Cybersecurity Due Diligence in Corporate Acquisitions

By Joseph V. DeMarco and Jeremy Apple

I. Privacy and Security Due Diligence for Corporate Acquisition and Venture Capital Firms

Recent rapid advances in technology over the last decade have transformed every aspect of our commercial and personal lives. Beyond the everyday use of smartphones and mobile computing technology that has transformed communications, nearly all U.S. small businesses (98%) now use wireless technologies in their operations, with two-thirds (66%) indicating they could not survive without them.[1] As access to the Internet and interconnectivity reaches new heights across the world, commercial enterprises have embraced this technology as both a commodity and a locomotive for daily operations in a global economy. So too have Venture Capitalist (VC) firms and other corporate acquirers, from adopting applications such as commercial acquisition research and analysis to supporting everyday business operations.

Increasingly, corporate acquirers have also—sometimes through painful lessons—grown familiar with many of the common cybersecurity risks posed to organizations. These include network intrusion and disruption by outsiders in addition to the well-known "insider threat." Importantly, this a not a "high-tech" issue, since *every* company collects and maintains data—and the value of such data forms a key component of a company's assets. These factors can, and often do, have real bottom-line financial and public relations implications, as Facebook and other companies have learned the hard way, often repeatedly. In short, information privacy and security failures have real and sometimes devastating legal and commercial implications when not adequately addressed. Home Depot proved this.[2]

Of course, legal liabilities are but one form of harm that can affect companies that get privacy and security issues "wrong." As was evident with the 2011 Epsilon e-mail data theft and resulting Congressional hearings, even where a company is the victim of organized cybercriminal hacking, legislators are not shy about publicly "blaming the victim."[3] Not surprisingly, customers and investors are also quick to penalize companies perceived as lacking appropriate security. And, as more and more companies become sensitized to these issues and insert undertakings into contracts with business partners to prevent them, the consequences of data privacy and security laxity grow exponentially. Thus, sound internal cybersecurity practices are now central to the competitiveness of modern corporate acquirers, supporting financial stability through bolstered commercial reputation and increased operational efficiency.

While some corporate acquirers have sophisticated IT infrastructure and control of their systems (though many do not), the targets of acquisitions by VC firms often are not so cyber-resilient. Although cyber threats by outside hackers and current or former employees plague these companies as well, these businesses are less likely to have significant real or human capital invested in sufficient information privacy and security practices. Thus, the businesses that are subjects to investments or acquisitions may not be well suited to prevent cyber threats or maintain adequate information privacy and security protections. As a result, the cybersecurity risks faced by these organizations have the potential to disrupt or significantly influence acquisitions in numerous ways. Specifically, cybersecurity and information privacy practices have significant implications for corporate acquirers in the related areas of (a) acquisition due diligence, and (b) successor liability, and (c) regulatory enforcement. It is therefore imperative that such firms make information privacy and security matters a priority in their due diligence.

II. Cybersecurity Issues for Corporate Acquirers

A. Pre-Acquisition Due Diligence

Pre-acquisition due diligence is a familiar concept. Typical due diligence analyzes compliance with laws such as the U.S. Foreign Corrupt Practices and UK Bribery Act, Patriot Act, as well environmental law and other areas of compliance. Even apart from compliance imperatives mandated by law, however, savvy investors and acquirers want to know *what* they are purchasing. Indeed, accounts receivables due diligence is one example of diligence performed even though the "quality" of a company's receivables may not implicate compliance with any federal or state statutes.

Like many U.S. businesses across various industries, corporate acquirers have acknowledged the emerging threat of insider misappropriation and fraud to some extent. The recent increase of criminal and civil matters involving theft of company intellectual property, confidential information, or personal identifying information is one byproduct of this growing trend.[4] Studies by organizations like the Carnegie Mellon University Software Engineering Institute's CERT Division and the United States Secret Service National Threat Assessment Center have helped organizations define and recognize the varying motivations and risks posed by current and former employees that harm U.S. businesses.[5] Importantly, the varied motivations of insiders seeking to harm an organization range from pure potential financial gain, to commercial competitive advantage, to simple revenge.[6]

While VC firms are sometimes aware of cybersecurity risks, they typically focus, however, on combating *internal* threats of misappropriation or sabotage by current and former employees. Accordingly, they tend to emphasize the security of information stored in their network from misuse by current and former employees. Equal focus, however, must be placed on *external* threats to VC firms *and* the companies in which they invest. Hackers and other intruders present an array of additional complications for businesses seeking to secure digital assets and protect confidential information. External cyber-threats include wrongdoers seeking financial, personal or corporate information that can be used for an advantageous purpose. From confidential work-product and sensitive business data to network and system architecture information, the loss of internal data can present a significant risk to a parent or acquiring company if misappropriated.

