Harrison Goldmintz

WRT 205

Dr. Geyer

17 April 2024

Blog Post - Strengthening Cybersecurity Together

Blog Website: thecyberwire.com

As many of us have seen in this modern world, there is an increased importance for cybersecurity in today's digital age. This increased need for comprehensive cybersecurity measures to protect individuals, organizations, and nations from cyber attacks has never been more significant than it is today. We must address this before individuals and organizations are taken advantage of. We must encourage and present to our policymakers to support allocating resources and creating legislation that prioritizes cybersecurity as a national security imperative. We must encourage leaders in corporations to invest in cybersecurity infrastructure and advocate for the adoption of safe practices to protect our sensitive data. And to the general public, we must make awareness of online safety practices, while encouraging the use of strong passwords and two-factor authentication.

We have seen on the news lately many disruptive and deadly attacks against individuals, corporations, and governments. Whether it was a ransomware attack, a data breach, a phishing scam, an attack on the supply chain, or even an attack on a local or large-scale government, many people are at risk. It's not only about the money that needs to be spent to scare off or repair the damages of an attack, these attacks have become deadly, taking large amounts of human lives, more than ever before.

Recent executive orders and proposed regulations have changed the definition of covered entities in a new cybersecurity landscape. The new version of covered entities has included various types of organizations, such as government agencies and critical infrastructure providers (i.e.: energy, healthcare, and finance). This also includes private corporations as everyone can be a victim of a cyber attack. This aims to ensure cybersecurity cybersecurity coverage across all sectors and industries.

In addition, these orders and regulations have brought up a new subject of mandatory reporting in the event of a cyber attack. These new obligations are for all various cyber attacks and threats in a timely and accurate way, in the hope of mitigating the impact of cyber threats. All reports must be submitted to the National Security Agency to be investigated, depending on the severity of the incident.

Failure to meet these obligations of implementing cybersecurity measures can result in financial penalties, legal action, and reputational damage. Covered entities need to prioritize cybersecurity compliance as a part of their risk assessment and risk management strategies. With the adaptation of good cybersecurity practices, organizations can mitigate liability risks and enhance their cybersecurity posture.

As a result, we must prioritize cybersecurity in policymaking for national security. We must demand and support the investment in the best cybersecurity infrastructure and training. We must support and educate the public about safe practices in cyberspace by using strong passwords and staying informed. Result, we must work together with policymakers, businesses, and individuals to create safer digital work for everyone.