Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Tips For Managing Cybersecurity And Privacy Risks In M&A

By **David Kessler and Anna Rudawski** (April 22, 2021, 3:11 PM EDT)

David Kessler

When working on mergers and acquisitions, certain aspects of closing have become de rigueur — call tax, employment and intellectual property — but more recently, issues related to privacy and cybersecurity have come to the forefront.

Routinely, cybersecurity and privacy have been relegated to a few due diligence questions or clauses in a purchase and sale agreement.

They were, for lack of a better word, an afterthought. But cybersecurity and privacy issues are now being viewed as essential parts of a deal, even as potential deal breakers.

Anna Rudawski

Due diligence regarding cybersecurity and privacy risks require subject matter expertise related to breach, digital technology, regulatory enforcement, and quantifying the risk and value associated with data assets.

And the check-the-box attitude toward cybersecurity and privacy issues is quickly becoming a thing of the past. Below we cover key issues in these areas when contemplating pursuing and closing a deal.

Wanna Buy a Bridge?

A common theme in privacy and cybersecurity due diligence is figuring out whether data transferred in connection with the transaction is clean.

In other words, was the target's data collected in compliance with all laws?

Were required notices provided?

If consents were needed, were they collected?

If data was transferred out of the European Union, are the appropriate transfer mechanisms in place?

For an alarming number of companies, these questions were not asked until a deal was on the horizon, and the answer is often, not really.

In those cases, the target company may be selling data it does not have the right to sell or transfer.

For instance, where no notice was provided to individuals whose data was collected, or where the existing notice makes representations that are inaccurate — e.g., the classic: we will never share your data with another third party — the acquirer needs to figure out whether they can use the data in the first place.

Essentially, what rights travel with the data — can it be shared, transferred, or sold?

Also, did the data owner or controller guarantee certain rights with respect to the data? For example, were individuals told they can delete or view their data at any time?

Indeed, this is a guarantee many companies made without limitation following passage of the EU General Data Protection Regulation and the California Consumer Privacy Act.

When confronting these questions, companies need to ask if they can still use the data in a way that drives value for the deal.

If the data has been collected in a noncompliant manner, is there a way to correct any deficiencies and what does that entail?

In some cases, companies can cure the defect by providing a new notice, an opt-out, or an opt-in. But the approach depends on the nature of noncompliance and the sensitivity of the data.

In other words, transferring business contact information may be a low-risk proposition, even if the notice at the time of collection was imperfect. However, transferring sensitive health or genetic information, where a required consent was not provided, may entirely obviate any value to the data.

In the latter case, the acquiring party may be unable to use the data without running a significant risk for regulatory action or private causes of action.

In addition, noncompliance or use of data that was improperly collected or processed may result in regulatory fines. This includes substantial fines under the GDPR, Federal Trade Commission rules or the CCPA for misuse of personal information.

Peering Behind the Curtain

In a number of deals, parties are asking to exercise audit-like rights earlier in a deal. Companies can and should rely on subject matter experts to review the cybersecurity infrastructure of an acquired company. To accomplish this, companies have a few options when conducting cyber due diligence.

The first and most commonly used option is to ask if the company has conducted an independent assessment of its cybersecurity program.

Ideally, the assessment should be recent and conducted in accordance with an industry standard protocol, like the Framework for Improving Critical Infrastructure Cybersecurity from the U.S. Department of Commerce's National Institute of Standards and Technology, or ISO 27001 certification from the International Organization for Standardization.

Findings should be carefully reviewed, and any gaps should be remediated or in the process of being addressed. If the target has not completed a recent audit, consider asking that they complete one during due diligence.

Who pays for the audit can be worked out as part of any agreement. Indeed, parties can agree to factor it into the purchase price or any determinations regarding representation and warranty insurance with respect to cybersecurity.

Another option, albeit a less frequent one, is conducting a threat hunting exercise with an independent expert. Although this approach is less common, requests for this kind of access are on the rise, especially given the number of breaches discovered after a deal closes. In this arrangement, a third party will stress test the target's systems.

If a threat hunting exercise turns up few or no vulnerabilities, parties can move forward with confidence. However, there is a risk that a breach or serious cybersecurity shortcomings are discovered, and this may affect the overall value of the deal, or scuttle it entirely.

Yet the rise in undiscovered cyberattacks may make this practice more common moving forward.

Further, even if a target does not agree to this kind of testing, companies should consider a threat hunting exercise before combining technology assets or connecting with potentially outdated systems.

Numerous large — read: expensive — breaches were discovered or amplified when outdated or compromised systems connected to larger, secure or more sophisticated systems.

Many companies have unknowingly integrated backdoors, vulnerabilities or outdated date security tools into otherwise state-of-the-art systems.

Keep in mind, many breaches are discovered after closing, and more often than not, they are the financial responsibility of the acquirer. To reduce risk, consider keeping systems segmented until they are deemed secure. If systems are segmented, companies can at least limit the scope of any attack.

Protecting Yourself

Companies can also seek contractual protections or insurance for digital vulnerabilities.

First, specific data or digital representations and warranties insurance is increasingly common for deals that involve large amounts of information. However, it is important that the information and risk associated with data is captured by a subject matter expert.

Misrepresentations about the risk can reduce the availability of coverage should a problem arise.

In addition, the risk of the data should be described accurately. This risk cuts both ways. In some deals, the risk is understated, but in others the risk is unnecessarily amplified because the parties involved do not understand how international and cross-border privacy laws actually govern the data.

For example, many companies make representations about the GDPR or CCPA when neither law applies.

Second, special indemnities may be used to cover certain risks associated with the information. While these sorts of indemnities can be difficult to implement generally, specific indemnities tied to certain assets, vulnerabilities or known issues can be baked into the agreement.

For example, if there was an attempted ransomware attack on a target company, the acquirer can seek coverage for any follow-up attacks connected to the initial attack — e.g., if the attacker later exploits a backdoor placed during the initial attack.

Last, figure out what insurance both sides have and what it covers. This is a straightforward step that involves speaking with the insurance company and looking at the policies.

Despite being an easy step, many parties often skip it or neglect to buy cybersecurity insurance. But this information is easily available and there is no excuse for failing to figure out what each party's policy covers, and for how long.

Some questions you should ask are: What is covered by the policy? Does it cover regulatory fines? What about third-party claims? Can the policy extend beyond closing? If so, for how long? Answers to these questions can attenuate concerns about financial liability for a data breach.

Valuing Data in the Information Economy

Even with these risks, data is an increasingly valuable part of any deal, and, accordingly, a potentially costly liability.

And while data can break a deal, it can make one too. Data is an asset that should be fully appraised and vetted as part of any due diligence process.

Still, too many parties rely on outdated or limited due diligence questions when assessing data and cybersecurity risk. Parties need to start investing, and demanding, a more robust accounting of data risks.

This requires more questions, a tougher look at cybersecurity and privacy programs, and even the assistance of subject matter experts, including lawyers that specialize in the field and third-party technologists.

At the end of the day, cybersecurity and privacy should now be treated on equal footing as other parts of the due diligence process, like tax, real estate and intellectual property. Otherwise, buyer beware.

David Kessler is head of data and information risk and Anna Rudawski is a senior associate at Norton Rose Fulbright.