Please Note: Cybersecurity is a rapidly evolving field. This document was last updated on February 2, 2019. Some of the technical guidance within this document may change, and some of the risks defined may increase or decrease in their potential likelihood or impact.

An introductory webinar to this guide including information about it's contents and how to use it, can be seen here: https://www.techsoup.org/community/events-webinars/cybersecurity-in-low-risk-organizations-understanding-your-risk-2019-02-19

Introduction

This guide is intended as an introductory document for low-risk organizations interested in improving their cybersecurity practices, ***specifically nonprofits and public interest organizations at low risk of targeted cyberattacks.*** By "targeted cyberattacks," this guide refers to attacks on systems that seek to disrupt or surveil a specific organization or individual (as opposed to attacks meant to compromise as many devices or accounts as possible). This document provides guidance to improve the resilience of low-risk organizations (LROs) to common cyberattacks, and a framework for LROs to develop a basic cybersecurity policy. It is worth noting that all organizations are at some risk of cybersecurity incidents. Though not all organizations are equally likely to be victimized by online attacks, there are basic steps that LROs can take to improve their resiliency and keep themselves at lower risk—even while recognizing the limits to their potential investments of time, people, and money.

This is not intended to be a comprehensive guide to cybersecurity, nor an exhaustive set of recommendations. This guide is intended to help individuals in leadership positions and technical staff with little or no cybersecurity background understand some of the fundamentals of their own security context and guide them toward initial steps for improving their cybersecurity. The audience for this guide could include executive staff, system administrators, financial officers, general counsels, non-profit board members, or anyone interested in elevating their organizations' appreciation of cybersecurity issues.

This guide has three primary sections: the first introduces basic cybersecurity concepts, including the fundamentals of cybersecurity risk management; the second describes a series of basic cybersecurity "controls" – or measures organizations can take to improve their resilience to cybersecurity threats; the third describes additional cybersecurity best practices and policies LROs should adopt. Appendix A is designed to help organizations draft a basic cybersecurity policy using the controls and best practices described in this guide. Appendix B provides guidance on how to implement selected cybersecurity controls. Appendix C describes a series of additional resources for organizations interested in moving toward a more sophisticated cybersecurity posture.