BURR ALERT 2018

Cybersecurity Best Practices Based on NIST Cybersecurity Standards and FTC Enforcement Actions

By Elizabeth Shirley March 2018

The National Institute of Standards and Technology ("NIST"), an agency within the U.S. Department of Commerce, has produced a number of detailed standards for various aspects of information security. These standards outline baseline information security controls and represent best practices that assist organizations in identifying, protecting, responding to, and recovering from cybersecurity risks. Additionally, the Federal Trade Commission ("FTC") has posted complaints, consent agreements, public statements, and business guidance brochures to provide guidance to companies about the FTC's standards for reasonable and appropriate data security practices, in relation to the FTC's Section 5 power to prohibit "unfair or deceptive acts or practices in or affecting commerce."

Taking the NIST's standards and the FTC's posted enforcement actions together, the following guidelines are some cybersecurity best practices:

1) **Security.** Start with Security. Don't collect personal information that you don't need. Hold on to information only as long as you have a legitimate business need. Don't use personal information when it's not necessary. Make sure your service providers implement reasonable security measures. Insist that appropriate security standards are part of your contracts, and verify compliance, including through cybersecurity audits of third-party providers.

   Update and patch third-party software. Act on credible security warnings, and move quickly to fix them. Securely store sensitive files, e.g., do not keep them in an open and easily accessible area. Protect devices that process personal information, e.g., securing PIN entry devices that may be vulnerable to tampering and theft. Dispose of sensitive data securely. If it is paper, shred it. If it is electronic information, make sure the documents are deleted to the point that they are unreadable and unable to be reconstructed.

2) **Identify.** Develop an organizational understanding to manage cybersecurity risks to systems, assets, data, and capabilities. This includes understanding the organization's computer systems and network; the personal information it collects; potential vulnerabilities of the organization's systems; and the degree of harm that customers may suffer by disclosure of their personal information. By understanding and weighing these risks, an organization can focus and prioritize its cybersecurity efforts in relation to risk management strategy and business requirements.

3) **Protect.** Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. This includes providing training to employees regarding cybersecurity risks and protection; limiting access to systems, data, and assets; using technology to secure

data; and maintaining cybersecurity policies and procedures. Control access to data sensibly, and restrict access to sensitive data. Limit administrative access to non-public information. Require secure passwords and authentication, and insist on complex and unique passwords. This will help guard against brute force attacks. Store passwords securely, e.g., not in plain text in personal email accounts.

Store sensitive personal information securely, and protect it during transmission. Use strong cryptography to secure confidential material during storage and transmission, for example, Transport Layer Security/Secure Sockets Layer (TLS/SSL) encryption, data-at-rest encryption, or an iterative cryptographic hash. Keep sensitive information secure throughout its lifecycle, including when it is at rest.

Segment your network. You can help protect particularly sensitive data by housing it in a separate secure place on the company's network, as not every computer in a company's system needs to be able to communicate with every other one. Secure remote access to your network. Make sure your company has firewalls and updated antivirus software. Don't turn off SSL certificate validation in mobile apps.

4) **Detect.** Develop and implement the appropriate activities to identify when a cybersecurity event occurred. This includes the monitoring of information systems frequently and testing processes to detect irregular activity. Use industry-tested and accepted methods for cybersecurity.

   Use an intrusion detection system, and monitor system logs for suspicious activity. Assess whether your web application is vulnerable to Structured Query Language ("SQL") injection attacks.

5) **Respond.** Develop and implement the appropriate activities to take regarding a detected cybersecurity event. This includes executing the organization's processes and procedures concerning a response; coordinating and communicating with internal and external stakeholders regarding the cybersecurity incident, as well as applicable law enforcement authorities; controlling and mitigating the cybersecurity incident in an adequate response time; and revisiting the organization's processes and procedures to incorporate lessons learned from the cybersecurity incident. Review the law of each state in which your company does business and in which it has customers, as you will need to comply with each state's various cybersecurity notification laws.

6) **Recover.** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were affected due to the cybersecurity incident. The goal is to help an organization timely recover to normal operations and to minimize the impact of the cybersecurity incident on the organization's internal and external stakeholders.

To discuss further, please contact:

Elizabeth B. Shirley in Birmingham at bshirley@burr.com or (205) 458-5186
or the Burr & Forman attorney with whom you regularly work.