September 2017

Acquisitions: Cyber Concerns to Consider

Mark Alberto, MBA, Vice President - IT, The Graham Company
Marc D. Leone, Esq., Producer, The Graham Company
Peter Nadeau, MBA, Consultant, Fiduciary Investment Advisors

Last month, a data breach at a large scale health network gave hackers access to the files of 300,000 patients, exposing private data including names, addresses and even social security numbers. The breached health group had recently completed a merger – and while the exact type of system failure that allowed this cyberattack to occur cannot be identified, this incident does shed light on a potential liability that is often overlooked during mergers and acquisitions (M&A). As the growing threat of cyberattacks and the aftermath of successful breaches continues to play out for organizations across the U.S., cybersecurity is becoming an increasingly important consideration for businesses to examine prior to executing a merger or acquisition.

In 2016, the global M&A market reached volumes of $39 trillion – the third highest year on record, with comparable levels predicted throughout 2017, according to a report by J.P. Morgan. While M&A contracts are frequently executed by companies across many verticals under a variety of circumstances, the goal is typically the same – to increase strength and resources and ultimately improve profitability. To ensure the overall long-term success of the transaction, organizations should not only consider potential cyber concerns associated with the acquired company, but should also work to identify solutions to reduce risk as part of the M&A due diligence process.

Cybersecurity Considerations

As M&A transactions continue to increase in both volume and complexity, organizations acquiring a secondary entity will first need to assess the target entity's information security programs to ensure that proper and sufficient precautions are in place. This is especially important because if the acquired organization has sub-standard safeguards, the acquiring company is at a greater risk of being successfully hacked.

Unfortunately, when one enterprise is in the process of acquiring another, the acquired organization could already have unknowingly been breached, setting the acquiring company up for significant risk once the target company is acquired. In 2017, the Ponemon Institute's Cost of Data Breach Study found that the average cost of a data breach was $7.35 million. Therefore, this is a particularly important consideration during an acquisition, as the damages resulting from a breach are inherited by the acquiring organization, which could result in significant expenditures.

In addition to evaluating potentially unidentified cyber exposures, organizations need to consider how their cyber risks will evolve following the acquisition. The acquiring company should first assess both the amount and the type of data being acquired. For instance, if the acquired organization frequently handles credit card information, the acquiring company will need to confirm their ability to properly protect this specific type of data and to comply with applicable Federal and State regulations.

Cyberattacks are not limited to the organization's financial data, but may also impact individual retirement plan participants. Plan sponsors offering retirement plans to their employees are at risk, as are retirement plan recordkeepers. All facets of the retirement plan's processes should be reviewed to ensure security and consistency across organizations. Areas of scrutiny will include, but are certainly not limited to, payroll files, data remittance, and website access.

Solutions

When acquiring an organization, it is crucial to take steps to improve cybersecurity measures as the likelihood of a breach increases as the total cyber footprint expands. Businesses should first develop and implement a thorough plan based on appropriate Federal and State requirements to assess the risks associated with the acquisition. In addition to performing both vulnerability and penetration testing of the new network, a third-party security firm should be brought on to inspect the network for potential threats and bad actors that may have already breached their systems.

Next, all employees should be regularly trained to recognize common threats like social engineering fraud and phishing schemes. According to an IBM Security report, 60 percent of successful cyberattacks in 2015 either originated from within the organization or were the result of internal missteps. Email-born threats against employees are the easiest way for hackers to breach an organization, therefore representing the greatest risk. It is critically important that staff is trained to identify and report suspicious emails.

All third-party relationships should be vetted from a cybersecurity perspective if they hold or have access to sensitive employee data. Oftentimes, during a merger the retirement plans are consolidated to a single vendor so as to take advantage of potential pricing and administrative benefits. A company should consider reviewing the vendor's contractual protections and insurance arrangements for cybersecurity events. Does the vendor have disaster recovery procedures in place? Are they conducting independent audits? Furthermore, are all those involved with the consolidation properly trained with regard to the handling of sensitive information? These are just a few of the many questions that should be considered when evaluating retirement plans in conjunction with a merger. An independent consultant may be able to assist with the process and documentation of this type of undertaking.

Finally, organization executives should work closely with their insurance broker to ensure that all cyber threats are properly analyzed and adequate coverage is in place, should a costly breach occur. Appropriate coverage not only provides necessary protection when a breach occurs, but can also provide front-end resources to reduce risk and protect against a breach occurring. As cybersecurity continues to become an increasingly significant business risk, vigilant brokers can help executives stay informed about the latest industry developments and protections, providing them with peace of mind that their business is secure.

About the Authors

Mark Alberto, MBA, Vice President – Information Technology, joined The Graham Company in 1996 and is the Vice President for Information Technology providing business innovation and cyber protection through the effective use of technology.

Marc D. Leone, Esq., Producer, joined The Graham Company in 2016 and works with clients across all industry groups at The Graham Company. Prior to joining The Graham Company, Marc spent seven years as a corporate attorney with one of the largest international law firms where much of his practice focused on Mergers & Acquisitions. Marc is a graduate of The Johns Hopkins University and Villanova University School of Law.

mleone@grahamco.com
215-701-5330

Peter Nadeau, MBA, is a Consultant at Fiduciary Investment Advisors, LLC (FIA). Based out of New Jersey, his focus is on defined contribution retirement plans in both the corporate and tax-exempt spaces. He has extensive knowledge in 401(k), 401(a) and 403(b) plan consulting. Peter received a Bachelor of Arts at the University of Hartford and later received both a Master of Science as well as a Master of Business Administration.

pnadeau@fiallc.com
973-240-8602

Fiduciary Investment Advisors, LLC ("FIA")

FIA is an independent institutional consulting group with over 20 years of investment consulting experience. FIA is an employee owned firm with 100% of the firm's revenue derived from fees clients pay for investment advice. Our mission is to provide customized investment consulting services to assist our clients in achieving their investment and financial objectives, while fulfilling their fiduciary obligations. Our clients include corporate retirement plans, endowments & foundations, public plans and private clients. Our consulting services include:

- Investment Policy Statement Review/Creation
- Retirement Service Provider Search (RFI/RFP)
- Plan Benchmarking
- Investment Menu Analysis and Design
- Total Plan Fee Analysis (full fee disclosure)
- Fiduciary Governance Consulting
- Investment Fund Performance Measurement, Analysis and Reporting
- Risk-Based Model Portfolio Construction
- Employee Communication and Education
- Asset Allocation Analysis
- Investment Manager Searches
- Liability Driven Investment ("LDI") Strategies for Pension Plans
- Quarterly In-Person Meetings with Finance/Investment Committees
- Strategic Guidance on Relevant Topics of Interest