ETHISPHERE
GOOD. SMART. BUSINESS. PROFIT.
6991 E. Camelback Rd. Ste. B-350
Scottsdale, AZ 85251
p: 888.229.3207

January 2018

The Cybersecurity Essentials Assessment

Microsoft TechSpark

The Microsoft TechSpark program has deployed the services of Ethisphere to work with companies in its geographic areas of focus so that they can benefit from resources to help organizations measure their cyber risk management capabilities. The Ethisphere Institute defines and advances business practices in high risk areas that fuel corporate character, marketplace trust, and business success. We have deep expertise in defining, measuring and implementing effective controls using data-driven insights. Companies in the TechSpark regions can access the Cybersecurity Essentials Assessment to measure the maturity of their cybersecurity approach.

Background

To protect against growing cyber threats, companies are implementing an array of cybersecurity measures. The most effective approach involves addressing 'people, processes and technology.' Organizations are making important changes to improve cybersecurity – from training employees about common threats such as not clicking on links in emails to implementing controls recommended in the cybersecurity framework launched by the U.S. National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework is based on broader enterprise risk management techniques and is becoming the *de facto* approach for cybersecurity among global enterprises and offers valuable recommendations for smaller organizations.

The Service

The Cybersecurity Essentials Assessment is a service designed to measure the maturity of an organization's cybersecurity approach. It is based on leading cybersecurity practices outlined by the U.S. National Institute of Standards and Technology (NIST) with input from information security experts and senior cybersecurity leaders from companies around the world. The assessment aligns to key controls in the NIST Cybersecurity Framework first issued in 2014 and broadly deployed by organizations in the U.S. and around the world. The Framework incorporates and references leading standards and guidance, including ISO 27001, and NIST 800-53 and 800-171, among others.

The Cybersecurity Essentials service is based on 25 of the 98 subcategories or controls in the NIST Cybersecurity Framework. By measuring an organization's maturity in implementing these controls, an organization can better manage its cyber risk and understand what areas to focus on improving its cybersecurity.

The tool includes an **Online Self-Assessment** providing insights into the processes and practices currently in place and benchmarked against these foundational 25 controls in the NIST Cybersecurity Framework. You will receive a **Summary Report** of your results.

Why should my organization take the Cybersecurity Essentials Assessment?

Cyber attacks can put companies at financial, reputational and legal risk. The *Cybersecurity Essentials service* helps your organization mitigate these risks by assessing current systems in place to prevent data breaches, and identifying areas where improvement is needed. An organization that develops an effective cybersecurity program can avoid costly litigation, penalties, and reputational harm, while enhancing its position as an organization that places the protection of its sensitive and private information as a top priority, differentiating itself from competitors, making the organization more attractive to investors, business partners, potential employees, and customers alike.