Harvard Journal of Law & Technology Digest
Online-only publication

CYBERSECURITY IN M&A TRANSACTIONS: WHAT THE UNITED STATES AND SOUTH KOREA JURISPRUDENCE CAN LEARN FROM EACH OTHER

Yong Bum Lee[*]

Published May 23, 2018
Original link: http://jolt.law.harvard.edu/digest/cybersecurity-in-m-a-transactions-what-the-united-states-and-south-korea-jurisprudence-can-learn-from-each-other

Recommended Citation

Yong Bum Lee, *Cybersecurity in M&A Transactions: What the United States and South Korea Jurisprudence Can Learn From Each Other*, HARV. J.L. & TECH. DIG. (May 23, 2018), http://jolt.law.harvard.edu/digest/cybersecurity-in-m-a-transactions-what-the-united-states-and-south-korea-jurisprudence-can-learn-from-each-other.

[*]J.D., Harvard Law School (expected 2019), B.A., Business Administration, Yonsei University (2016).

TABLE OF CONTENTS

INTRODUCTION

Data is one of the most valuable assets in today's business world. Many companies are collecting an increasing amount of data related to customers, competitors or suppliers to improve their own performance; at the same time, these companies risk cybersecurity breaches by third parties who also hope to monetize this valuable data.[1] Victims often have no recourse because it is almost impossible to identify the breaching party, regardless of the legality of their actions.

In response, cybersecurity has gained increased importance to businesses. This applies to company operations generally, but much attention has been devoted to cybersecurity concerns specifically in M&A transactions as well. This paper aims to identify how various influences have shaped the way cybersecurity considerations in M&A transactions developed, with a comparative focus on the United States and South Korea. Within the M&A context, this paper will place emphasis on the role of cybersecurity in due diligence, which refers to an acquirer's investigation of a target company to identify risks and make an informed decision.

Part I of this paper studies legal obligations related to cybersecurity that exist in the United States and South Korea, and how such obligations may have affected

[1] Companies monetize data assets in different ways. Most traditionally, companies collect data on customers and use this data for targeted marketing or improving their product or service. Other companies build their businesses on collecting, processing, and directly selling customer data to generate revenue. Recently, some companies use customer data to regularly improve their product or service by building in data collection and utilization into their platform. One example of such a company is Uber, which uses customer location as well as evaluation information to continuously alter its service offering. Cybersecurity breaches can occur for a variety of reasons, but often the perpetrators are motivated to sell valuable data assets in the black market.

cybersecurity considerations in M&A transactions. Cybersecurity laws and regulations in the United States tend to be industry-specific, while the South Korean counterparts focus on the type of data. However, both countries currently lack laws and regulations that specifically address cybersecurity in the M&A transactions context.

Part II analyzes how cybersecurity has developed as a standalone consideration in M&A due diligence, in the absence of substantial legal obligations. This part provides an overview of what cybersecurity due diligence looks like as well as the substantive grounds commonly covered by acquirers and advising law firms. Most of the literature so far addressing cybersecurity concerns in M&A transactions have been generated in the United States. This may be due to the greater abundance of attractive cybersecurity targets in the United States, the internalization of cybersecurity functions by South Korean companies, or both.

Part III closely examines Verizon's acquisition of Yahoo in 2017, which was discounted from $4.83 billion to $4.48 billion due to two cybersecurity incidents that occurred in 2014. This part explores which substantive cybersecurity due diligence areas discussed in Part II are applicable to the Verizon-Yahoo deal as well as how a thorough diligence process may have helped Verizon carry out the deal in a smoother manner.

Part IV discusses the takeaways of this paper. Without substantial legal obligations, understanding of what is appropriate cybersecurity due diligence in M&A transactions will rely primarily on trial and error. In this context, United States companies can learn from the internalized cybersecurity functions of South Korean companies, and South Korean law firms can learn from the M&A-related cybersecurity expertise of United States law firms. Parties to M&A transactions should remember that cybersecurity due diligence is necessarily individualized and contextual.

