Technical Assessment

In support of mergers, acquisitions and investments

Mergers, acquisitions and investments ("investments") carry inherent risk with them and, as an investor, you attempt to identify and evaluate these risks.

The business plan is reviewed, the financials are evaluated and often, even the staff is interviewed.

But what about the company's technical report card? How important is technology in a particular investment?

If the company is a technical company, the investor should evaluate the development, QA, release and bug management processes, among others, to understand the level of technical maturity, and the risk the investor is assuming. This process can be a very technical one.

Sample components of any effective M&A technical assessment program (for both technology and non-technology companies) include:

- Identify the cyber crown jewels – this is what a thief is going to try and steal. This could be financial, trade secret, credit card, health care or other sensitive information.
- Review access control tools, methodology and implementation. Could an employee, contractor or vendor walk away with the crown jewels and sell them or compete with you?
- Review vendor access to the business information systems? Is each vendor's technical environments, policies and training evaluated periodically? The breach at Target in 2013 was caused by an air conditioning contractor clicking on a link in an email.
- Review IT audit capabilities. In the absence of good audit data and processes, if a breach occurs, it may go unnoticed. (See article on LaCie breach below. LaCie learned of the breach when the FBI knocked on it's door).
- Review information backup, disaster recovery and business continuity plans. In some cyber-attacks, the information is silently stolen. In others, the systems are compromised and must be shut down and rebuilt from known good backups. How well will this investment respond to a disaster or attack.
- Create or review cyber breach public relations strategy. Some firms (see link to Jimmy Johns breach below) believe a good strategy is silence, denial, and as a last resort, confirmation. Assume that you will be attacked in the social media; have a response plan ready.
- Are public facing web sites and social media sites secure? Has an external security assessment team be engaged and were the issues found addressed?

The list above is not complete. Does the company deal with any regulatory agency? Does it have a breach response plan? Is its software licensed and can they prove it.

Prior to making an investment and periodically post investment, a technical audit can help an investor reduce the risk inherent in his or her investment.

Mitch Tanenbaum Consulting Mitch@mtanenbaum.us 720-891-1663

About Mitch Tanenbaum

Mr. Tanenbaum has over 30 years of experience in managing data centers, computer operations teams, developers and security teams. Mr. Tanenbaum started out as a developer of real time command and control systems and from there moved into managing IT Operations and information security. In the role of Chief Technical Officer he has been responsible for the development of large scale systems in support of the mortgage and banking industries, supporting several of the top five US banks. Most recently, he was the CTO for an information security startup creating a new paradigm for protecting information wherever it travels.

Articles:

http://www.itproportal.com/2014/04/17/fbi-alerts-storage-company-lacie-of-year-long-data-breach/

http://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system/

http://www.csoonline.com/article/2458048/security-leadership/insecure-connections-enterprises-hacked-after-neglecting-third-party-risks.html

http://ww2.cfo.com/technology/2014/07/five-tips-preventing-cyber-security-breaches/

http://krebsonsecurity.com/2014/07/sandwich-chain-jimmy-johns-investigating-breach-claims/

http://www.azcentral.com/story/money/business/abg/2014/07/27/cyber-security-growing-problem-small-business/13242313/

http://www.idt911.com/KnowledgeCenter/NewsAlerts/NewsAlertDetail.aspx?a=%7BEE057FC3-BEB3-49AC-815D-3076E517D7CC%7D (government alerted 3,000 businesses to breaches)