Securities
Regulation Daily

Wolters Kluwer

August 5, 2020

Mergers & Acquisitions: Cybersecurity Traps for the Seller & Buyer

*By Alan S. Wernick, Esq.**

If you, someone you know, or your client is considering buying or selling a business, why should you or they care about privacy/cybersecurity issues? Imagine a scenario where the merger/acquisition ("M&A") deal you've been working on for months is about to close in 48 hours and the seller's C-suite officers get a short urgent message from their "IT Guy" (the person responsible for managing their information technology infrastructure): "I think we've been hacked."

This article briefly discusses some actual M&A transactions where a data breach impacted the transaction, some anecdotal observations from the C-Suite, costs related to the data breach, and some due diligence considerations.

Impact of a Data Breach on an M&A Transaction

After you resume breathing and your heart starts pumping again (perhaps slightly faster than before you received the message from the IT Guy), you might then recall news headlines you glanced over about cybersecurity breaches that occurred shortly before or after their M&A closing:

- Verizon Communications Inc.'s acquisition of Yahoo's Internet properties: 2017, $350 million valuation discount after security breaches discovered before the deal closed. Over $47 million in litigation expenses related to the data breach.
- Marriott International Inc.'s, acquisition of Starwood: 2016, $12.2 billion acquisition. Starwood data breach allegedly compromised information of more than 300 million people. On July 9, 2019, the U.K.'s Information Commissioner's Office ("ICO") announced its intention to fine Marriott more than $122 million related to the Starwood Hotels data breach. The ICO's announcement states, "The ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems."

---

* **Alan S. Wernick,** Of Counsel at Aronberg Goldgehn, is an experienced business transactions attorney, advocate, and arbitrator/mediator handling legal matters for businesses in the areas of information technology, privacy/cybersecurity and intellectual property. He has an extensive track record advising organizations acquiring, using and selling/licensing technologies and related services, including the drafting and negotiation of a variety of technology and commercial agreements; data privacy/cybersecurity compliance and remediation, including responding to data breaches; IP protection; mergers and acquisitions due diligence; compliance processes, procedures and policies. Additional information is available at his LinkedIn profile: www.linkedin.com/in/alanwernick or at his bio on his law firm's website: agdglaw.com. Alan can be reached at 312.755.3172 or AWernick@agdglaw.com.

- Spirit AeroSystems Holdings, Inc.'s planned acquisition of Asco Industries: May 2018 purchase agreement executed, then Asco's C-suite discovered it was a victim of a large-scale ransomware attack disrupting Asco's business in multiple countries. A July 14, 2019, SEC 8-K filing[1] by Spirit AeroSystems stated that the parties entered into an amendment to the purchase agreement to address several issues including (1) extending the time for the parties to automatically terminate in the event that conditions to the acquisition were not satisfied or waived; (2) addressing the cyber-attack by requiring Asco to promptly provide to Spirit all information in its possession relating to the cyber-attack and indemnify Spirit for up to $150 million in damages resulting from the cyber-attack; and (3) providing that the amendment did not constitute a waiver of any party's right to allege that the adverse consequences of the cyber-attack created a "Material Adverse Change" under the purchase agreement, the occurrence of which would permit any party to terminate the purchase agreement upon five business days' notice to the other parties.

The Cost of a Data Breach

In addition to lower valuations and other expenses related to a data breach, there's also the risk of potential fines from government regulators, as indicated by the 2019 ICO announcement concerning Marriott.

According to the 2019 14th Annual Cost of a Data Breach Study[2] by the Ponemon Institute, the global average cost of a data breach was $3.92 million. For the United States the average total cost of a data breach was $8.19 million – an increase of 130% over the 14 years of the study. Breaking that down to a per data record cost, the average total global cost for each lost or stolen data record containing confidential and/or sensitive information (e.g., Personal Identifying Information, trade secrets, etc.) was $150 per record. For the United States the average cost was $242 per record.

How many data records is your business the steward of for your customers, your vendors, plus your own proprietary business records? Do the math. Then consider how many devices (e.g., desktop computers, laptop computers, mobile devices, etc.) and third parties (e.g., vendors, customers) have access to that data and the level of security protecting those devices from unauthorized access and malware/viruses.

Does an M&A Transaction Impact the Risk of a Data Breach?

With respect to cybersecurity, C-suite executives of small to mid-market companies, in particular, often believe their companies are too small to be on any cyber-criminal's radar. Or they presume their IT Guy "has that covered." They are also concerned about cost. Unfortunately, all too frequently for some businesses privacy and cybersecurity aren't an issue until they are an issue.

