Oct 2017

MobileSolve Group, Inc. is a boutique investment bank providing M&A, Capital Raising and Financial Advisory services to technology emerging and growth companies.* This newsletter presents short articles on industry or transaction topics of current interest, and a summary of recent notable transactions.

www.MobileSolve.com

By: Steve Gaynor, Patrick Nguyen and Mansi Srivastava

Cyber-Worries in M&A

The extraordinary breadth of the recent hacking of Equifax, the US consumer data company, has reminded everyone of the importance of security in the digital world. Unsurprisingly, cybersecurity has emerged as an issue in M&A due diligence and deal terms.

Online risks to a company can take several forms. They can involve theft of customer data, company intellectual property or corporate information such as employee or financial records. Alternatively, such records may be destroyed. A “ransomware” attack where criminals lock computers and seek payment to unlock them can disrupt operations and leave the company under threat of extortion.

In addition to such theft, loss and disruption, a company found to have failed to comply with cybersecurity and data privacy laws may be assessed fines, become subject to consent decrees, or have to pay damages in civil suits. A buyer that fails to uncover such problems in its due diligence, or to mitigate their risks in an acquisition agreement, may find itself responsible for these liabilities.

Verizon's Acquisition of Yahoo

A vivid example of these risks playing out in M&A is the acquisition of Yahoo and its one billion users by Verizon for just under $4.5 Billion, which closed in June of this year. Yahoo has since been combined with Verizon’s previously acquired AOL unit to form a new digital media company called Oath. The deal was driven by Verizon's need to scale its online presence to compete with Facebook and Google for digital advertising.

The acquisition was initially announced in July 2016. A bare three months later in September Yahoo disclosed a likely "state-sponsored actor" in late 2014 had stolen account information that variously included names, email addresses, telephone numbers, dates of birth and hashed passwords of approximately 500 million users.

Verizon learned about the breach after terms of the acquisition had been agreed, generating doubt whether the deal would be concluded on the original terms. Then a mere two months later in December, 2016, Yahoo announced an "unauthorized third party" stole user data from more than one billion accounts in August 2013.

That was enough to reduce Yahoo's acquisition price by $350 million, and to require Yahoo to split the cost of any legal liabilities resulting from the breaches. Finally, this month, four months after the transaction closed, Verizon announced all of Yahoo's three billion accounts were hacked in the August 2013 breach.

These recent events have illustrated the risks of insufficient cyber security protections to both buyer and seller in a M&A. Deal professionals are justifiably taking actions in due diligence and deal terms to protect their clients from cyber risks in a transactions.

Digital Due Diligence

In planning the due diligence, the buyer must decide the amount of testing it wants to do on the seller's network security. Ironically, the companies with the most severe security issues are often those that don't realize they have a problem. So the buyer cannot rely solely on the assurances of the seller.

If the seller agrees, which may not always be forthcoming, a buyer may want to engage a third party expert to test the seller's network and conduct searches on the dark web to learn if its information is available for purchase.

Obviously such a step can be expensive and time consuming. A buyer should consider the seller's digital sophistication, any history of online breaches, the value of its digital assets, the regulatory scheme in which it operates, the transaction timeline and whether a third party review has previously been performed and when. The result of the review will be a risk assessment based on the seller's network administration, technical and physical security controls, and actual performance during testing.

An offset to the expense of a third party review may come in the form of a lower premium if the buyer intends to purchase representation and warranty insurance, which has become typical in M&A transactions, or standalone cyber insurance. The purchase agreement representations will undoubtedly include cybersecurity (see discussion below), and the underwriter will consider the quality of the buyer's due diligence review in pricing the agreed terms.

Even where a buyer decides not to engage an outside firm to conduct testing, the due diligence team should interview the IT and other relevant staff at the seller, review the company's cybersecurity governance and vendor management, and examine reports of vulnerability assessments, penetration testing, vendor audits, incident reports and response plans. Of course, if there were any cybersecurity incidents, the team should look into how well they were managed and disclosed to relevant parties such as customers and suppliers, and whether the company informed the appropriate regulators, law enforcement or other third parties.

Deal Terms

As with any due diligence, the results should be reflected in the deal terms to reduce a buyer's risks and to cover the costs of any remediation needed in compliance or risk management, and the potential costs of any post-closing indemnity claims. At a minimum, the representations and warranties should cover the seller's compliance with applicable cybersecurity and data privacy laws, its own internal and external privacy policies, and the lack of any unauthorized access to the seller's data.

A seller should seek to limit such representations and warranties to the actual knowledge of the seller's executives, to impose a materiality threshold on cyber-related claims, and if possible, to include exceptions in the disclosure schedule regarding possible breaches that have not been discovered.

As in the Verizon/Yahoo transaction, indemnity for post-closing claims may be used to hold the seller responsible for its representations and liable for hidden or undisclosed cybersecurity breaches that result in liabilities to third parties. The parameters for such indemnity provisions should be guided by the due diligence findings.

In conclusion, recent events and transactions have exposed the high risks to both buyers and sellers and all of their stakeholders of failures in cybersecurity. M&A practice must keep up with new developments in our digital economy, demanding greater focus on cybersecurity in both due diligence and in deal terms informed by a well-executed due diligence that may involve cybersecurity experts.

Note: This newsletter if for informational purposes only, and not for the purpose of providing legal, financial or other advice.

Transactions

The following are notable M&A Transactions and Capital Financings announced or completed in the last month.

Notable M&A Transactions

Booz Allen Hamilton announced it will acquire Morphick Cyber Security, a leader in managed detection and response (MDR) services. See details here …

Decision Tech acquires Mobilephonechecker, a mobile comparison engine that helps customers compare over 1.2 million deals in seconds. See details here …

Fidelis Cybersecurity acquires TopSpin Security, a provider of deception and detection technologies. See details here …

HeroTel acquires Sonic Telecoms, largest wireless internet service provider (WISP) in Cape Town. See details here …

Intralot acquires Bit8, an iGaming technology company. See details here …

Mitek Systems acquires Icar, provider of consumer identity verification solutions in Spain and Latin America in €12.75 million. See details here …

Start Today acquires VASILY, a Tokoyo based start-up - which runs online fashion coordination service iQON. See details here …

Notable Capital Financings

Altibbi, the Middle East's digital health platform, has raised $6.5M. The round was co-lead by MEVP and DASH Ventures. See details here …

Coverfy, a Spanish Mobile Broker App., has raised €3.5 million. The round was led by K Fund, Seaya Ventures, and Sabadell Venture Capital. See details here …

HYPR, a cyber-security startup, has raised $8 million Series A funding. The round was led by RRE Ventures. See details here …

LimeBike, a leading dockless bikeshare mobile app. company, has raised $50 million in Series B funding. See details here …

MessageBird, a cloud communications platform, has raised $60 million in Series A funding. The round was led by Accel and Atomico. See details here …

Snap, is the first end-to-end mobile messaging platform, has raised $6 million in Series A funding. See details here …

Truphone, "the first global mobile operator," has raised £255m. See details here …

STAY CONNECTED:

Email: **steve.gaynor@mobilesolve.com**

View our profile on LinkedIn