THE
NATIONAL LAW REVIEW

The GDPR and Mergers and Acquisitions: What Corporate Buyers and Sellers Need to Know

Friday, April 6, 2018

As cybersecurity incidents affecting Target, Home Depot, Anthem, Sony, Ashley Madison, and many other companies have demonstrated, cybersecurity poses a significant legal risk to companies. Not to mention it makes their electronically-stored corporate assets a virtual sitting duck at the mercy of the company's IT infrastructure. While companies continue to grapple with regulatory, legal, and technological obligations, one area that has received less attention is the area of corporate mergers and acquisitions. This, however, is not an area that should be ignored, especially when so many mergers and acquisitions concern multi-national companies, companies operating in the EU, and/or companies with employees or customers in the European Union (EU), all of which will be responsible for complying with the EU's General Data Protection Act (GDPR) come May 25, 2018.

One primary issue is when companies go through the acquisition process, not only can vulnerabilities in the security network be transferred to the acquiring company but so are regulatory and other non-compliance issues. For example, the Federal Trade Commission (FTC) and other regulators, including the EU Data Protection Authorities, who will enforce the GDPR, can hold an acquiring company responsible for the faulty, false or lax security practices of the company it acquires.

Article By Dickinson Wright PLLC
Sara H. Jodka

Global
Mergers & Acquisitions
Communications, Media & Internet
All Federal
European Union
United Kingdom

Take, for example, a company acquires a company in late 2017 only to discover that the company is covered under the GDPR based on the type of information it collects on customers but did not take any steps pre-acquisition to do so. Now, the acquiring company has limited time to review the acquired company's data and security infrastructure and make the necessary compliance changes in a very short period of time. That key piece of information will significantly increase the financial regulatory burden on the acquiring company, but because the issue was not disclosed pre-acquisition, that financial burden was not negotiated as part of the purchase price.

Typically, there are three avenues for a corporate merger and acquisition: (1) asset sale – where an entity purchases the assets of another; (2) stock sale – where an entity purchases a majority stake in the equity of another entity; and (3) hostile takeover – where an entity takes a majority stake in the equity of a target entity that had no desire to lose its majority stake.

In all of these transactions, cybersecurity is a risk for all parties including their C-suite, board members, underwriters, and legal counsel. This is because, in the typical setting, the target company has intangible assets of significant value. As we have learned from some of the more publicized breaches, such intangible assets including, trade secrets (the company's secret sauce); customer lists; personal identifying information; intellectual property/work product (as demonstrated by the Sony breach with the release of several films including The Interview featuring Seth Rogen and James Franco); high-level executive conversations detailing corporate strategies, financial issues, client confidences, etc. (as also demonstrated by the Sony breach); private health information of clients and employees (as demonstrated by the Anthem breach); and private sexual preferences and other personal information of clients/website users who import information (as demonstrated by the Ashley Madison breach).

Other company assets can also lose significant value in the event of a breach including customer goodwill and brand reputation. This was demonstrated quite prominently in the Anthem, Home Depot, and Target breaches. For example, on the heels of its 2012 breach, Target's brand reputation and customer goodwill took a significant hit – not to mention its stock prices and the jobs of some of its higher-level executives. Although Target came back to pre-breach stock price levels, it stands as a good reminder of what is at stake.

As such, governance, risk, and regulatory and other compliance issues should be a part of the due diligence process, when closing the deal, and when finally integrating the companies.

Due Diligence -

From the due diligence standpoint, there are many potential issues. First, many companies rely so much on cloud and digital storage and do not fully understand how that information is shared or who has access to it. Second, many companies have no idea what information has been transferred to personal or company-owned devices, thumb drives, or other places that also places it at issue. Third, while a large global company will likely have well-established policies and procedures regarding and concerning cybersecurity defenses, cybersecurity may not be as robust and vulnerability-deterrent as some of its smaller, acquired, or geographically-extended divisions or departments.

These factors play well for attackers who look for acquisitions, subsidiaries, and vendors (e.g., access in the 2013 Target breach was accessed through a Target vendor) to find a security vulnerability that does not adequately restrict access. Once the attacker is inside the less secure network, it looks for connectors into the larger corporation. If the attacker finds a connection, the attacker can use that opening to gain a traction foothold in the larger corporation's secure network.

In the merger and acquisition context especially, it is not difficult for attackers to identify the weak links. Many mergers/acquisitions are publicly announced through press releases, industry pieces, etc. For public companies, they are required to list their subsidiaries in their filings with the Securities and Exchange Commission (SEC).

In addition to outside threats, companies should also protect against employees and former employees stealing company information via external transfers, downloading to mobile devices, etc. Companies on both sides of the transaction must pay attention to insider threats and cybersecurity risks involved in the due diligence process.

To demonstrate just how important cybersecurity is in the due diligence process, in 2014, TripAdvisor acquired Viator, a tour booking company, for $200 million. The deal closed and about two weeks later, Viator announced it was the victim of a data breach that compromised the personal details and credit card information of approximately 1.4 million of its customers. TripAdvisor's stock fell five percent immediately on the news.

