CYBERSECURITY AND THE M&A DUE DILIGENCE PROCESS

A 2016 NYSE GOVERNANCE SERVICES/VERACODE SURVEY REPORT

NYSE Governance Services

VERACODE

2015 was a phenomenal year for mergers and acquisitions around the globe: Shell, AT&T, Kraft Heinz, Kinder Morgan, Charter Communications, Albertsons, Anthem, Dell, andAetna, to name a few.

Boards of directors have a great oversight responsibility in these transactions, more so against a backdrop where the risks of cybersecurity breaches are continuously on the rise. In the fall of 2015, NYSE Governance Services teamed up with Veracode to conduct a survey of 276 public company directors and officers to draw parallels among the cyber risk management practices of corporate directors in an M&A environment and provide benchmarking practices to serve the interest of public companies' boards of directors and their shareholders. This report presents our findings.

THE NUMBER OF SIZEABLE DEALS ACROSS ALL sectors increased at a rapid pace in the past five years, and 2015 was a record-breaking year for acquisitions. According to Dealogic, global M&A volume reached $5.05 trillion, surpassing the 2007 record of $4.6 trillion. The data firm reports that nearly half of the 2015 activity targeted US-based companies, while Europe accounted for a third, followed by the Asia Pacific region with approximately a quarter of the total value. In the UK, total M&A deals reached $621 billion, the highest recorded since the $826 billion seen in 2000, although experts predict a possible surge on the back of a weakening Sterling Pound caused by Brexit.

Today, as we enter the third quarter of 2016, the election cycle, terrorism, and tightening regulations have so far pushed withdrawn M&A volume to a record high in the US, particularly with the withdrawal of five jumbo deals—including Allergan and Pfizer, the biggest on record to date. While 2016 activity is said to have fallen to its lowest year-to-date level in 21 years, major deals such as Sherwin-Williams, Marriott, Fortis, Tyco, TransCanada, and Shire, have nonetheless managed to leave their mark on this otherwise rapidly deflating M&A landscape.

Three-quarters of respondents say a high-profile data breach at an acquisition target would have serious implications **on the pending transaction.**

Sound mergers and acquisitions fuel economic growth, but they also carry a certain level of risk and, therefore, entail a highly extensive due-diligence process. Manifestly, an acquiring company will want to authenticate what it is buying—assets, threats, vulnerabilities—and the process of doing so has been intensifying.

Twenty years ago, acquiring companies mainly focused on the evaluation of a target's fundamentals, which primarily comprised financials, consumer sentiment, and strategy. Cybersecurity and IT due diligence was carried out in less than 50% of deals[1]. A Freshfields Bruckhaus Deringer report revealed that just a year ago, 78% of deal makers still didn't specifically quantify cybersecurity as part of their M&A due diligence process.

Modern M&A practices are only now beginning to show signs of change, despite the well-known impacts of the mere discovery of software application vulnerabilities on the profitability and reputation of an organization, as well as the significant disruption to productivity and business processes in general. Buying a company translates to buying data. And buying data means you are buying past, present, and future data security problems. The economic impact of a transaction can shift dramatically if, after the deal is consummated, past or ongoing data breaches come to light.

If boards of directors are in fact beginning to pay greater attention to a potential target's cybersecurity efforts during their M&A due diligence process, it matters which aspects of the target's infrastructure are being evaluated, how the audit is conducted, and who is included as part of the discovery and analysis process.

As a result, NYSE Governance Services, in collaboration with Veracode, surveyed 276 directors and officers of public companies to determine if and how the growing presence of cybersecurity threats has had an impact on their M&A due diligence process.

Firms betting on an M&A strategy may be well advised to pay heed to their cybersecurity efforts. While a high-profile data breach may not be a complete barrier to a merger or an acquisition for many organizations, more than half (52%) of surveyed directors and officers claim it would significantly lower the valuation (Figure 1).

In fact, 85% say the discovery of major vulnerabilities during the audit of an acquisition target's software assets would "likely" or "very likely" affect their final decision (Figure 2), and one out of five (22%) directors surveyed say the occurrence of a high-profile data breach at an acquisition target would deter them entirely from completing the transaction.

FIGURE 1

WOULD YOU CONSIDER ACQUIRING A COMPANY THAT HAS RECENTLY SUFFERED FROM A HIGH-PROFILE DATA BREACH?