I. CYBERSECURITY OBLIGATIONS IMPOSED BY LAW IN THE UNITED STATES AND SOUTH KOREA

In the United States, there have been sporadic efforts by various bodies of the federal and state governments to promote cybersecurity in the public and private contexts. These efforts attempted to address the growing relevance of cybersecurity in specific industries, such as those that are traditionally data-driven, but did not reach so far as to mandate cybersecurity-related considerations and processes in the context of corporate transactions.

Financial and healthcare institutions have been primary targets of Congress as they handle large amounts of sensitive customer information for daily opera-

tions.[2] For example, the Financial Services Modernization Act of 1999 (FSMA)[3] and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) generally require regulated parties to put in place protective systems for information integrity.[4] While both statutes contain more details regarding what data must be protected, the statutes as well as regulations pursuant to those statutes are vague as to what manner or level of security is required of the regulated parties.[5] Furthermore, acts of Congress have failed to address other industries that are equally, or arguably even more, data intensive, such as internet service providers and software companies.

The most notable cybersecurity efforts that have implications on M&A transactions are those by the Securities Exchange Commission (SEC).[6] To be sure, the SEC has not imposed any general protective requirements on due diligence for M&A transactions. However, it is conceivable that the SEC's efforts to increase cybersecurity awareness and preparedness in the financial services sector has had some impact in the realm of corporate transactions as well. In 2015, following an examination of more than 50 registered broker-dealers and investment advisors, the SEC issued guidelines on how it will conduct cybersecurity examinations in the future.[7] These guidelines highlight five areas as the focus of future examina-

[2] The Federal Information Security Management Act (Title III of the Confidential Information and Statistical Efficiency Act of 2002) includes cybersecurity mandates for federal agencies. While this act is not industry specific *per se*, like the Financial Services Modernization Act and Health Insurance Portability and Accountability Act, it shares the shortcoming that the requirement to protect sensitive information is vague and non-substantive. Confidential Information Protection and Statistical Efficiency Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (2002).

[3] This act is also known as the Gramm-Leach-Bliley Act.

[4] Gramm-Leach-Biley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999); Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936.

[5] For example, regulations promulgated pursuant to HIPAA contain the "Privacy Rule," which details data privacy requirements with regard to personal health information. In part, the regulations provide that "appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement." 45 C.F.R. §164.514 (2013). Under the FSMA, financial institutions must follow "appropriate standards . . . relating to administrative, technical, and physical safeguards" for protection of nonpublic personal information. 15 U.S.C. § 6801 (2010).

[6] The SEC website states that "[t]he mission of the SEC is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation." *About the SEC*, SEC. EXCH. COMM'N, https://www.sec.gov/about.shtml (last visited Sept. 13, 2017). To this end, the SEC has regulatory oversight of the exchange of securities, including exchanges by managers of private funds.

[7] SEC. EXCH. COMM'N OFF. OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, OCIE'S 2015 CYBERSECURITY EXAMINATION INITIATIVE (2015). This initiative was led by the SEC's Office of Compliance Inspections and Examinations (OCIE). The OCIE conducted its first round of examinations of more than 50 broker-dealers and investment advisors in 2014 and 2015. The OCIE has announced that there will be at least one more examination soon to follow.

tions: cybersecurity governance and risk assessment, access rights and controls, data loss prevention, vendor management, and training and incident response.[8]

Again, the SEC's efforts are not directly relevant to M&A or other corporate transactions.[9] However, the 2015 guidelines pertain to investment advisors, including private equity firms, which are often parties to an M&A transaction. Therefore, the SEC's guidelines are very likely to have some substantial impact on how data and cybersecurity is handled in M&A transactions as well.[10] The SEC's further clarification regarding its five cybersecurity focal points will provide guidance as to what constitutes regulatory compliance.

