You already recognize that cybersecurity is critical to small and midsize businesses (SMB). **But where do you go from here?** This list of top resources will help guide your business toward stronger cybersecurity and risk management practices.

1. C³ Voluntary Program SMB Toolkit

This packet contains resources specially designed to help SMBs recognize and address their cybersecurity risks. Resources include talking points for business managers and leadership, steps to start evaluating your cybersecurity program, and a list of hands-on resources available to SMB.

2. Cybersecurity for Startups

This one-page overview provides information on how startups can begin to grow their cyber resiliency efforts in tandem with their business to maintain consumer trust and company longevity. Included is an overview of why cybersecurity is important consideration for startups and five steps startups should take to begin increasing their cyber resilience.

3. Stop.Think.Connect. Resource Guide

The Stop.Think.Connect.™ campaign has an online Resource Guide specific to SMBs. The guide contains information from SMBs on mobile safety information, cybersecurity guidance for employees, and a small business tip card, among many other resources. The Resource Guide for Small Business can be found here: http://www.stcguide.com/explore/small-business/

4. Small Business Administration (SBA) Training

This 30 minute, self-paced training exercise provides an introduction to securing information in small businesses. More information and the training can be found here: https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses.

5. Federal Small Biz Cyber Planner

This tool helps businesses create custom cybersecurity plans. The Small Biz Cyber Planner includes information on cyber insurance, advanced spyware, and how to install protective software. More information can be found here: http://www.fcc.gov/cyberplanner.

6. Internet Essentials for Business 2.0

This guide for business owners, managers, and employees focuses on identifying common online risks, best practices for securing networks and information, and what to do when a cyber incident occurs. More information about this guide can be found here: https://www.uschamber.com/internet-security-essentials-business-20.

7. NACD Cyber-Risk Oversight Handbook

The National Association of Corporate Directors (NACD), in conjunction with AIG and the Internet Security Alliance, has identified five steps all leadership and management teams should consider as they seek to enhance their oversight of cyber risks. The NACD Cyber-Risk Oversight Handbook can be found here: http://www.nacdonline.org/cyber.