FIGURE 2

THE LIKELIHOOD OF MAJOR SECURITY VULNERABILITIES AFFECTING A MERGER OR ACQUISITION

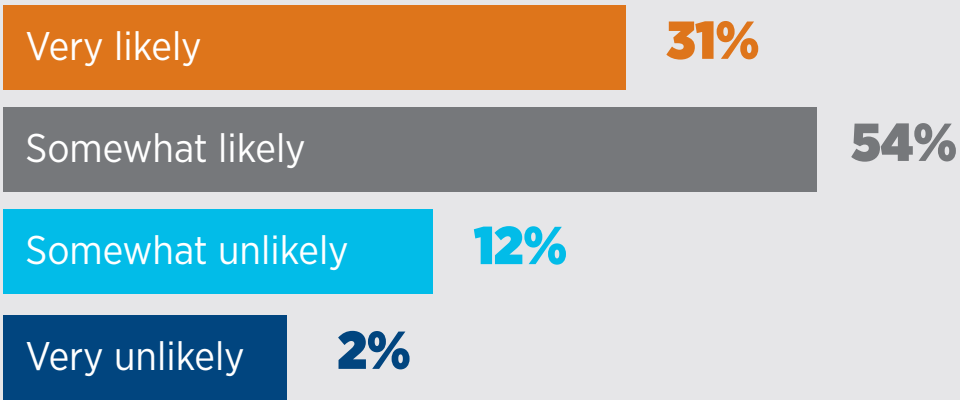


FIGURE 3

COMPONENTS OF M&A DUE DILIGENCE PROCEDURES

For example, had Telstra known about Pacnet's breach before signing a deal to acquire them, would Telstra have improved their standing in negotiations or ended them entirely? As reported by Bloomberg, Pacnet only informed Telstra after the deal had gone through that an SQL injection on a web application server in Pacnet's network had allowed access to its network, and a third party had gained access to Pacnet's corporate IT network, including its email and administrative systems.

Most corporate officers today understand the impact of major cybersecurity vulnerabilities on a target's valuation, as well as on the resulting entity, including its brand and reputation. Surely, the highly publicized consequences of recent breaches on affected companies have served to boost that awareness. While there may still be room for improvement, our survey indicates that a great majority of companies now use cybersecurity audits—such as application security assessments—to obtain assurances that their M&A due-diligence process is conducted in a manner that limits any potential future damage once the deal goes through.

Two-thirds of companies surveyed say their due-diligence process includes a security audit of the target's **software applications.**

In addition to reviews of recent compliance audits (83%) and security policies (86%), which continue to take precedence in the cybersecurity due-diligence process for mergers and acquisitions, 64% of directors and officers say their company conducts an audit of software applications and how secure they are as part of the due-diligence process (Figure 3). To start, due diligence around application security audits should look to existing regulations as a baseline. The energy industry has NERC CIP, health care has HIPAA, and anyone who takes and stores credit card information falls under PCI DSS.

Three-quarters of directors place the quality of intellectual property, as a top consideration in their M&A due-diligence process.

Where regulations don't help, however, is in assessing the risk potential of the expanded security perimeter created by adding every web application from the acquired company. It is common practice to create "short-lived" sites that often get forgotten and become a security risk. Case in point, British pub giant Wetherspoons suffered a breach due to the company failing to decommission old web applications, illustrating how companies that don't take steps to determine the full scope of their IT environment leave themselves open to be exploited through unpatched vulnerabilities in these forgotten applications.

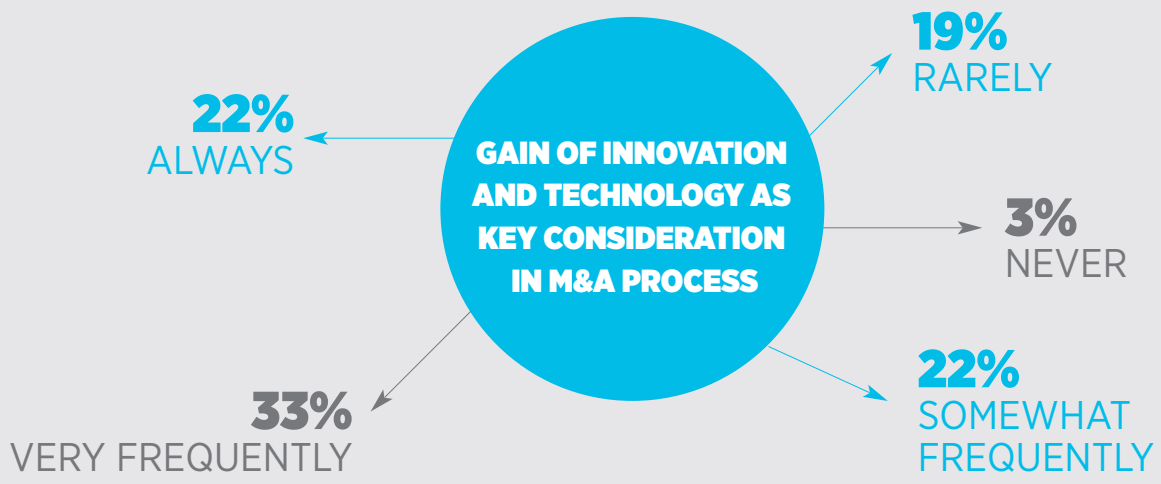
In fact, web application perimeter assessments conducted by Veracode over the past two years found more than 350,000 web applications that customers were unaware of—nearly 40% more than they thought they had. Due diligence prior to an acquisition needs to incorporate means to identify risks the target company doesn't even know it has.

