Eigenspace

Cybersecurity Awareness and Resiliency

The concept of Cyber Awareness and Resiliency (CAR) has three specific elements, which must work together to provide a security posture required in the 21st century and beyond. According to Merriam-Webster (2017), CYBER is defined as "relating to, or involving computers or networks (such as the Internet) or within the cyber marketplace." As posited by Merriam-Webster (2017), the Cyber both definitions apply to this concept. Merriam-Webster (2017) defines AWARENESS as "the quality or state of being aware, knowledge and understanding that something is happening or exists." As postulated by Merriam-Webster (2017), both Awareness definitions apply to this concept. Merriam-Webster (2017) defines RESILIENCE as "the capability of a strained body to recover its size and shape after deformation caused especially by compressive stress or an ability to recover from or adjust to misfortune or change." As claimed by Merriam-Webster (2017) the Resilience definitions do not apply to this concept.

MITRE (2017), defines resiliency as "cyber-attacks requires technical, procedural, and policy changes to the infrastructure, architecture, and enterprise operations." CAR modifies the posited Merriam-Webster and the MITRE definitions to declare its definition, which is "the ability to predict, identify, protect, detect, respond, and recover known and unknown attack vectors wherever they may be found." This includes the decision-making process of individual or groups that may affect or compromise security postures for an organization. The CAR ethos requires a litmus test that measures for the effect in the decision-making process by detecting the wittingly, unwittingly, knowing and unknowingly impact for ethical, moral, and legal characteristics for security. Thus, the character of security within the context of cyber reinforces the CAR concept by adherence to the morality in decision-making processes measured by the outcome for accountability and responsibility for a given frame of reference.

The ability to dynamically adjust leadership to adopt to this form of moral conscious will require a new type of Cyber Executive Leader (CEL) and elevates the role of the Chief Information Security Officer (CISO) as a key contributing member of the Board of Directors (BoD) decision-making process (or any Key Decision Maker). The CISO should be supported by a team of subject matter experts, that provide the due diligence of emerging security standards, requirements, and technologies to achieve the primary goal of the CAR, which is to ensure moral, ethical and legal cybersecurity decisions as a factor of honest authority and legal awareness. The CISO's team should be independent to operational business decision-making processes and have an isolated budget that supports, defends and protects the security posture required in the data concentric 21st century and beyond. The CAR provides a conceptual idea needed in the ever-changing world of cybersecurity that now includes the evidentiary requirements of transparency, accountability and responsibility for the protection of data provided by the customers, clients and employees for today and the future.

Cybersecurity Awareness and Resiliency

Reference(s)

Merriam-Webster (2017). Definition of AWARENESS. Retrieved from https://www.merriam-webster.com/dictionary/awareness

Merriam-Webster (2017). Definition of CYBER. Retrieved from https://www.merriam-webster.com/dictionary/cyber.

Merriam-Webster (2017). Definition of RESILENCE. Retrieved from https://www.merriam-webster.com/dictionary/resilience

MITRE (2017). Security breaches are inevitable; IT infrastructures must operate anyway. Retrieved from https://www.mitre.org/capabilities/cybersecurity/resiliency

Questions?

For Additional Information Contact:

For Additional Information Contact:

Eigenspace
312 Main Street, Suite 300
Gaithersburg, MD 20878
240-654-4097
www.eigenspace.us