NIST Publishes Guide to Secure an Organization’s Mobile Devices

Tuesday, March 19, 2019

Just last month, the National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), published guidance for public and private companies to protect mobile devices and help prevent data breaches. The publication, titled “Mobile Device Security: Cloud and Hybrid Build,” is a how to guide for companies to secure mobile devices using commercially available technology. Through collaboration with technology organizations, government agencies, and academic institutes, the publication essentially acts as a practice guide for network architects to ensure employees can access information remotely, while minimizing security risks. It presents a variety of security solutions that can be tailored to a company’s needs and includes instructions for installing security products that meet the NIST’s standards. As stated by the NCCoE, the guide “demonstrates how commercially available technologies can meet your organization’s needs to secure sensitive enterprise data accessed by and/or stored on employees’ mobile devices.”

Companies that permit their employees to use mobile devices benefit from ease of communication and the convenience of allowing data to be accessed practically anywhere. However, security controls have not kept pace with the risks inherent in using mobile devices. As a result, a poorly secured mobile device may present significant security risks to a company.

Stolen or infiltrated mobile devices can be a gateway for wrongdoers to access a company’s sensitive and confidential information, email accounts, contacts, calendars, and other proprietary information. Even worse, a wrongdoer could gain remote access and hold a company’s data and information hostage, a tactic that has gained popularity in recent years. Moreover, not only is a company at risk of having its data compromised, but mobile device security breaches have resulted in significant financial penalties. See HIPAA Enforcement Actions.

With many states recently enacting or proposing consumer privacy and security legislation, companies must be mindful of the security risks presented by using mobile devices and ensure the devices are adequately protected. Moreover, companies must have an effective “Bring Your Own Device” (BYOD) policy in place concerning the use of the device, in addition to the security controls on the device. Be on the lookout for our article on the cost – benefit analysis of implementing a BYOD policy, coming later this week.

Jackson Lewis P.C. © 2019

Source URL: https://www.natlawreview.com/article/nist-publishes-guide-to-secure-organization-s-mobile-devices