Cybersecurity Risk Management Implementation Assistance for Small Communications Operators

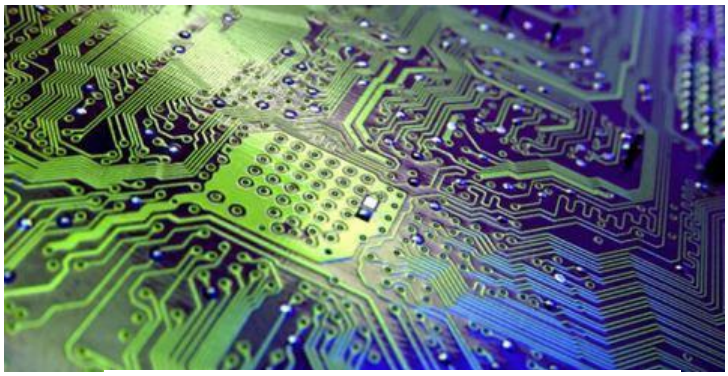
The Challenge

There are more than 1,000 independent telecommunications operating companies providing services mostly in high-cost, sparsely populated markets. Due to the high costs and sparse populations of the areas they serve, independent carriers typically have relatively few employees to cover a large geographic area, and lack economies of scale and scope.

The Communications Sector Coordinating Council (CSCC) has recognized that small communications companies inherently have limited financial, human, technical information and other resources. As such, small telecom providers face unique and disproportionate challenges associated with using the complex NIST Cybersecurity Framework, and developing and maintaining comprehensive cybersecurity risk management programs that address their unique circumstances.

Project Overview

This project will help managers and key employees at small telecommunications providers be better versed in how to identify and mitigate cyber risks, as well as recover from and respond to cyber incidents when they occur. Instructional and assistive materials will help small providers evaluate their current program and respond accordingly. Those who attend the half-day educational sessions that are planned will leave with a basic understanding of cyber risk assessment and management tactics specific to the operations and needs of small telecommunications providers. Surveys will be utilized to assess the effectiveness of the training sessions and the progression of knowledge. Participants in the Cyber Risk Manager Recognition Program will have the tools necessary to create a culture of awareness and risk mitigation within their individual companies.



Computer Circuit Board (Source: DHS)

Next Steps

As this project moves forward, it will demonstrate how small communications carriers with limited resources can enhance their cybersecurity posture and contribute to the protection of the Nation's critical infrastructure through the adoption of a risk-management approach, organization-wide use of best practices including leveraging of the NIST Framework, and developing and sustaining a culture of internal security awareness throughout their companies.

To learn more about this program, contact
Jay Robinson, DHS Program Manager, at jay.robinson@hq.dhs.gov or
Ewell Balltrip, CEO, NIHS at eballtrip@thenihs.org 2018-06.1pager