MITRATECH

4 Steps to Greater Cyber Resilience

While there are a variety of tools that deal directly with specific elements of the cyber, regulatory and risk lifecycle, an integrated solution packages multiple processes in an all-in-one platform. The end-to-end integrated functionalities available in Mitratech's GRC platform provide your organization with some powerful capabilities imperative to achieve cyber resilience.

1 Define your cyber controls.

A lack of mature cyber security controls can cause instability in the organizational structure and often leads to significant financial loss. Building cyber security practices that maintain cyber resilience requires that organizations stay up-to-date in their analysis, and a conventional approach makes this challenging.

A *proactive approach* must be taken to implement all relevant controls such as policies, managing user privileges, network security and malware prevention. Organizations should also ensure that formal processes enabling continuous improvements are put in place and enforced.

2 Perform regular cyber risk assessments.

Cyber risk assessments are vital in helping organizations identify any existing gaps or vulnerabilities. These assessments help an organization obtain tangible information about the maturity levels of their cyber security capabilities, assess the level of knowledge and cooperation amongst its own employees, and gain insight into the compliance of their third party suppliers.

Within Mitratech's Alyne platform, the assessment's instant risk results provide teams with measurable and actionable insights dynamically loaded into a risk inventory. From the results, teams analyze the threats, gaps and vulnerabilities of their assets – allowing them to prioritize the highest cyber security risk areas and assist in their incident response planning.

MITRATECH

info@mitratech.com

For more information visit mitratech.com

3 Monitoring and analytics.

Collecting the risk data from within your organization and the likes of third party vendors is just a first step in the cyber risk management process. In order to effectively manage the data results, it needs to be thoroughly analyzed and most importantly, understood.

Analytics plays a big part in quantifying the collected risk data and creating an accurate picture of the risk because it provides the organization with an unprecedented ability to identify, measure and mitigate risk. Continual monitoring of systems is imperative in order to detect potential gaps or weaknesses before they occur.

4 React, recover and review.

In the case of a security breach, you need to respond by implementing your organization's incident response management and business continuity management (BCM) plan to ensure that your business can continue to operate and recover to a normal state as quickly as possible. Alyne's built-in incident management feature allows teams to register, view criticalities and obtain a holistic view of any cyber security incidents, in an all-in-one platform.

Take Action Now

At Mitratech, we believe in simplifying, digitizing and automating cyber security management processes.

Learn more about how we can provide you with some powerful advantages in achieving greater cyber resilience across your organization.