Understanding Defense in Depth and Cybersecurity Frameworks

Getting Started

When you're starting from scratch, how should you embark upon a Cybersecurity Plan? Understanding the various standards, controls and frameworks of cybersecurity can be confusing and overwhelming. How do they work together? What's best for your organization? Do you have to implement them all?

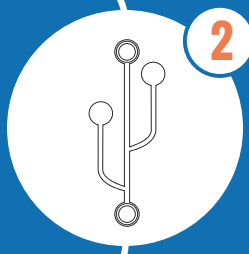
And better yet, where do you even begin?

1 Familiarize yourself with Defense in Depth

This is an overarching strategy or conceptual approach to protecting your organization with the coordinated use of multiple security countermeasures to protect the Confidentiality, Integrity and Availability of your information assets. As each security tool or process you implement will eventually have a vulnerability or risk, it's important to implement layers of security each protecting different attack vectors with minimal overlap.

What it's not: Buy a bunch of security tools and hope it all works.

2 Outline your NIST Cybersecurity Framework



The National Institute of Standards and Technology (NIST) developed "The Cybersecurity Framework" to improve critical infrastructure security and provide a loose set of guidelines to flesh out the Defense in Depth strategy in 5 functional areas: Identify, Protect, Detect, Respond and Recover

What it's not: A simple 5 step process – there's much more than what's outlined here.

3 Implement the top 5 CIS Controls

Now that you have a framework outline, it's time to get practical. A good place to start is The Center for Internet Security's Critical Security Controls for Effective Cyber Defense V 6.1. (more succinctly known as CIS Controls). While there are 20 controls in total, the top 5 controls are considered to be the immediate tactical steps an organization can take to effectively reduce their cyber-attack risk by 85%.

What it's not: A guarantee that you're "in the clear" once you implement

impulse

With these 3 steps, you're off to a great start on your cybersecurity journey!