---

1 The Spirit SEC 8-K filing is available at http://d18rn0p25nwr6d.cloudfront.net/CIK-0001364885/558f886b-f1b0-4716-b1b6-c181c1efc981.pdf

2 2019 study sponsored by IBM. IBM provides a link to the study and a "Cost of a data breach calculator" at https://www.ibm.com/security/data-breach .

Assuming the cyber-criminals have not learned about the deal in advance, the time between the public announcement of the M&A transaction and the closing can increase the vulnerability of the seller or buyer to a cyber-attack. Consider the number of late-night e-mails between and among the parties, their counsel, and other players (e.g., the investment bankers, insurance brokers, banks, etc.) involved in the deal. This creates opportunity for the cyber-criminal to engage in "spear-phishing" (e-mails that look like they are from trusted senders but in fact are not, and are targeted at specific individuals or companies)[3] and other social engineering techniques. The cyber-criminal's goal is to trick you into providing the information they seek (e.g., access to your business's digital data, network infrastructure, financial account information, etc.).

Sellers and Buyers Beware

- Sellers:
  - Cyber-thieves (and the disgruntled employee) know that often small and mid-market companies do not put sufficient, or any, resources toward preventing data breaches. Some cybersecurity professionals refer to these companies as "the low hanging fruit" for cyber-criminals.
  - When did you and your business last take time to learn about privacy/cybersecurity issues (technology and legal) and how they impact your industry/profession and your business?
  - Was your business prepared for the "new" shelter in place and work at home paradigm thrust upon the global economy by the COVID-19 virus? "A growing number of cyber-criminals and other malicious groups online are exploiting the COVID-19 outbreak for their own personal gain, security officials in the UK and USA have revealed."[4]
    - What preventive cybersecurity steps did you take?
    - For instance, before the pandemic did you educate employees throughout the business about privacy and cybersecurity and their role in helping to protect the business from cyber-threats? How prepared was the business and its employees to pivot to working remotely? Preventive steps can go a long way in helping to minimize cybersecurity risks to the business.
    - Employees without proper training or mindfulness can create cyber-risks for themselves and the business. Such risks include:
      - An employee opening an e-mail attachment without an awareness that the attachment might contain malware (even if it looks like it came from the CEO of the company).
      - Clicking on a link in an e-mail that takes them to a website that installs malware on their computer and the company's network connected to their computer.
      - Working at home on an outdated unsecured modem/router (or a modem/router with improper security settings).
    - What proactive resources did the business provide to help make everyone in the company more cyber-threat aware?

---

3 "Phishing doesn't attack computers. It attacks the people using computers." Quinn Norton, Phishing Is the Internet's Most Successful Con," *Atlantic* (Sept. 12, 2018) https://www.theatlantic.com/technology/archive/2018/09/phishing-is-the-internets-most-successfu-lcon/569920.

4 "UK and US Security Agencies Issue COVID-19 Cyber Threat Update" Cybersecurity & Infrastructure Security Agency, 20200408 available at https://www.cisa.gov/news/2020/04/08/uk-and-us-security-agencies-issue-covid-19-cyber-threat-update (last visited 20200520).

  - When was the last time you examined/reviewed the types of personal identifying information ("PII") and other sensitive data your business collects, stores, and/or shares with third parties? This includes, without limitation, customer data, employee data, trade secrets.
  - When was the last time you reviewed your Written Information Security Plan ("WISP")? Does your business even have a WISP?[5]
  - When was the last time you reviewed and inventoried all of the business's contracts with third-parties related to sharing PII and/or other sensitive information? Do you monitor the third-parties' compliance with how the contract says they are to handle that information?
  - Caution: this willingness to learn about the legal and technology implications of privacy/cybersecurity requires leadership from the top in order to succeed.

- Buyers:
  - Do you include in your due diligence a thorough examination of the seller's legal health concerning privacy and cybersecurity issues? By way of example, do you examine the seller's existing privacy/cybersecurity policies, seller's compliance with those policies, seller's history of any cybersecurity incidents, seller's contracts with third parties concerning handling of PII and sensitive data, reports concerning seller's monitoring of compliance with the third party's obligations?
  - Do you engage privacy and cybersecurity technologists, and lawyers knowledgeable in technology, privacy and cybersecurity law, to assist in your due diligence?
  - Do you examine seller's preparedness for handling cybersecurity incidents? Does seller have a WISP and can they provide evidence of compliance?
  - Is seller in compliance with its own privacy policies?
  - How do the reps and warranties in the transaction documents address privacy and cybersecurity issues?

The above is not exhaustive of the issues confronting sellers and buyers considering an M&A transaction.

Does Your Due Diligence Properly Address Cybersecurity Risks?

