JBW Group International
Information Assurance

Why Information Security is a Critical Aspect of M&A Due Diligence

An Executive Update Volume 1 Number 3 April 2009

Most due diligence activities focus on a financial analysis of profit/loss and the bottom line. Experts from accounting firms, venture capital companies and law firms are very good at assessing the profitability and potential synergies of a merger/acquisition. But frequently, little, if any, attention is paid to the security posture of the organization under scrutiny, often with disastrous results.

An Information Security and Privacy Assessment should be part of any M&A activity to fully identify and understand the potential risks of the transaction.

Why an External Assessment is Critical

Using your own internal information security professionals to conduct due diligence takes them away from their daily operational responsibilities and may push the limits of their expertise

Organizations that do consider information security, privacy and compliance as part of due diligence likely call on their internal security experts for help. These internal resources are very knowledgeable security professionals that are already stretched thin with daily operational security activities. They also may lack the necessary legal and regulatory compliance and privacy assessment skills to address that area of due diligence. And like so many due diligence activities, time is of the essence.

"The majority of security breaches related to merger and acquisition activities are failures of business processes, not failures of technology."

continued on page 2

Failures of Due Diligence

Customer Data Breach: LexisNexis

In March of 2005, LexisNexis, an international information brokerage, reported a security breach that exposed the personal financial records of 32,000 individuals. This breach was significant not only because of the number of exposed records but also because the breach occurred at a newly acquired subsidiary.

Employee Information Breach: Vekstar

In September of 2006, after Vekstar acquired Indianapolis-base Telesource, employees discovered their personnel files in a dumpster. Files containing Social Security Numbers (SSNs), dates of birth and photocopies of SSN cards and driver's licenses for an unknown number of Telesource employees were found after the office was cleaned out and shut down.

These examples illustrate how ignoring Information Security prior to a merger or acquisition can have severe consequences. ◙

continued from page 1

The solution to protecting a company's reputation, bottom line and its critical internal and customer information is to look outside the organization for professional help. The best solution is to work with consulting resources that are skilled in the all three areas and can *also* provide the bridge between the practitioners and the boardroom.

Organizations that go through the time and expense of pursuing M & A activities have identified compelling business reasons for pursuing the target organization. The objective in information security due diligence should not be to reject or rubber stamp the transaction but rather to provide a more complete picture of the associated risks for the decision makers. Being able to anticipate potential areas of risk in a target organization can smooth the transition, avoid surprises and help realize the shareholder value that made the deal attractive in the first place.

Prevention Strategy

External help to assess the information security posture of the target organization benefits the acquiring company in numerous ways:

- Provides an objective third-party assessment
- Enables the communication bridge between security practitioners and the board room
- Provides resources and expertise not available internally
- Expedites the due diligence process
- Frees critical internal resources to do what they do best

M & A Due Diligence for Information Security

Using ISO 27001 as a guiding framework and basis for assessment methodology, JBW Group International will assess a target organization's information security posture and gather critical information for these and other critical questions:

- What is the current information posture of the organization?
- Is there a comprehensive inventory of critical information assets?
- Is there ownership, responsibility and authority for security? Privacy? Legal and regulatory compliance?
- What are the information security risks associated with this transaction?
- What efforts would be required to address the most critical risk areas?

John B. Weaver, president and CEO of JBW Group International, advises executive management to think beyond the financial and legal assessments of due diligence and utilize external information security experts to proactively review the information security status of the target organization. The time to find out about inherent security weaknesses and create plans for remediation is before the transaction takes place, not after.

JBW Group International would like to work with you to add a critical aspect of any due diligence activity – understanding the information security, privacy and compliance risk. ◙

"Breach notification laws have been enacted in 34 states and federal legislation is under consideration. . .

There is no avoiding the potential PR nightmare that comes with an information security breach."

For More Information…

JBW Group International

P.O. Box 19373

Minneapolis,

Minnesota 55419 USA

www.jbwgroup.com

Email: info@jbwgroup.com

1.877.97.27001