B. Successor Liability and Regulatory Enforcement

Beyond the loss of its own confidential or proprietary data, corporate acquirers should also be concerned with regulatory liability under principles of successor liability.

Successor liability is, of course, nothing new in government enforcement actions. Massive fines and penalties have been imposed upon companies under the Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. (FCPA) and export control area under this principle of corporate responsibility. In an era of vigorous data privacy and security enforcement by the Federal Trade Commission (FTC) and State Attorneys General, as well as mass data-breach litigation, no company can fail to be concerned about its information and privacy security risk profile—or the companies that it does business with or acquires.

Understanding and minimizing cybersecurity risks are especially important VC firms whose business it is to invest in other companies. Any entity seeking to acquire or investing in another company simply can no longer "hope for the best" when it comes to the data privacy and security history of a target company. Notably, the FTC—the federal agency chiefly responsible for enforcing the nation's emerging privacy laws—has since 2008 asserted in publicly filed litigation that where a data breach straddles an acquisition, both the target company *and* the acquiring company bear responsibility for the breach, even where the breach began prior to the acquisition and was not discovered until afterwards.[7] More recently, a major Internet behavioral advertiser almost went bankrupt because it acquired a company that had engaged in questionable data collection practices. When asked how this could have occurred, the head of compliance at the acquiring company said that those questionable data collection practices were "missed in the due diligence."

III. Achieving Cyber Best Practices in Acquisition Transactions

A. Assessment

What can VC firms do to protect themselves and their acquisitions from the threats presented above? Organizations such as VC firms must take precautionary measures on several fronts, including mitigating insider threats, external intrusions, as well as inadvertent loss or disclosure. While no outright formal industry-specific standards exist to benchmark VC cybersecurity initiatives, corporate acquirers can look to subject matter experts (ideally, legal counsel, for privilege purposes) well versed in cybersecurity counseling. Expert counsel can also assist such firms in aligning their cybersecurity and information privacy programs to the guidelines and benchmarks in various financial sector standards laws as Gramm-Leach-Bliley Act and private standards such as the Payment Card Industry Data Security Standard (PCI DSS).[8]

Corporate acquirers should also adapt their governance strategies to confront cyber-risks of acquired-entities with thorough, size and subject-matter appropriate due diligence. While a comprehensive assessment may not be warranted for certain transactions, performing even a basic review of the cybersecurity risks faced by the company being acquired will provide essential insight for the such firms to develop the optimal strategy to mitigate those risks. Cybersecurity experts can provide acquirers with a clear understanding of the true nature of an acquired entity's risk, which may be leveraged in the acquisition. In short, VC firms can work to address particular areas of risk identified by experts, and perform targeted analysis that will maximize the corporate acquirer's return on investment (ROI) in that due diligence.

B. Compliance Review

Beyond retaining an expert to perform a cybersecurity risk assessment, corporate acquirers must also ask essential *legal* questions of the company being acquired. Just as no company can effectively disclaim liability for contaminants in the ground of real property that it owns or acquires (or FCPA liability), no company can avoid the consequences of data and privacy problems "in the ground" at an acquired company. In an era of blossoming regulatory actions, class action litigation, front-page headlines regarding data breaches, supposed online tracking of consumers, and finger-pointing all around when a data mishap or "problematic" use of technology comes to light, avoiding legal exposure and reputational risk is of paramount importance.

Acquirers must therefore consider the legal implications surrounding each type of data that the target company stores in its systems and databases. For example, certain state and federal laws and regulations will govern certain internal protocols for the storage, transmission, or disposal of certain types of information. Corporate acquirers should consider the nature and location of the infor-

mation being both *stored* and/or *used* by the acquiring company. An entity will be subject to certain laws or standards if it stores or maintains certain personal, financial or other confidential information about employees, customers, or third party vendors and partners. Compliance with those regulations and standards will likely depend on the security measures implemented at the physical and logical locations where such information is stored.