South Korea takes a different, more generalist approach to imposing cybersecurity obligations by law. The Personal Information Protection Act ("PIPA") lays out general privacy and data protection requirements related to collecting and processing sensitive information.[11] Other laws work together with PIPA to impose more specific obligations; rather than focusing on the different industries that handle sensitive information like in the United States, South Korean laws focus on the type of information to be protected. For example, the Use and Protection of Credit

[8] In assessing governance and risk assessment, the SEC will look for periodic evaluation of cybersecurity risks and tailored controls and processes. For access rights and controls, the SEC will look for controls to prevent unauthorized access to systems or information, such as network segmentation and tiered access. For data loss prevention, the SEC will look at how companies monitor data transfers into and out of themselves. For vendor management, the SEC will look for appropriate due diligence of, oversight of, and contract terms with third party vendor platforms. For training, the SEC will look for proper employee and vendor training to protect data. Finally, for incident response the SEC will for established policies, plans, and roles for responding to breaches. *Id.*

[9] Another notable regulatory movement that is industry-specific is the proposed cybersecurity regulation for large financial institutions (financial institutions with consolidated assets of $50 billion), by the Federal Reserve Bank, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation. This new proposed framework would regulate cybersecurity in five categories: (1) Cyber risk governance, (2) Cyber risk management, (3) Internal dependency management, (4) External dependency management, and (5) Incident response, cyber resilience, and situational awareness. While this proposed regulation was expected to be significantly more stringent than existing ones, industry opposition and lack of support from the Trump administration have raised significant barriers so far. Cadwalader, Wickersham & Taft LLP, *Proposed Federal Cybersecurity Regulation for Financial Institutions Face Uncertain Future* (Mar. 13, 2017), https://www.natlawreview.com/article/proposed-federal-cybersecurity-regulations-financial-institutions-face-uncertain.

[10] Indeed, many law firms that advise on corporate transactions have elaborated on how cybersecurity should be incorporated into M&A due diligence to satisfy the SEC's guidelines. Such law firms include Skadden, Arps, Slate, Meagher & Flom LLP, Sullivan & Cromwell LLP, and Cleary, Gottlieb, Steen & Hamilton LLP. The substance of these guidelines is discussed in detail in Part II of this paper.

[11] PIPA also establishes the Personal Information Protection Commission to "deliberate and resolve the matters regarding data protection." Personal Information Protection Act, Act. No. 14839, Sept. 30, 2011 (S. Kor.).

Information Act pertains to personal credit information and the Communications Secrecy Act pertains to privacy of telecommunications.[12] While this focus on types of information rather than specific industries means South Korean cybersecurity laws have greater reach and less ambiguity than their United States federal law counterparts, like the United States, South Korea continues to lack laws imposing legal cybersecurity obligations in the context of corporate transactions.

II. CYBERSECURITY AS A STANDALONE CONSIDERATION IN M&A DUE DILIGENCE

Cybersecurity due diligence by the acquirer in an M&A transaction seeks assurance that the target company has taken appropriate measures to protect its data and electronic assets.[13] At a substantive level, cybersecurity due diligence has developed to address at least five main concerns: data management risk, technical risk, corporate risk, employee risk and track record.[14] The target company's history of cybersecurity-related compliance also sheds light on its cybermaturity.[15] This due diligence is most often conducted by a questionnaire prepared by the ac-

[12] Some more examples are the Use and Protection of Location Information Act (location-based information relating to living individual or moveable objects) and the Act on the Promotion of Information Technology Network Use and Information Protection (sensitive information in electronic form or online). Use and Protection of Location Information Act, Act. No. 14840, July 26, 2017 (S. Kor.); Act on the Promotion of Information Technology Network Use and Information Protection, Act. No. 10560, Apr. 5, 2011 (S. Kor.).

