What is a Framework

What is a framework when discussing Cyber Security? A framework in it's simplicity is where you start. Think of the base of any structure, just like cement is used as the foundation of a building, a framework is the foundation of computer security. More accurately a NIST framework is serves as guidance to help you follow legal regulations for private organizations to help identify, protect, detect, respond, and recover. Everything is organized around frameworks.

Identify. This stage of the five pillars of NIST is your ability to identify problems and the tools at your disposal. In a sense, this is where your Digital Literacy comes in to play (your understanding of technology and how it works). You have to be able to prioritize risks to deal with first based on the business needs. Identify physical and software assets, business environment organization supports, policies, vulnerabilities, risk management, and supply chains.

Protect. After you Have successfully identified a problem, you have to be able to protect against that problem. Put systems in place to perform a preemptive strike. If you can stop something before it even becomes a problem, then you are going to be ahead of the game. Ideally you want to be able to protect Identity management and access controls in the organization, train and empower staff through awareness, establish data security protection, implement protection procedures, protect organization's resources, and manage technologies.

Detect. Even though, you set up strong defenses for protecting all of your assets, you still must be vigilant, anything can slip in through cracks, in a hole, or undetected. This is when it is important to be able to notice these things, detect where anomalies are and can come from. A detect function can help discover cyber security events. Ensure events are detected and potential

is understood, implement continuous security monitoring capabilities, and maintain detection processes.

Respond. Being responsive is an important part of stopping incoming threats. After you detect a threat, it is imperative to know the appropriate way to respond to it. A respond function is meant to support the ability to contain the impact of events. Ensure response planning is executed, manage communications with appropriate individuals, adjust the amount of activities preformed to prevent growth of an incident, put improvements in place.

Recover. Finally, you I have to be able to recover lost or harmed data that was messed with in an attack. Identify appropriate plans, to strengthen and restore any services that were affected from an attack. Ensure your organization puts plans in place for recovery and restore procedures, implement improvements based on what you learned from the attack, review existing strategies, and communicate.