C3 VOLUNTARY PROGRAM

Cybersecurity for Startups

About the C³ Voluntary Program

The C³ Voluntary Program is a public-private partnership led by DHS to help align critical infrastructure owners and operators with existing resources to assist the use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

The C³ Voluntary Program aims to support startups in establishing cyber resilience, increasing awareness and use of the Cybersecurity Framework, and managing cybersecurity as part of an all hazards approach to enterprise risk management.

Why Should Startups Address Cybersecurity?

Startups comprise a large part of the Nation's intellectual capital and business growth. These companies face unique financial and personnel constraints and as a result, cybersecurity may become a lower priority. Unfortunately, all it takes is one attack or security breach to destroy a startup's reputation before it has even been established in the marketplace. Although many information technology (IT) services can be outsourced, startups cannot survive the risk associated with improper cybersecurity planning. Security does not have to be expensive, but it does require effort.

Where to Start

First, startups should consider how they address risk. Is there a structured way that risk is managed within the startup? The NIST Cybersecurity Framework provides a common language for understanding, managing, and expressing cyber risk.

Second, startups should identify and track cyber connected devices and software within their company. Does the company assign value to business critical information? Is the information protected to the right level? Is your company utilizing cloud-based services? If yes, what information assurance agreements do you have in place? Without this asset tracking, access control and configuration management policies are ineffective.

Third, review IT or security service agreements to ensure event detection and response actions meet the company's risk threshold and needs. Do you have an agreement in place for incident response?

Fourth, ensure the company has a recovery plan to restore critical business functions if there is a cyber event. How do you collect revenue if your payment system is compromised?

Lastly, consider building or joining resilient communities, comprised of organizations that share a regional and/or industry identity to support one another and share information related to strengthening their cybersecurity resilience.

For all of these steps, tips, resources, and information can be found on the C³ Voluntary Program website:

https://www.us-cert.gov/ccubedvp