[13] A general assessment of the target company's cybersecurity policies and systems is often referred to as a measurement of the company's "cybermaturity." At a basic level, this measurement analyzes the adequacy of the target company's security policy, incident response policy, data access control policy and other relevant cybersecurity policies.

[14] FRESHFIELDS BRUCKHAUS DERINGER LLP, CYBER SECURITY IN M&A (2014). Data management risk refers to any threats to valuable data as a target company acquires, protects, and capitalizes on that data. Relatedly, technical risk refers to any shortcomings of systems in place to protect data such as encryption and firewalls. Corporate risk refers to inbound and outbound contracts that touch on the sharing and protection of valuable data that the target company relies on for its operations. Employee risk refers to potential security breaches related to employee behavior; the target company may guard against employee risk using internal processes for handling of valuable data, protective clauses in employment contracts, or both. Finally, track record refers to past cybersecurity breaches, what factors caused the breaches and what protective measures the target company took afterwards.

[15] The laws and regulations relevant to compliance would be the industry-specific ones discussed in Part I of this paper. Again, industries often have cybersecurity-related laws, regulations, and audits that can be used to demonstrate a target company's adequacy or inadequacy of cybermaturity compared to market standards. Of course, it should be noted that compliance (and relatedly market competitiveness of cybermaturity) is not a direct measurement of adequacy in an absolute sense.

quirer's legal team and advisors.[16] Depending on the sophistication of the acquirer and the relevance of cybersecurity risks to the target company, a more thorough testing of the target company's cybermaturity can be conducted with the help of third parties. For example, some acquirers hire "white hat hackers" to attempt to breach, and thereby assess, the target company's cybersecurity system.[17]

In the United States and South Korea, cybersecurity has not always been a standalone consideration in due diligence. In both countries, relevant cybersecurity concerns were often addressed in conjunction with other risk areas.[18] For example, software escrow arrangements[19] and open source software[20] have historically led parties in M&A transactions to protect assets through representations and warranties related to intellectual property as well as inbound and outbound contracts.[21] However, as data, software, and other electronic assets become more crucial, it is increasingly common for cybersecurity concerns to "make or break" a deal. For example, in the United States, 22% of surveyed public company directors and officers refused to acquire a company affected by a high-profile data

[16] While due diligence questionnaires are almost always tailored to the client and the situation, many legal advisors have now developed or are developing a set of fundamental questions related to cybersecurity. According to a report by Latham & Watkins LLP partner Jennifer Archie, the following questions should be included:

- What types of information or computer systems and operations are most important to your business? What sensitive data do you handle or hold relating to natural persons (which data elements in particular?)
- Where is sensitive information stored?
- How is it protected in transit, at rest, and in motion?
- What are the most concerning threats to information, networks, or systems?
- Have there been prior incidents?
- What is the cybersecurity budget?
- What are your recovery plans if critical information or systems become unavailable?

Jennifer Archie, *Cybersecurity Due Diligence in M&A Transactions: Tips for Conducting a Robust and Meaningful Process*, *in* NAVIGATING THE DIGITAL AGE: THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS 143, 143–44 (Matt Rosenquist ed., 2015).

[17] *Cybersecurity Diligence in M&A Transactions*, COOLEY LLP (Oct. 26, 2016), https://cooleyma.com/2016/10/26/cybersecurity-diligence-in-ma-transactions-lessons-from-verizonyahoo/. Some other acquirers choose to employ cybersecurity assessment tools or to perform an audit for software securities or coding structures with the help of third parties.

[18] *Id.*

[19] A software escrow arrangement refers to when the licensee of a software requests that the software source code be deposited with a third-party escrow agent, to prevent abandonment by the licensor.

[20] An open source software is publicly accessible, and therefore a company's control and ownership of the software may be challenged by the open source community.

[21] *Supra* note 17

breach, while 52% responded that they would acquire the company at a significantly reduced value.[22] In this context, cybersecurity is increasingly shifting from being a secondary consideration related to particular assets, such as intellectual property, to a standalone and integral part of M&A due diligence.[23].

