment, almost all companies have become increasingly reliant on Information Technology systems and digital data in some way. From calculating financials, supporting operations, to being a consumer product, technology can sometimes touch every facet of a business. While these technologies often help drive efficiencies, increase productivity and reduce costs, they also introduce new vulnerabilities that can cause significant harm to a business and its shareholders.

When conducting an M&A transaction, due diligence is a core requirement in assessing the potential risks of the transaction. The due diligence process will determine the outcome of three key areas: valuation, representations and warranties, and, ultimately, the completion or termination of the deal. Historically, the due diligence process has focused on the following traditional risk areas: financial, legal, commercial, management, intellectual property, insurance and environmental.

While these areas are essential, in today's business environment that list is no longer complete without the consideration of cybersecurity.

Cyber Asset Risk Points

For a successful M&A transaction, cybersecurity now needs to be front and center. When buying a company, you are buying not only its physical assets, but its digital assets. It is in those digital assets that significant risk can exist. These risks can include things such as:

- **Theft of intellectual property** – Intellectual property might be the main driver of the interest in the transaction and the driver of the valuation. If not properly restricted from cyber threats, that intellectual property could easily be exposed to competitors.
- **Breach of personal data** – Personal data is almost universally regulated in some form. A cyber breach of personal data can result in regulatory fines, private rights of action, and devaluation as a result of lost consumer confidence.
- **Failure of mission critical systems** – With the rise of Ransomware over the last year, many organizations sustained significant financial losses and failed to recover. After completing an M&A transaction, it would be catastrophic to learn that the acquired company needs to close its doors because it didn't properly prepare for a Ransomware type attack and all of its digital assets are lost.
- **Compliance risk** – Depending on the company being acquired and the industry in which it operates, it could have strict regulatory obligations, such as healthcare with HIPAA or hospitality with PCI-DSS. If the acquired company is not meeting its compliance obligations, this could result in significant monetary penalties and reputational damage.
- **Remediation costs** – If the acquiring company requires a significant amount of remediation to address security concerns and regulatory compliance, these need to be identified and factored into the valuation.

When thinking about the potential cyber risks, one thing is certain — it will impact the valuation, how you proceed with the transaction and ensure appropriate post-transaction safeguards, such as indemnifications.

Cyber Due Diligence Factors

The extent of the cybersecurity due diligence process is going to depend on many factors, such as the role IT plays in the organization; however, common approaches include:

- Questionnaires and documentation review.
- Assessments by third parties.
- Penetration and vulnerability testing.

When performing the cybersecurity due diligence, the assessor must consider not only the existing cyber program, but also the past and the future. If an entity, in preparation for sale only, recently invested in creating a cybersecurity program, a significant amount of historic risk may go unaccounted for. While on the surface, questionnaires and documentation may look reasonable as a result of the recent investments, they will not be a true indication of the total risk and may be misleading. To that end, questionnaires and documentation reviews should only be considered as the starting point to the cybersecurity due diligence process. What may vary is the extensiveness of the follow-up post-documentation review.

Having a structured and planned approach to the cybersecurity due diligence process will help ensure that it is efficient, effective and complements the overall risk review across all areas. You will likely find that IT underpins almost all areas of the business. The cybersecurity due diligence process should not operate in a silo, but must take into consideration the context of the entire business, the role it plays in supporting the business, and the value of the data it consumes and produces.

Cyber Due Diligence Steps

As part of any cybersecurity due diligence process, we recommend the following approach:

- Evaluate the ability of your M&A due diligence team to assess the IT and cybersecurity risks.
- Identify all digital assets of value to the company and the importance of those assets in determining its overall valuation.
- Evaluate how those digital assets are protected — now and in the past.
- Establish clear ownership of those assets; for example, if the company is a software based company, ensure it legally owns all rights to that source code.
- Identify if the company has any regulatory data protection obligations and evaluate the extent to which the company is in compliance.
- Identify if the company has a cybersecurity program and evaluate the sophistication and maturity of that program.
- Identify if the business has had any cybersecurity incidents or breaches and their resulting impact. Is there a breach they are aware of that they have not yet reported?
- Identify any dependencies and the extent in which third parties are used and relied upon.
- Evaluate the state of the overall IT infrastructure. Is it outdated and in need of significant investments to continue operations?
- Evaluate the potential complexity of integration and the associated costs and risks.
- Compile all the facts from the above and establish what should be included as representations and warranties in the definitive acquisition agreement.

M&A Cyber Support

The importance of the role cybersecurity will play in the future of M&A transactions is only going to increase. While cyber due diligence may seem overwhelming, consider the use of a third party to assist in the cybersecurity and IT due diligence process. Such third party insight is beneficial to both the buyer and seller as it allows for an unbiased opinion.

Contact Us

At PKF O'Connor Davies, LLP, we have experienced professionals who specialize in business valuations, cybersecurity, IT risk, operations, governance and strategy. If you have any questions, please contact Tom DeMayo at 646.449.6353 or tdemayo@pkfod.com.

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, nine offices in New York, New Jersey, Connecticut and Maryland, and more than 700 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 28th on *Accounting Today's* 2017 "Top 100 Firms" list and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by *Accounting Today.* In 2017, PKF O'Connor Davies was named one of the 50 best accounting employers to work for in North America, by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.

Our Firm provides the information in this e-newsletter for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.