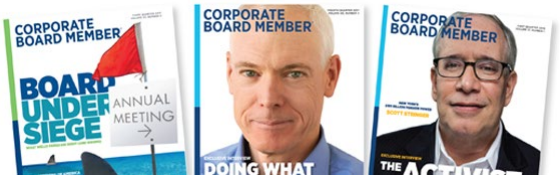
CORPORATE BOARD MEMBER®



MARCH 2019

How Cyber Breaches Will Shape Your Next M&A Deal

By **David R. Owen** and **Kimberly Petillo-Décossard**

The Verizon-Yahoo merger was rocked when two major cyber attacks were revealed mid-transaction. While the data breaches themselves had occurred years earlier, Verizon soon shaved $350 million off its original offer for Yahoo.

Recent headlines suggest that the largest dealmakers continue to face similar challenges as a result of inadequate data-protection due diligence. But, while media reports focus on the largest brands with the most affected customers, middle market companies and their M&A transactions are not immune.

In just the first quarter of 2018, data breaches were reported by 19% of companies with revenues between $50 million and $1 billion, based on a survey by the US Chamber of Commerce and RSM.

For M&A deals of every size, cyber vulnerabilities and cyber breaches are like dangerous pathogens hidden in healthy-seeming patients. And when they go undetected, the consequences are expensive and disruptive, requiring firms to undertake internal investigations, IT remediation projects and public relations campaigns, each of which can last months if not years.

Meanwhile, external actors can drive additional problems, including class action lawsuits, regulatory investigations, Congressional attention, GDPR enforcement actions and federal law enforcement inquiries.

Throughout such storms, senior leaders and key professionals are left to manage the fallout: loss of customers, departure of important employees, damage to critical business relationships and increasingly-expensive cyber insurance.

Just as in medicine, when it comes to cyber due diligence, an ounce of prevention is worth a pound of cure. Yet, M&A trends over the last few years have actually reduced both the time available and the incentives that could help detect such problems. Record levels of dry powder, low interest rates and double-digit multiples have fueled a seller's market. Feeling pressure and afraid to miss opportunities, buyers of every stripe have been willing to compress acquisition timelines, sometimes down to as little as four weeks between proposal and announcement day.

However, with cyber attacks increasingly an issue in M&A deals, boards who are buyers and sellers can take steps to properly inform and inoculate themselves.

Advice for Sellers

If a buyer finds an undisclosed data breach or related cyber security vulnerability during the due diligence phase, it can kill a deal. And while reliable cause-of-death statistics are not available for M&A transactions, anecdotal evidence suggest data security problems are a prolific, if often silent, executioner.

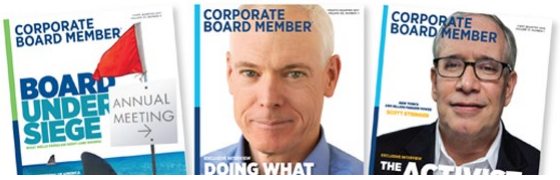
When preparing for a sale, board members and company leaders should initiate their own internal data security due diligence review. It is much better to understand any vulnerabilities independent of a potential buyer. Companies can then groom themselves in order to present the best possible case, by framing any concerns pro-actively.

Preparation by the seller often involves examining and reviewing:

• The types of valuable or legally-protected data the company collects and stores, which can include consumer information, employee data and IP, as well as an analysis of the applicable legal and regulatory rules.

• The company's internal data security policies, employee privacy and phishing training, corporate governance, disaster preparedness and insurance coverage.

CORPORATE BOARD MEMBER®



MARCH 2019

• The company's internal and external assessments and auditing, including penetration testing and/or certification of third-party technical security standards.

• Any material cyber incidents, which can include hacking and phishing attacks, security breaches, regulatory inquiries or criminal or fraudulent activity, plus any regulatory responses, litigation or liability as a result.

With this assessment in hand, sellers are prepared for a buyer's inquiry and can properly address any questions or concerns.

Advice for Buyers

A 2017 survey of M&A executives found that 80% of dealmakers discovered data security issues in at least one-quarter of their deals over a two-year period.
Buyers, then, must be sure to use their pre-signing due diligence time to investigate the full range of data protection issues—rather than deferring the examination to the period between signing and closing, or the post-closing period.

Buyers must not only examine existing policies, staff and relationships, but also must have a solid grasp on historical activity. While past breaches offer an opportunity to improve security and close vulnerabilities, historical information stolen by hackers can still be used to refine future attacks.

Buyer's cyber due diligence should further consider how companies are preparing for future threats. This includes the technical and IT related tools utilized for defense, and also staff training, policies and procedures and regulatory compliance – areas too often over-looked.

Buyers can also protect themselves with the appropriate reps and warranties in the transaction document.

The deal itself is a perilous time for cyber security and can be a magnet for hackers, as further detailed below. Buyers, then, should take responsibility for ensuring that systems, policies and procedures on both sides of the transaction are prepared to identify and defend against attacks before any public announcements.

Advice for Everyone

Just as doctors must take precautions because their work exposes them to infectious disease, the entire deal-making community—from boards and the C-suite, to their lawyers, public relations consultants and investment bankers—must be aware that they are an active and on-going target of scammers and hackers. Precautions are warranted.

The period between announcing and closing a transaction is especially ripe for attacks. Hackers know that companies are not only exchanging confidential information but that attention may be diverted to completing the deal.

Transactions move quickly, and often involve late-night emails on tight deadlines from less-familiar parties with important-looking attachments. This environment is ripe for "spear-phishing," a technique hackers use to mimic trusted senders, in hopes an unsuspecting target reveals information that can later be used to penetrate information systems.

Next, hackers use that information to deploy ransomware attacks, which block access to information systems, or alternatively, threaten to reveal sensitive data, if a ransom is not paid. In fact, ransomware is the fastest-growing weapon in the cyber-criminal arsenal. These tactics are especially effective during an M&A transaction, when time is already of the essence. Hackers know that some companies may be willing to make a problem go away to ensure the transaction moves forward.

Consequently, every organization should ensure its cyber security training is up-to-date. Companies should also consider regular warnings and refresher courses for employees before transactions. During deals, special precautions should be taken. Emails with sensitive information should be encrypted and virtual data rooms should meet the latest security standards, including two-factor authentication.

In today's information-driven economy nearly every company faces some cyber security risk. As a result, proper cyber defense, training, policies and procedures should be an everyday focus, not simply left until a deal is on the horizon.

But when that time comes, a comprehensive cyber examination by both buyer and seller ensures that any issues can be properly incorporated into the deal negotiation, instead of killing it outright.

Without such best practices, dealmakers leave themselves vulnerable to all manner of infectious cyber danger.

David R. Owen and Kimberly Petillo-Décossard

David R. Owen leads the privacy and cyber security practice at Cahill Gordon & Reindel LLP. He is qualified as a Certified Information Privacy Professional (CIPP-US) by the International Association of Privacy Professionals (IAPP), the largest and most comprehensive global information privacy community. Kimberly Petillo-Décossard is a partner at Cahill, where she advises corporations, boards and private equity firms on complex business law matters, focusing on domestic and cross-border public and private mergers and acquisitions and related financing transactions.