The above analysis is mainly derived from the literature of law firms that operate primarily in the United States, not South Korea.[24] A quick study of the cybersecurity landscape in the South Korean M&A market reveals some unique characteristics: first, there is significantly less literature produced by law firms related to cybersecurity in the corporate transactions context, and second, this expertise is instead provided by third parties that specialize in tailored cybersecurity assessment services for M&A participants.[25] The same service providers are often also able to provide longer term cybersecurity support, including post-M&A integration.[26]

One possible explanation for this difference between the United States and South Korea is that cybersecurity is still a relatively niche demand in the latter market for M&A purposes. In other words, both the level and need for corporate cybermaturity may generally be lower in South Korea. This is consistent with relatively less M&A activity and lower incidence of cybersecurity breaches (and corresponding less attractive breach targets). Annual M&A deal value consistently exceeds $1 trillion in the United States, reaching $2.1 trillion in 2015 and $1.7 trillion in 2016.[27] The South Korean counterparts to these figures were only $84.9 billion in 2015 and $46.8 billion in 2016.[28] Similarly, an overwhelming

---

[22] NEW YORK STOCK EXCHANGE, CYBERSECURITY AND THE M&A DUE DILIGENCE PROCESS: A 2016 NYSE GOVERNANCE SERVICES/VERACODE SURVEY REPORT (2016).

[23] *See supra* note 17

[24] Examples of law firms that produced literature that this paper relies on are Latham & Watkins LLP, Freshfields Bruckhaus Deringer LLP, and Cooley LLP. It should be noted that Latham & Watkins LLP does not consider any one of its office to be its headquarters (and has offices in both the United States and South Korea), while Freshfields Bruckhaus Deringer LLP is a British law firm. Nonetheless, it remains true that all of these law firms maintain a disproportionate amount of business in the United States as compared to South Korea.

[25] One example of such a service provider is FireEye. Generally, FireEye's services can be summarized as providing cybersecurity risk assessment specifically for M&A participants, with a focus on data policies, security systems, breach response framework and overall data infrastructure. FireEye also provides cybersecurity integration services following execution of the M&A deal. *Why FireEye?*, FIREEYE, https://www.fireeye.com/company/why-fireeye.html (last visited Sept. 30, 2017).

[26] *Id.*

[27] Richard Peterson, *2016 Announced U.S. M&A Summary*, S&P GLOB. MKT. INTELLIGENCE (Jan. 5, 2017), https://marketintelligence.spglobal.com/blog/2016-announced-u-s-m-a-summary.

[28] Park Ga-young, *M&A Deals in 2016 Halves in Value Due to Political Scandal: Report*, KOR. HERALD (Jan. 23, 2017),

proportion of the most notable past cybersecurity breaches targeted companies whose headquarters, main operations or executive personnel are in the United States, such as JPMorgan and Home Depot in 2014, Hilton Hotels in 2015 and Chipotle in 2017.[29] Because such breaches often target customer credit card information, the United States, with its larger population and traffic, is naturally a prime target. In South Korea, only M&A deals that involve parties that have or process particularly valuable data may require special attention to cybersecurity. Specialized third parties, rather than general-service law firms that counsel on a wide array of corporate transactions, may be better positioned to provide advice in such niche situations.

An alternative explanation to South Korea's unique approach to cybersecurity concerns in the M&A context may be that South Korean conglomerates are choosing to take on these concerns themselves rather than rely on legal advisors. Multi-industry, family controlled conglomerates like the Samsung Group and Hyundai Motor Group are one of the most unique features of the Korean economy.[30] Ten of these conglomerates accounted for 76.5% of South Korea's total Gross Domestic Product in 2011.[31] Assuming that there are no regulatory issues, it is sensible and scalable for such "groups" to internalize almost any function.