Practically, corporate acquirers can formalize the privacy and security practices of a target company identified during diligence assessments and develop a Written Information Security Policy (WISP) and Cyber Incident Response Plan (CIRP) which reflect industry standards and practices. The exercise of creating formal policies surrounding the target firm's security and privacy practices can provide significant assurances that particular information and security standards are met by the target company. Furthermore, where the target company's practices fail to meet industry standards or best practices, acquirers may have additional leverage in certain transactions.

C. Let Industry Standards and Best Practices Be Your Guide

In the end, of course, information privacy and security is not just about risk analysis and minimization. *Even more fundamentally, it is about helping VC firms deepen their understanding of valuation.* For even if a company has not had any data spills, and is not engaging in illegal data collection practices (and the line between lawful and unlawful uses is often quite hard to discern), certain uses of technology are unpopular with business partners and consumers even where they are arguably properly disclosed and permissioned. Similarly, acquirers must also examine their *own* practices and amend their WISP and CIRP to reflect additional cybersecurity or privacy issues emerging in the course of its transactions. Knowing what data a company has and how it obtained that data is, therefore, literally to know what you (a) own, (b) are selling, and (c) are buying. And this knowledge can, when properly analyzed, play a critical role in pricing and valuation. Put simply, it should be a tool in every corporate acquirer's negotiating tool box.

Endnotes

1. *See* AT&T Small Business Technology Poll (2013), *available at* http://about.att.com/mediakit/2013techpoll.
2. *See, e.g.*, Jaikumar Vijayan, *Data Shows Home Depot Breach Could Be Largest* Ever, ComputerWorld (2014), *available at* http://www.computerworld.com/article/2601349/data-shows-home-depot-breach-could-be-largest-ever.html; Trefis Team, *Home Depot: Could The Impact Of The Data Breach Be Significant?*, Forbes (Sep. 24, 2014, 1:39 PM), http://www.forbes.com/sites/greatspeculations/2014/09/24/home-depot-could-the-impact-of-the-data-breach-be-significant/.
3. *See Sony and Epsilon: Lessons for Data Security Legislation: Before the Subcomm. on Manufacturing, Commerce, and Trade*, 112th Cong. (2011), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg71258/html/CHRG-112hhrg71258.htm.
4. *See* Stephanie Overby, *Hacked: The Rising Threat of Intellectual Property Theft and What You Can Do About It*, CIO.com (July 30, 2007, 8:00 AM), http://www.cio.com/article/2438356/risk-management/hacked--the-rising- threat-of-intellectual-property-theft-and-what-you-can-do-about-i.html.
5. *See, e.g.*, Andrew P. Moore, et al., The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures, Carnegie Mellon CERT Program (2008), *available at* http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8703; George Silowash, et al., Common Sense Guide to Mitigating Insider Threats, 4th Ed., Carnegie Mellon CERT Program (2012), *available at* http://repository.cmu.edu/cgi/viewcontent.cgi?article=1669&context=sei.
6. Silowash, *et al.*, at 4.
7. *See* In the Matter of Reed Elsevier Inc. et al., File No. 052-3094, No. C-4226, at 10 (July 29, 2008) ("although some of these attacks occurred before respondent [Reed Elsevier] acquired respondent Seisint, they continued for at least 9 months after the acquisition, during which time respondent Seisint was operating under the control of respondent [Reed Elsevier].").
8. *See, e.g.*, Gramm-Leach-Bliley Act of 2000, 65 FR 31722, Title V, Subtitle A, § 502 (2000); Security Standards Council Payment Card Industry (PCI) Data Security Standards, v. 3.0 (2013), *available at* https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

Joseph V. DeMarco is a partner at DeVore & DeMarco LLP. He previously served as an Assistant United States Attorney for the Southern District of New York, where he founded and headed the Computer Hacking and Intellectual Property (CHIPs) program. Jeremy Apple is an Associate Attorney at DeVore & DeMarco LLP.