How to Make Sure Your Business Data Stays Secure

Samantha Higgins

The data your company collects and stores are extremely important. Not only your own but also the personally identifiable information (PII) of your clients. Without the proper security that data is subject to theft and other forms of cyber extortion.

In 2020 alone close to 740 million files were breached across all business sectors. Many of these were related to security gaps that could have been quickly repaired. Instead of following their examples, you need to make sure your business data stays secure. Here are a few tips on how to make that happen.

Conduct a Risk Management Analysis

The first thing to do is conduct a risk management analysis of your technology infrastructure. It can be done in a few ways. When trying to find good-quality healthcare IT security measures consider looking at a third-party organization to help safeguard PII. Companies like Techumen provide this service as well as risk management audits, such as Techumen's HIPPA audit checklist, to ensure all the bases are covered.

The other way to handle this is to gather a team of managers and staff at your business to conduct the analysis. They need to record all potential issues and suggest solutions to mitigate them. The ones that seem the most useful need to be applied and tested. If they don't work, then the next group must be tried. Risk management is a continual task and can't be taken lightly.

Enable A Virtual Private Network

One of the easiest ways for cyber extortionists to pilfer PII and other business data is via remote access. If an employee logs into their work environment from an unsecured location, attackers can piggyback on their link and get into vital areas of a company's network. Avoid this by implementing a Virtual Private Network.

Known as a VPN for short, this method of access creates a secure tunnel that allows employees to access their work files. It does this by hiding their Internet Protocol (IP) address and Domain Name Service (DNS) from those observing the connection. When they link to a VPN, workers look like they've disappeared. In turn, they can work within a company's virtual environment with minimal risk.

Activate Multi-Factor Authentication

Cyber extortionists find quick paths into an organization’s data from a user’s password. Either they’re so simple as to be quickly deciphered or continually reused by someone. By utilizing multi-factor authentication (MFA), companies can shield cyber extortionists from easy access.

The reason is it adds an extra layer to the username/password model. After an employee enters their credentials, MFA requests an additional form of identity. Normally, this is a phone call or a numeric code sent to a person’s smart device. While not 100% secure, this form of authentication has been proven effective. The only way cybercriminals can obtain the code is to have the smart device in their possession.

RAM-Only Servers

Server farms and disk arrays are prime targets for cyber extortionists. They’re filled with terabytes of PII ready for stealing. Nevertheless, this risk can be minimized by switching to a RAM-only server environment.

These devices store data retrieval and use it in a random access memory (RAM) cache instead of a hard drive. When an employee logs out of this form of server, it can be programmed to remove all instances of their footprint from the RAM. Additionally, if this is combined with a VPN, a kill switch can be used to quickly shut down a server when malicious activity is detected.

Move To The Cloud

The Cloud is the best place to store your company’s data. The companies that support your organization’s PII have strict

security protocols enabled. As a result, the risk of cyber extortion is minimized. Furthermore, if Cloud service providers get attacked, they have backups of data to ensure your business continues without a loss of income or productivity.

Yes, the risk of cyber extortion is out there. However, you don’t have to be constantly afraid of it. By implementing one or all of these suggestions into your risk management plan you make sure your business data stays secure. When you do that, your patrons will also feel secure and continue working with you. Overall, this is the best outcome to have in a world of constant cyber attacks.

About the Author: *Samantha Higgins is a professional writer with a passion for research, observation, and innovation. She is nurturing a growing family of twin boys in Portland, Oregon with her husband. She loves kayaking and reading creative non-fiction.*