---

http://khnews.kheraldm.com/view.php?ud=20170123000977. The sudden decline from 2015 to 2016 can be attributed in large part to a political scandal that eventually led to the impeachment of President Park, which significantly slowed corporate activity.

[29] In 2014, a cybersecurity breach of JP Morgan led to the exposure of millions of bank accounts later used for fraud schemes amounting to approximately $100 million, while a breach of Home Depot led to the exposure of personal and financial information of more than 50 million customers. In 2015, a breach of Hilton Hotels led to the exposure of credit card information of customers from dozens of hotel locations across the United States. In 2017, a breach of Chipotle led to the exposure of credit card information of millions of customers. Other notable cybersecurity breaches in the United States targeted Target in 2013 (led to the exposure of 110 million customers' personal and financial information), and Cravath, Swaine & Moore and Weil, Gotshal & Manges in 2015 (led to insider trading amounting to approximately $4 million). Jeff Roberts, *Here are 10 of the Biggest Corporate Hacks in History*, FORTUNE (June 22, 2017), http://fortune.com/2017/06/22/cybersecurity-hacks-history/.

[30] The term "group," both in South Korean literature and in this paper, is used flexibly to refer to a large number of corporate entities that are not necessarily legally interconnected but are effectively controlled by a small number of individuals (of the founding family) through familial, political, and economic ties. The terms "chaebol," "founding family," "group" and "group family" are often used interchangeably.

[31] While this is not the topic of this paper, conglomerates are intimately connected with the problem of wealth polarization in South Korea. The ten largest conglomerates not only account for over 76% of South Korea's Gross Domestic Product but also consistently outpace the Korean economy by various measures including growth in sales and assets. By way of example, South Korea's Gross Domestic Product grew by a factor of 1.8 from 2002 to 2011, while sales and assets of the ten largest conglomerates grew by factors of 2.6 and 3.3 during the same period. Eun-Jung Kwon, *Top Ten Chaebol Now Almost 80% of Korean Economy*, HANKYOREH (Aug. 28, 2012), http://www.hani.co.kr/arti/english_edition/e_business/549028.html.

With its growing relevance, cybersecurity would be no exception.[32] With the help of third parties dedicated to providing cybersecurity-related services, these Conglomerates would be able to receive counsel at the operational level (as opposed to event-driven cybersecurity advice focused on a particular M&A transaction) as well as tailor this expertise to suit their business needs.

It is likely that both reasons partially contribute to the different approaches to cybersecurity in the United States and South Korea. Indeed, the two explanations are not mutually exclusive. Given the relatively smaller size of the South Korean economy in the aggregate, less cybersecurity threats are directed at South Korean companies and a lower level of cybermaturity is required; at the same time, the concentration of economic activity and resources in South Korea allow conglomerates to command a position where they can afford to customize or internalize cybersecurity concerns. While companies in the United States and South Korea may conduct cybersecurity due diligence in different ways, it is worth noting that the underlying substantive concerns are similar because they are driven by broad business risks associated with cybersecurity.

III. YAHOO-VERIZON CASE STUDY

In September and December 2016, Yahoo announced that the company suffered two cybersecurity breaches in 2014 that led to the exposure of at least 1 billion customers' confidential information, including their names, email addresses, phone numbers, birthdays, passwords, and security questions.[33] Yahoo was two months into discussing its acquisition by Verizon for $4.83 billion.[34] While Verizon presumably had started due diligence, it expressed much surprise at this announcement.[35] After weeks of speculation regarding the survival of the deal, in February 2017 Verizon took the position that it would move forward with the deal,

[32] Consistent with this analysis, South Korea saw abnormally large amounts of M&A and other business activity involving cybersecurity companies in the latter half of 2016. Many of these activities involved enhancement of security in cloud computing and portfolio diversification. For example, KT (South Korean conglomerate with an emphasis on telecommunications) partnered with Vectra Networks (United States company that provides cybersecurity solutions) to develop a solution to detect and prevent cybersecurity breaches. Byungcheol Won, *Cybersecurity Related M&As and MOUs in Second Half of 2016 Provide Hints of Future Trends*, BOAN NEWS (Dec. 27, 2016), http://www.boannews.com/media/view.asp?idx=52779.