Placing the abovementioned considerations in the context of an M&A transaction, what roles do privacy and cybersecurity issues play (or should play) in structuring the due diligence in these transactions? Have you even considered them as part of the due diligence process? Why should you?

"In the United States, recent cybersecurity-related intrusions have brought heightened attention and scrutiny to questions of risk oversight and effective risk mitigation practices."[6] If the M&A transaction's due diligence reflects inadequate (or no) attention to the privacy and cybersecurity issues, how

---

5 *See*, Boy Scouts of America motto "Be Prepared." Originally published by Robert Baden-Powell in Scouting for Boys" (1908).

6 Emmerich, Adam O. and Savitt, William and Niles, Sabastian V and Ongun, S. Iliana, *The Corporate Governance Review: United States* (April 1, 2019). Law Business Research, London, 9th ed. 2019; at page 413. Available at SSRN: https://ssrn.com/abstract=3399676.

will the business stakeholders and investors react if these issues arise shortly before or after the M&A transaction closes?

As demonstrated by the abovementioned Verizon, Marriott, and Spirit AeroSystems transactions, a cybersecurity incident can have repercussions on an M&A deal including a valuation reduction or the triggering of a Material Adverse Change ("MAC") provision.

- For a potential seller, the time to think about and plan for privacy and cybersecurity issues is before the business is put up for sale. Under the microscope of a thorough due diligence process, a number of things might be discovered that can impact the business's valuation. These include, without limitation,[7] weak or nonexistent attention to privacy/cybersecurity issues or a data breach, lack of proper agreements both internal and external that properly address privacy/cybersecurity issues, lack of proper technology controls and procedures to minimize or prevent unauthorized access, etc.
- A buyer considering the purchase of a business should address privacy and cybersecurity issues impacting the target acquisition no later than the beginning of the due diligence phase. Privacy/cybersecurity should be one of the foremost and thoroughly addressed issues as appropriate to the M&A transaction.

In a June 2019 study released by Forescout, the Executive Summary posits, "By 2022, Gartner reports that 60% of organizations engaging in M&A activity will consider cybersecurity posture as a critical factor in their due diligence process, up from less than 5% today. In our survey of 2,779 IT and business decision makers from around the globe, 73% of respondents agreed that technology acquisition is their top priority for their M&A strategy over the next 12 months—and, 62% agreed that not only does their company face significant cybersecurity risk by acquiring new companies, they also expressed that cyber risk is their biggest concern post-acquisition."[8]

Conclusion

Business sellers need to proactively plan their privacy/cybersecurity strategies and tactics to minimize or prevent unauthorized access (e.g., identify and address potential vulnerabilities that put them at risk for cyber-attacks), detect and control breaches in progress, and respond to breach incidents. Government regulations, legislation, and developing case law have elevated privacy/cybersecurity issues to become an additional responsibility of the business's Board of Directors. The Board should not be in the position of first addressing these issues when negotiating an agreement to sell the business or responding to a buyer's due diligence requests.

---

7 Dear reader: The focus of this article is on privacy/cybersecurity. There are other issues that can impact valuation including, without limitation, the business's technology licenses to use 3rd party software, IP rights/registrations, etc.

8 "The Role of Cybersecurity in Mergers and Acquisitions Diligence," Forescout Technologies, Inc., 2019; Executive Summary. The Forescout study is available at https://www.forescout.com/solutions/asset-management/merger-and-acquisition-cybersecurity-report/. The reference to the Gartner report is from "Cybersecurity is Critical to the M&A Due Diligence Process," Gartner (April 2018) https://www.gartner.com/en/documents/3873604 .

Waiting to address cybersecurity issues while in the midst of a transaction risks the valuation of the business or could trigger a MAC provision in the purchase agreement.

Business buyers need to proactively include privacy/cybersecurity (as well as other technology and intellectual property issues) as part of their due diligence investigation into target acquisitions. Failing to properly do so may result in buying a lawsuit in addition to, or instead of, buying a business.

While there are many legal, business, and technology issues in an M&A transaction, the bottom line for sellers and buyers in these transactions is the need to be aware of the impact that privacy/cybersecurity issues can have on the M&A transaction. While general corporate counsel may handle the general corporate due diligence, it is advisable to retain knowledgeable and experienced resources (e.g., technologists and attorneys familiar with privacy/cybersecurity) to address the due diligence for privacy/cybersecurity issues. As Benjamin Franklin is credited with saying, "An ounce of prevention is worth a pound of cure." And, when privacy/cybersecurity issues leap to the front burner, it should not be the first time you think about them.

If you have any questions about this article, please contact the author:

Alan S. Wernick, Esq.
T: 312.755.3172
E: AWernick@agdglaw.com
LinkedIn: www.linkedin.com/in/alanwernick