Thus, the risk of not performing cybersecurity due diligence is largely two-fold: First, the acquired company could have a bomb sitting in its network that has infiltrated its infrastructure waiting to explode (maybe even years later as in the case of the Yahoo! Breach), including after the deal has closed, leaving the acquiring company holding the bag. Second, the acquired company could have legal compliance obligations that are difficult to understand, time consuming and costly, e.g., GDPR that the acquired company wants to avoid or did not know they were subject to follow. If proper cybersecurity due diligence is not conducted, the acquiring company could get stuck with significant compliance costs and obligations that it was not expecting and that went unaccounted for in the original purchase price.

Just some of the GDPR issues that an acquiring company could face include:

- Losing a significant amount of customer marketing and other data due to not being properly obtained via the GDPR's consent requirements;
- Having to identify relevant protected information to properly protect it;
- Having to revise internal and external-facing customer and employee policies to include GDPR requirements;
- Having to appoint a Data Protection Officer;
- Having to conduct a Data Protection Impact Assessment;
- Having to monitor and track all data subject requests to enforce their rights under the GDPR, including the right to be forgotten, portability of information, etc.;
- Reviewing vendor/Subprocessor agreements to ensure they conform to the controller/processor requirements; and
- Entering into model clauses or getting certified under the Privacy Shield in order to transfer customer and/or employee data from the EU to the United States or elsewhere.

There are four steps companies in a transaction should undergo at the due diligence stage to minimize cybersecurity risks:

1. Develop an M&A Strategy: This is accomplished by first realizing that cybersecurity is not an IT issue; it is a governance and risk issue as well. That means a comprehensive cybersecurity review is necessary at the board level prior to engaging in any acquisition discussions. When reviewing privacy and security issues at this stage, the following should be taken into account:
    1. Scope of expansion and whether that includes expanding into new industries and/or new geographic regions with new/differing laws, i.e., require compliance with GDPR, HIPAA/HITECH, COPPA, GLBA, etc.;
    2. Whether any new products or technologies are part of the business goals;
    3. Whether the company is going to change how it uses certain categories of information; and
    4. How the risk profile of both companies may change.
2. Evaluate and Engage: Both parties should gain a comprehensive understanding of the data privacy and security profiles of each other. This is because a breach on either side of the transaction can kill a deal.

When specifically reviewing the target company, the acquiring entity should review the following key pieces of information, which is typically done via a secure online data room that is used to store relevant data during the due diligence phase:

- A “data map” outlining where and how the target companies stores data and related security controls and protocols.
- Privacy policies, procedures, and notices, including website terms and conditions and external-facing privacy policies.
- Policies regarding how the target company collects, uses, discloses, transmits, stores, shares, retains, secures (encrypts/password protect) and destroys personal information and other protected categories of information. Of note, the Federal Trade Commission (FTC) views statements made by companies in their privacy policies as promises that must be kept even when the company that made them is acquired by another.
- Identify the international scope of data and data transfers to review compliance requirements, including if the acquiring company has proper protections in place, i.e., GDPR compliant and certified under the Privacy Shield to transfer personal data out of the EU to the United States.
- Determine the scope of scrutiny controls, e.g., administrative safety controls and programs, security audits, data/electronic risk assessments, comprehensive information security program, disaster recovery and business continuity plan, management of internal and external vendors including cloud service providers and data processors, compliant with industry standards, remediation effort protocol, and incident response plan.
- Create a risk profile that should include information about any prior breaches, security incidents, or attempted breaches or security incidents. This also includes identifying past or present litigation, complaints, administrative investigations/fines/penalties relating to security issues.

Third party experts can also be brought in to conduct a cyber audit to ensure the deal is viable and that the risks are properly addressed and/or priced. This includes repeated penetration testing the target’s networks and systems.

3. Insurance. The parties should consider purchasing cybersecurity insurance to protect against any unforeseen events that occur during and/or in the immediate aftermath of the deal.

4. C-Suite Involvement. Boards on both sides of the transaction should focus their cybersecurity cultures to determine whether their views on cybersecurity match. For example, a company with well-established policies may face a lot of push back if the target company is more relaxed. This is especially true when it comes to requiring employees to set certain passwords; use certain security protocols with respect to Smart devices; refrain from accessing company information via unsecured Wi-Fi networks; continued compliance including the monitoring and tracking requirements under the GDPR; etc.

After the deal Closes -

Whether due diligence was properly done is usually readily apparent once the acquiring company takes over operational control of the target company. There are two fronts the acquiring company must deal. The first is operational as the acquiring company must ensure the initial connectivity between the companies. This is largely an IT function, but will also concern other functions, including HR, as employees’ computers and devices are reconfigured for on-site and remote work. The second is interpersonal as human resources and other teams will

have to prepare, organize, and train employees, including onboarding new employees, with the new, integrated systems.

Documentation and Continued Compliance and Monitoring -

Once the acquisition is complete, the work is not finished. The acquiring company must continue to improve its security, monitor and be mindful of internal and external threats vectors, continue to update security procedures and protocols, and delineate a clear line of information security responsibilities, reporting, costs, and shared responsibilities between the applicable departments, such as, IT, legal, HR, compliance and governance, etc.

Source URL: https://www.natlawreview.com/article/gdpr-and-mergers-and-acquisitions-what-corporate-buyers-and-sellers-need-to-know