[33] Jill Abitbol, *Essential Cyber Due Diligence Considerations in M&A Deals raised by Yahoo Breach*, *in* 2 THE CYBERSECURITY LAW REPORT (Oct. 5, 2016).

[34] *Id.*

[35] Ethan Baron, *Yahoo-Verizon Deal Closes. It's the Fall of a Giant, End of an Era*, L.A. TIMES (June 13, 2017), http://www.latimes.com/business/technology/la-fi-tn-yahoo-verizon-20170613-story.html/.

but at a discount up to $925 million.[36] In the same month, Verizon announced that it agreed to acquire Yahoo at $4.48 billion, with a $350 million discount from the original offer.[37] The deal was closed in September 2017.[38]

Yahoo either did or did not know of the 2014 breaches during the two months in which it was involved in negotiations with Verizon but had not yet announced them. If Yahoo knew but did not disclose, this is probably simply an intentional wrongdoing which would have subjected Yahoo to indemnification, re-negotiation of valuation, or termination fees, depending on what stage the deal was in and what steps Verizon wanted to take.[39] While Verizon may have nonetheless discovered the 2014 breaches with thorough cybersecurity due diligence, this would probably have been difficult if Yahoo intentionally attempted to hide the relevant information, and may explain Verizon's initial surprise at the exposure of the breaches.

On the other hand, it is also possible that Yahoo simply did not know about the breaches (or how serious and widespread the breaches were) until they were forced to learn about them, in the process of answering Verizon's due diligence questions. While this second scenario does not implicate intentional non-disclosure by Yahoo, it does not indicate good news in relation to cybersecurity due diligence. As mentioned in Part II of this paper, at a substantive level, cybermaturity encompasses not just preventative measures but also identification and remedial measures that a target company took following past cybersecurity breaches.[40] The absence of such efforts (which, if present, would have notified Yahoo of the seriousness of the 2014 breaches) not only highlights the questionability of the original valuation of Yahoo's data assets, but also indicates that the acquisition of Yahoo will come with many additional costs.[41] On one level, the absence of effec-

[36] Reuters, *Verizon Tried to Cut the Price it's Buying Yahoo for by $925 Million But Got Rebuffed*, BUS. INSIDER (Mar. 13, 2017), http://www.businessinsider.com/r-verizon-sought-925-million-discount-for-yahoo-merger-got-350-million-2017-3.

[37] *Id.*

[38] Baron, *supra* note 35.

[39] Of course, now that Verizon has re-negotiated and closed at a different valuation after receiving the relevant information, termination or indemnification on the basis of the 2014 cybersecurity breaches are no longer a viable option for Verizon. However, it is not hard to imagine an acquirer demanding termination or indemnification if it only learned new material adverse information after closing, especially if the target company intentionally failed to disclose the relevant information to get a more favorable valuation.

[40] *See* discussion *supra* Part II. In relation to the Verizon-Yahoo deal, the most applicable substantive focus would be "Track Record." In relation to the cybersecurity breaches of 2014, Yahoo's cybermaturity with regards to Track Record would turn on what measures the company took to reduce the harms of those breaches and to put in place a system to identify and prevent further breaches. While it is difficult to identify what cybersecurity systems Yahoo had in place in 2016, the fact that Verizon was surprised by Yahoo's announcement indicates that any efforts at Yahoo to remedy the 2014 breaches were not well documented (if they existed at all).

[41] *Supra* note 33 (Link to Jill Abitbol)

tive cybersecurity governance, which probably led to the failure to timely remedy and disclose the 2014 breaches, means that time and resources must be expended to safely capitalize on the data assets held by Yahoo. Also, a newly discovered breach is more likely to lead to federal and state regulatory proceedings as well as class action litigation.

