FrankelZacharia LLC

Certified Public Accountants

The Cybersecurity Roadmap

Effective cybersecurity defense is a journey. Do you have a roadmap for your journey?

The reason that most compliance requirements focus on some type of documented plan is that it is a fundamental way to lower your risk.

HIPAA calls it a "Risk Analysis" and it is the one, clearly stated, universal requirement of the HIPAA security rule. The IRS refers to it as a "Data Security" plan and reminds tax preparers that they are subject to the Safeguards Rule of the Gramm-Leach-Bliley Act, going clear back to 1999 (Did we even HAVE data then?) which requires a regular risk assessment and a plan to improve.

If you are an organization or an associated vendor of an organization which falls into these or similar compliance categories, it is a requirement. If you do it with the right methods and techniques, the act of creating the document keeps you safer.

All cybersecurity assessments have these key elements in common:

Know your assets: You cannot protect something unless you know and understand what it is, where it is, and how it works. The key elements are data and systems, but it goes beyond that into processes and people. If you have not done this before, it can take a long time, but if you perform an asset review on a regular basis it can become a quick and efficient process.

Evaluate the Risks: Once you have a well-documented picture of what you must protect, you need to know what could happen to these assets to cause harm to you, your customers, and your staff. This is where it helps to have a cybersecurity professional involved who is trained to "think like a hacker" and model the threats to your organization.

Evaluate Controls: After you have a thorough inventory and a list of the top ways your assets can be compromised you compare them to your defenses to look for gaps. This could be something technical such as an older firewall which is no longer supported and patched, or perhaps not "technology" at all, but a process involving people and the steps they take to handle sensitive information.

Create a Roadmap: No journey works without a map and in the constantly changing landscape of cybersecurity threats, you are lost without it. If technology were free, you would just get a list of things to implement and check them off the list. Since all technology costs both money and effort, you need to identify the most important areas of improvement for your business and focus on improving them over time.

Cybersecurity and compliance can be a daunting task. Frankel Zacharia Technology Services has experienced security professionals that are available to help navigate your way through the miles of information to create a plan to protect your business from threats over the long term. Call us at 402.963.4375 or schedule a time to visit at https://resultdriventech.com/schedule/.