NIST Helps Small Businesses Improve Cybersecurity

written by Lauri Moon | December 7, 2016

NIST provides guidance to help small businesses secure their data and information in the new publication.

(NIST – Evelyn Brown: 11-10-16) Small-business owners may think that they are too small to be victims of cyber hackers, but Pat Toth knows otherwise. Toth leads outreach efforts to small businesses on cybersecurity at the National Institute of Standards and Technology (NIST) and understands the challenges these businesses face in protecting their data and systems.

“Businesses of all sizes face potential risks when operating online and therefore need to consider their cybersecurity,” she said. “Small businesses may even be seen as easy targets to get into bigger businesses through the supply chain or payment portals.”

Toth is the lead author of NIST’s *Small Business Information Security: The Fundamentals (link is external)*. The guide is written for small-business owners not experienced in cybersecurity and explains basic steps they can take to better protect their information systems.

“Many small businesses think that cybersecurity is too expensive or difficult; *Small Business Information Security* is designed for them,” Toth said. “In fact, they may have more to lose than a larger organization because cybersecurity events can be costly and threaten their survival.” In fact, the National Cyber Security Alliance found that 60 percent of small companies close down (link is external) within the six months following a cyberattack.

The new NIST publication walks users through a simple risk assessment to understand their vulnerabilities. Worksheets help them to identify the information they store and use, determine its value, and evaluate the risk to the business and customers if its confidentiality, integrity or availability were compromised.

The guide is based on NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, which was issued in 2014 as part of efforts to protect the nation's critical infrastructure. The framework's processes and tools provide key standards and best practices developed over decades by the federal government and industry. Its simple language allows organizations to better communicate, and its overall design helps them identify, assess and manage cybersecurity risks.

For example, the new guide describes how to:

- limit employee access to data and information;
- train employees about information security;
- create policy and procedures for information security;
- encrypt data;
- install web and email filters; and
- patch, or update, operating systems and applications.

Other recommendations may require new equipment, and the guide can help businesses perform cost/benefit analyses. "We recommend backing up data through a cloud-service provider or a removable hard drive and keeping the backup away from your office, so if there is a fire, your data will be safe," Toth said. And a backup can be used to restore data in case a computer breaks or malware infects a system.

The guide also suggests:

- installing surge protectors and uninterruptible power supplies to allow employees to continue to work through power outages and to save data;
- considering the purchase of cybersecurity insurance; and
- ways to find reputable cybersecurity contractors.

NIST has been in the business of helping small businesses with information security since 2001 when it joined forces with the U.S. Small Business Administration (link is external) and the Federal Bureau of Investigation's InfraGard (link is external) program to provide introductory cybersecurity workshops to small businesses.