The Yahoo-Verizon deal highlights the critical role of cybersecurity due diligence in M&A transactions, particularly from the acquirer's perspective. Although Verizon eventually did achieve its deserved discount of $350 million, this was at least partly a product of Yahoo's voluntary disclosure two months into its discussions with Verizon. In alternative universes where Yahoo failed to disclose, intentionally or not, the result may have been that Verizon closes the deal with incorrect valuation, or that the breaches become known too late in the process for the deal to be saved. By contrast, thorough cybersecurity due diligence by Verizon regarding Yahoo's past breaches, remedial measures and cybersecurity systems may have allowed Verizon to learn about the 2014 breaches, identify the attendant costs and achieve the deserved discount at an earlier stage of the deal negotiation. In any case, thorough cybersecurity due diligence on the part of Verizon would have gone a long way in coming to the same conclusion more efficiently, with less risk.

IV. CONCLUSION

While cybersecurity has already received much attention in the M&A deal context, it remains true that standards are still amorphous and will continue to evolve. Beyond recognizing that cybersecurity is a critical consideration in almost any M&A deal, relevant parties should outline key due diligence objectives with regards to cybersecurity according to substantive considerations[42] and link the resulting findings to valuation, representations and warranties, and other components of the deal.

Without substantial legal obligations touching directly on cybersecurity due diligence, much of the learnings that apply to M&A transactions will occur through trial and error.[43] Because both the United States and South Korea have sophisti-

[42] *See* discussion *supra* Part II

[43] It is worth noting that in the United States, the Trump administration is generally expected to deregulate. For example, as mentioned in footnote nine, a proposed cybersecurity regulation pertaining to large financial institutions (financial institutions with consolidated assets of $50 billion) put forward by the Federal Reserve Bank, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation in 2016 faces much uncertainty, partly due to the new administration's unwillingness to increase regulations. In January 2017 President Trump signed an executive order that required federal agencies to identify two regulations to eliminate every time they propose a new one. Joseph Facciponti et al., *Proposed Federal Cybersecurity Regulation for Financial Institutions Face Uncertain Future*, NAT'L LAW REV. (Mar. 13,

cated and voluminous M&A markets, transferring learnings across the two regions will significantly expedite the trial and error process.

More specifically, companies operating primarily in the United States can learn from their counterparts in South Korea that have placed a greater emphasis on internalizing or customizing cybersecurity functions, to encompass not just individual transactions but all company functions pervasively.[44] By taking on cybersecurity expertise at the operational level, South Korean companies are probably better able to identify and address the particular risks that apply to their businesses and critical processes.

At the same time, law firms operating primarily in South Korea would be well served to learn from law firms in the United States that have devoted much attention to cybersecurity concerns in M&A transactions.[45] As legal advisers in M&A transactions, one of the most important competitive advantages of law firms is the ability to counsel clients regarding pertinent risks, among which cybersecurity is increasingly included. As the Verizon-Yahoo deal demonstrates, cybersecurity risks may even be unknown to or intentionally undisclosed by a target company, in which case it may fall on law firms to identify such risks through thorough due diligence.

Finally, acquirers, and advising law firms should remember that cybersecurity due diligence is necessarily an individualized and contextual inquiry. While a standardized approach may provide a starting point, cybersecurity due diligence should account for valuable assets particular to a target company as well as the present cybersecurity policies and systems in the target company as well as the acquirer. With this broad and thorough understanding of the target company's cybermaturity, identified assets, and risks should be reflected generally in the M&A transaction process, including valuation of the target company as well as clauses in the representations and warranties.

2017), https://www.natlawreview.com/article/proposed-federal-cybersecurity-regulations-financial-institutions-face-uncertain.

[44] *See* discussion *supra* Part II.

[45] *Id.*