October is Cybersecurity Awareness Month – It's a Good Time for a Security Checkup

By David G. Ries / Oct 13, 2020

This month is the 17th Annual National Cybersecurity Awareness Month in the United States. This year's theme is "Do Your Part. #BeCyberSmart." For businesses and organizations that have established cybersecurity programs, it's a good time to review and update them. For those that do not, it's a good time to start the process and follow through to implement a comprehensive cybersecurity program.

Cybersecurity is a process to protect the confidentiality, integrity, and availability of information. Comprehensive security should address people, policies and procedures, and technology. While technology is a critical component of effective security, the other aspects also are critical and should be addressed.

Cybersecurity is best viewed as a part of the information governance process, which manages documents and data from creation to final disposition. Managing and minimizing data is an essential part of information governance, including security, privacy, and records and information management.

Security starts with an inventory of information assets and data to determine what needs to be protected and then a risk assessment to identify anticipated threats to the assets and data. The next steps are development, implementation, and maintenance of a comprehensive cybersecurity program to employ reasonable physical, administrative, and technical safeguards to protect against identified risks. A cybersecurity program should cover the core security functions: identify, protect, detect, respond, and recover. Programs covering these elements are frequently required by laws, regulations, and contracts for covered industries, protected information, or both.

Comprehensive cybersecurity programs are often based on standards and frameworks like the National Institute for Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, (April 2018), more comprehensive standards, including NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations (September 2020) and standards referenced in it, and the International Organization for Standardization's (ISO), ISO/IEC 27000 family of standards, (consensus international standards for comprehensive Information Security Management Systems (ISMS)).

These standards can be a challenge for small and mid-size businesses. The Federal Trade Commission (FTC) maintains a website, Cybersecurity for Small Business, which includes links to a number of security resources that are tailored to small businesses. This website is a joint project of the FTC, NIST, the U.S. Small Business Administration, and the U.S. Department of Homeland Security. NIST also maintains a Small Business Cybersecurity Corner website.

Businesses and organizations with cybersecurity programs should periodically review, evaluate, and update their programs. The review and evaluation should address areas like new or changed hardware, software and business processes, changes in personnel or job functions, supply chain changes, lessons from any security incidents, and updated threat information. Those without programs should assign responsibility and adopt a plan and schedule for developing and implementing one.

Training is a critical part of a cybersecurity program. The goal should be to promote constant security awareness, by every user, every day, every time technology is utilized. This Cybersecurity Awareness Month is a good time for a refresher, followed by periodic repetition.

If you have questions about the content of this alert, please contact David Ries (dries@clarkhill.com; 412.394.7787), Lara Forde (lforde@clarkhill.com; 713.374.5743), or another member of Clark Hill's Cybersecurity, Data Protection, and Privacy Group.

 |