EXECUTIVE INSIGHT – THE HIGH COST OF HACKERS AND OTHER SECURITY BREACHES

It seems like every day we read about another company whose computers have been compromised by some form of hack.

CEO's and owners of small and medium sized businesses oftentimes lack the security resources that are afforded to much larger organizations to prevent a security breach or adequately respond to a breach that could lead to significant penalties. Some state statutes charge as much as $2,500 per customer record exposed or many states require proper notifications in the event of a breach or risk paying penalties.

In some cases, companies have been held responsible for paying attorney's fees on behalf of the customer as a result of a security breach. There are also compliance standards such as PCI and NIST that should be implemented by companies of any size to protect sensitive data. While this can seem daunting and expensive, there are also the significant costs associated with damage to your reputation and your brand as a result of poor security practices and a data breach. Perhaps the most daunting impact, however, is the business downtime as a result of a random hacker in to your system or actual money out the door as the from some malicious behavior or phishing scheme.

The good news is that there are cost effective and simple solutions for small and medium sized businesses that ensure companies are taking the right steps to protect their business and their customers.

Upon exploring these solutions, business leaders should consider the following key areas to any security solution for their business:

Prevention Assessment and Plan

The best place to start is an initial security assessment to identify points of exposure and the development of initiatives within your roadmap to prevent these random business continuity events from occurring moving forward.

While this one-time assessment is not full proof, it does examine current vulnerabilities and provide guidance for improving practices and avoiding threats in the future.

Has your company had a comprehensive evaluation of your current security environment including your physical environment, systems, applications, workstations, backup, policies and practices? Any of these areas can present vulnerabilities that subject your business to significant risks. A comprehensive security assessment is the best way to prevent these events from impacting your business and begin to develop a comprehensive security program to best protect your business from unwanted attacks on an ongoing basis. If you engage with a managed service provider, the output of and evaluation can be integrated in to your overall technology roadmap for the business.

ELEVATE

Periodic Audits and Ongoing Management

While an initial assessment and roadmap projects are the best way to uncover any potential vulnerabilities, there is also the need to perform ongoing maintenance and management to avoid potential attacks moving forward. This can be done through periodic audits or an ongoing managed services program that provides ongoing security management including policy support and education and training. Do you perform ongoing audits and management of your systems to ensure everything remains current and up to date including change of passwords, updates to operating systems, antivirus updates, backups, asset management, event monitoring and patch management?

Governance Structure, Policies, Practices Education and Training

While you can protect your physical environment, and systems through an initial assessment and ongoing management, you also are vulnerable to the human element both out of ignorance and malicious intent. Once again, you can make tremendous progress toward prevention against harm to your business through strong governance, policies, practices, and ongoing education and training. With proper governance and a response plan you are in the best position to create a structure to prevent potential attacks or respond accordingly to a malicious attack should it occur. Also, information security (InfoSec) policies and practices such as computer and internet usage policies, password protection, proper onboarding and offboarding procedures and scheduled backups can go a long way to protect your environment on an ongoing basis.

Do you perform ongoing education and training of personnel to ensure policies and practices are being followed on a regular basis? You should have some formal training and education on proper security practices including awareness and tests to potential phishing schemes that could compromise your systems.

Standards Compliance

In addition to internal technology standards, there are several formal standards bodies and practices that should be followed within an industry or when handling customer data including PCI and NIST as well as standards such as the Center for Internet Security and other international standards bodies. Do you comply with industry standards that apply to data use protection, access and privacy?

Putting a proper security program in place has tremendous return on investment as penalties, legal fees and business continuity costs from a single incident could cost tens of thousands to hundreds of thousands od dollars to a company. In addition to these hard costs are the potential costs to your brand and preserving customer relationships as factors that should be considered in any business case associated with security. Having strong governance, policies, practices and training can have a dramatic impact on your customer relationships and brand. Whether your business is strictly interested in a security solution or a fully integrated program within a comprehensive managed services solution, consider all of the factors both systems and human in nature to protect your business from an unnecessary attack.