Cyber Risk Mitigation

As businesses increase the amount of information that is stored digitally, the protection of that information is an important concern.

After Target had a security breach, sales went down 14% and they will spend over a billion dollars to cover costs related to that breach. Target was in the news, day after day, and not in a good way. Customer's attention was focused on the security breach rather than Target products and services. To make things more complex, the source of the attack was a third party vendor who allowed its systems to be compromised and Target is now suffering the financial and PR consequences. Fines in healthcare can be up to $1.5 million per violation and most incidents are broken down into multiple violations.

Cyber risk management is the component of a company's overall risk management strategy that addresses the risk to a company's reputation, sales and finances associated with storing information electronically versus on paper.

For all but the very smallest company, some executive should be fulfilling the role of Chief Risk Officer (CRO). For smaller companies, this is a part time job and the person performing in this role is likely not a risk management professional. Consultants can play an effective role in assisting the executive acting as the CRO in creating and managing the company's cyber risk mitigation strategy.

Even large, well prepared companies have cyber risk events. See article below on the Israeli defense firms that were plundered

Sample components of an effective cyber risk management program 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.
- Determine access requirements and controls by role of user. Groups to consider include employees, contractors, vendors, customers, regulators and the public.
- Create and deliver user training regarding the protection of corporate information
- Determine audit requirements and review processes and assign the individual responsible for reviews.
- Create or 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.
- 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 and have a response plan ready.

The list above contains samples and is not complete. For example, do you need to deal with any regulatory agency? Many times businesses find out about breaches when the FBI comes to visit (see article on LaCie below). Do you have a plan for what happens when the FBI knocks on your door and seizes all of your computers as evidence?

Companies that have an effective cyber-risk mitigation strategy and plan will be much more likely to effectively deal with a cyber-incident with the least pain and damage.

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

http://www.idt911.com/KnowledgeCenter/NewsAlerts/NewsAlertDetail.aspx?a=%7BEE057FC3-BEB3-49AC-815D-3076E517D7CC%7D