Cyber Risk Management Tools for Nonprofits

Project Objective

Nonprofits lack research- and data-driven cyber risk management tools to help them make good cybersecurity investments. A solution exists for commercial organizations, but these solutions need to be updated with research, analysis, and models that are unique to nonprofits. Re-launching and widely distributing existing cyber risk management tools with underlying research, analysis, and models will fill an important gap.

The specific need that this project will fill is the need for cyber risk management tools to help nonprofit executives address cyber risk at the top of the organization. The proposed tools are cost effective, user-friendly, and suitable for immediate use by nonprofit executives that need to participate in establishing cyber risk management as part of their operational culture. The follow-on effect is that government and private organizations in critical infrastructure sectors will benefit from the enhanced security of the nonprofits that are part of their supply chain.

Project Overview

The objective is to make basic cyber risk management resources available to resource constrained nonprofits that reflect the subtle, but important, differences that define their cyber risk. One facet of the problem is that the tools' underlying data change rapidly and must be maintained over time. Hosted, online tools are necessary to ensure nonprofit end users are always using the latest underlying data. Likewise, the education strategy will need revision over time to keep pace with new versions of the NIST Cybersecurity Framework. Therefore, an important part of the mission is to find a self-sustaining economic model that pays for the ongoing costs. In short, this project is the very essence of public/private partnerships.

Cyber Agents Working on Computers (Source: FBI)

Next Steps

The outcome will be an increased adoption rate of the NIST Cybersecurity Framework by providing specific guidance, and basic cyber risk management tools, to operationally lean nonprofits. This will also greatly improve the posture of critical infrastructure sector participants that count nonprofits as part of their supply chain. The transition-to-use plan will demonstrate the ability of the private sector, government, and academia to come together to make progress toward solving a large, complex problem. The primary objective is to reduce the inherent risk nonprofits face and the risk of there becoming a backdoor for attackers to impact the critical infrastructure of our society.

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