protiviti®
Face the Future with Confidence

Private Equity and Cybersecurity – Gaining a Holistic View

An emerging trend among private equity firms is their growing attention to the remediation, monitoring and reporting of cybersecurity capabilities of the companies in their portfolios. Historically, they have not fully appreciated the varying degrees of cybersecurity risk relative to a company's specific industry. And understandably, the emphasis on investing in promising businesses and improving their operations to add value and create attractive acquisition or initial public offering candidates has typically taken precedence over other considerations.

Yet today, enhancing a company's valuation means ensuring it possesses sound cybersecurity systems, protocols and procedures. It is a requirement that has become as vital as shoring up an accounting, supply chain or customer service function, particularly over the past several years amid the rising threat of companies falling victim to cybercrime.

A Growing and Costly Threat

Even before COVID-19, the cost of global data breaches, virus attacks, phishing and other cybercrimes was expected to reach $6 trillion in 2021, up from $3 trillion in 2015, according to cybercrime researcher Cybersecurity Ventures. Beyond direct losses in the form of funds, data or intellectual property, organizations that allow hackers to steal data or breach the privacy of their customers or employees also face the potential of fines, lawsuits, loss of revenue and damage to the brand.

The pandemic and subsequent economic lockdowns that forced the vast majority of corporations to pivot to a work-from-home operating model have only increased cyber risk and emboldened malevolent actors to intensify their attacks on digital infrastructure. In a recent poll conducted by *Threatpost*, an IT and business security news organization, 40% of corporations reported a rise in cyberattacks as they shifted to remote working.

The increasing emphasis on digital threats and IT security parallels a growing investor focus on environmental, social and governance (ESG) issues, which adds further pressure on private equity firms to consider the data and privacy strength of their portfolio companies. Following the

lead of the European Union, which introduced the General Data Protection Regulation (GDPR) as law in 2018, California enacted the California Consumer Privacy Act in 2020. Currently, roughly 60 countries have data and privacy rules on the books and 14 states in the U.S. are mulling similar measures. In all likelihood, private equity firms have portfolio companies operating in many of these jurisdictions.

Valuation Risk

Ultimately, portfolio companies that lack effective IT security or that have yet to reconcile a past cyberattack will be less attractive to potential buyers. That can not only erode the value of a private equity firm's investment, but it also can tarnish the firm's reputation and negatively impact future fundraising. Thus, resources invested today to enhance portfolio company cybersecurity will save money in the long run.

A strong commitment to IT security starts at the top, and while some private equity firms have been slow to adjust their focus beyond the traditional valuation metrics of companies within their portfolios, more are becoming cognizant of cybersecurity risk and the necessity to address it. That's especially true when private equity firms are buying or making an initial investment in a company.

Despite this growing recognition, however, the private equity industry has lacked a practical approach to address the cybersecurity issues and concerns of their portfolio companies. The reality is that assessing and formulating a tailored cybersecurity strategy for each company in a portfolio is an inefficient prospect that would saddle the companies as well as the private equity firm with undue investment in time and costs. What's more, private equity teams may feel compelled to focus their cybersecurity efforts on their most highly valued investments when in reality companies with lower valuations may be in greater danger.

Adopting a Holistic Approach

So what is the best way for private equity firms to tackle the cybersecurity needs of their investments? An ideal solution involves looking at portfolio investments holistically versus individually – that is, bringing the IT security of portfolio companies as a group to an acceptable minimum threshold, and then maintaining that threshold and/or tweaking it for specific company needs. The strategy provides private equity firms with a number of benefits, including the ability to:

- Leverage cybersecurity assessment and protection spend across the portfolio, creating greater efficiency compared with evaluating each company individually.
- Identify companies with higher risk to cyber threats, as well as those in specific industries that present unique IT security challenges, and formulate a game plan on how to address them.
- Establish the practice at the fund level as another foundational business function akin to financial reporting or investor relations, demonstrating a commitment to responsible governance in an era in which investors are focusing more on ESG concerns.

Following is a high-level overview of a holistic security risk program for private equity firms.

Maturity Self-Assessment and External Exposure Assessment

As a first step, private equity firms should assess the current state of cybersecurity within their portfolio companies.

- Conduct a security benchmarking survey based on leading industry frameworks.
- Perform a maturity self-assessment survey for selected portfolio companies and related IT security programs.
- Develop profiles of company-specific threats for each company in a portfolio.
- Analyze survey and threat assessment results and how they compare with the risk appetite of the private equity firm, other portfolio companies and industry data.

Targeted Assessment Procedures

This step is focused on companies in a portfolio that rank below threshold maturity and/or that face an elevated risk. It also covers companies in which private equity management is considering investment decisions. Whatever the case, targeted procedures that are performed include:

- Cyber risk quantification
- Security program assessment
- Internal vulnerability scanning
- Social engineering and phishing testing
- Incident response and compromise assessments
- Other industry-specific actions

Reporting and Analysis

Develop reports on overall IT security risk exposure based on self-assessment maturity benchmarks and targeted procedures, and create detailed summaries, observations and maturity scoring at the portfolio and individual company levels.

In Closing

At a time when cybercrime is growing, private equity firms need to illustrate that they are governing their portfolio companies in a way that recognizes and addresses cybersecurity issues. The maturity level of private equity firms varies on these matters, but regardless of where they find themselves, private equity firms should adopt a holistic approach to ensure that their portfolio companies have an acceptable minimum threshold of cybersecurity proficiency.

Private equity executives must set the tone at the top in order for the firm to take action. Those that step forward will not only enhance the chances for a profitable exit of their investments, but they also will demonstrate proper governance to their investors. Private equity firms will undoubtedly be happy to highlight both capabilities when it is time to raise capital.

How We Help Companies Succeed

The current market environment presents both challenges to and opportunities for the traditional private equity operating model. Firms that have increased their operational focus are enjoying a competitive advantage stemming from their ability to strengthen their portfolio companies while at the same time identifying and mitigating challenges presented by rapidly changing markets. Increasingly, firms are looking to implement portfolio-wide risk management programs to create greater governance and confidence. At the portfolio company level, the focus is on executing targeted business, operational and financial changes that improve cash flow and enhance competitive advantage.

Private equity firms are turning to Protiviti for our problem-solving capabilities as they look to identify and create value. From our business consulting skills to our risk management and internal audit depth, we work with private equity firms and leaders of portfolio companies to help them achieve greater confidence in this changing environment. We seek to understand the unique strengths, risks and opportunities of your portfolio companies and where you want to take these businesses. We then collaborate with you to build custom solutions that maximize your chances for success and bring a tailored, multidisciplinary team of professionals that fits your situation. While the process is never simple, our goal is to help you face the future with confidence.

Contact

Rob Gould
Managing Director
+1.212.708.6354
rob.gould@protiviti.com

Terry Jost
Managing Director
+1.469.965.6574
terry.jost@protiviti.com