This increased cognizance over application security risks shouldn't come as a surprise, considering that software assets are a critical part of what is being acquired by today's companies. In fact, 77% of respondents say the gain of innovation and technology can be a key consideration in their M&A discussions (Figure 4).

Indeed, besides the fundamental concerns regarding an organization's financials and strategy, almost three-quarters of directors and officers (71%) place the quality and extent of intellectual property (IP) and technology, such as applications, as a top consideration in their M&A due diligence process (Figure 5).

FIGURE 4

GAIN OF INNOVATION AND TECHNOLOGY AS KEY CONSIDERATION IN M&A PROCESS



At this time, the only way for the board to uncover latent risks and mitigate future hits to the company's reputation is to conduct a comprehensive audit of the target's cybersecurity protocols. For example, unbeknownst to Ares Management as it was in the midst of negotiating to acquire Neiman Marcus for $6 billion, cyberattackers had compromised the high-end retailer's payment security system, walking away with credit card data for hundreds of thousands of customers.

FIGURE 5

IMPORTANCE OF DUE DILIGENCE CONSIDERATIONS DURING THE M&A PROCESS

	Very important	Somewhat important	Not important
Financial: Past performance and reasonableness of projections	**95%**	**5%**	**0%**
Technology: Quality and extent of intellectual property and technology	**71%**	**25%**	**4%**
Customers: Customer satisfaction, concentration issues, and other sales issues/risks	**76%**	**23%**	**2%**
Strategic: Fit with buyer	**94%**	**6%**	**0%**
Material contracts	**49%**	**49%**	**3%**
Employee/management issues	**50%**	**47%**	**3%**
Litigation	**59%**	**40%**	**1%**
Regulatory issues	**65%**	**34%**	**1%**

Beyond the obvious threats to cybersecurity, conducting an audit of cybersecurity protocols can also reveal vulnerabilities that could require significant expenditures for the acquiring company. Furthermore, overlooking this step could increase the risk of liability suits for negligence or lack of due care on the acquirer's part.

Unfortunately, the people typically involved in an M&A transaction often do not have the technical skills necessary to thoroughly assess the cybersecurity or application security risk of a company, particularly given the fact that if difficult to detect from the inside, system vulnerabilities—whether internal or relating to third-party applications—are even harder to expose as an outsider.

As a result, companies involved in an acquisition may benefit from enlisting the support of cybersecurity experts to not only assist in the audit process of uncovering hidden flaws, known or otherwise, but also to ascertain the true cost and consequences of such vulnerabilities. Outside consultants could play a pivotal role in determining the value of an acquisition or integration target, based on these findings.

[1] James A. Sherer, Taylor M. Hoffman & Eugenio E. Ortiz, Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, e-Discovery, and Information Governance into Due Diligence Practices, 21 Rich. J.L. & Tech. 5 (2015), http://jolt.richmond.edu/v21i2/article5.pdf

JOIN OUR RESEARCH PANEL AND REAP EXCLUSIVE REWARDS

The quality of our research relies on direct input from you so that we can bring rich data sets and fresh insight to the corporate governance community and help you build strategies for success. That is why when you agree to participate in only three surveys per year, you are awarded one free pass to an NYSE Governance Services conference of your choosing, among other benefits! We invite you to contact our research editor at Melanie.Nolen@nyse.com for all the details about our research panel.

ABOUT VERACODE

Veracode is a leader in securing web, mobile, and third-party applications for the world's largest global enterprises. By enabling organizations to rapidly identify and remediate application-layer threats before cyberattackers can exploit them, Veracode helps enterprises speed their innovations to market—without compromising security.

Veracode's powerful cloud-based platform, deep security expertise, and systematic, policy-based approach provide enterprises with a simpler and more scalable way to reduce application-layer risk across their global software infrastructures.

Veracode serves hundreds of customers across a wide range of industries, including nearly one-third of the Fortune 100, three of the top four U.S. commercial banks, and 27 of Forbes' 100 Most Valuable Brands. Learn more at www.veracode.com, on the Veracode blog, and on Twitter.

ABOUT NYSE GOVERNANCE SERVICES

NYSE Governance Services is the leading governance, compliance, and education solutions provider for companies and their boards of directors. Through a complete set of technology-enabled and data-driven solutions designed to address compliance, accountability, and risk management, NYSE Governance Services helps companies comprehensively build a culture of integrity from employee to board level. NYSE Governance Services is a subsidiary of the New York Stock Exchange Group, an Intercontinental Exchange company (NYSE:ICE). For more information, connect with us at nyse.com/governance, @nysegov, or LinkedIn.