Guilmartin, DiPiro & Sokolowski, LLC is an independent member of BDO Alliance USA. We are proud to share important information with our clients.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA

MANAGING YOUR RISK DURING THE COVID-19 CRISIS

The novel coronavirus (COVID-19) pandemic has companies searching for alternative ways to conduct business. In light of CDC recommendations to practice social distancing, organizations are relying heavily on online conferencing platforms and telecommuting to sustain operations and support their customers.

Implementation of these solutions is fairly simple. Even companies with limited resources can implement a "Bring Your Own Device" (BYOD) Policy and eliminate the need to purchase new equipment. However, businesses need to address the security risks associated with adding employees' personal devices to their IT infrastructure.

Personal devices may be infected or compromised and could bypass security controls and/or disable security counter-measures. Additionally, allowing employees or contractors to save company data on personal devices relinquishes data control/protections. Finally, teleconferencing increases opportunities for bad actors to intercept/eavesdrop on poorly configured computer systems and software applications. Although these risks exist, they can be mitigated by implementing cybersecurity counter-measure's like Virtual Private Network (VPN) and Mobile Device Management (MDM) solutions.

A VPN solution establishes an encrypted communication channel between off-premise devices (e.g., laptop, tablet, mobile phone, etc.) and the corporate network. This is critical when employees are connecting to the corporate network from open or unsecured wireless networks. Using a VPN, employees can securely connect to digital resources and can prevent disclosure of private information.

MDM solutions provide companies with several ways to mitigate potential threats associated with use of personal devices to connect to corporate networks. These solutions include several features, including:

- Device compliance to ensure devices adhere to corporate policies related to:
  - Anti-Virus
  - Malware protection
  - System and software patches

- Device management to enforce security on personal device, including:
  - Password management
  - Device authentication
- Data Protection features that:
  - Enforce data storage restrictions
  - Allow remote data wiping to ensure data is not stored on personal devices
  - Applies encryption to company data

Implementation of these types of solutions allows companies to address risk associated with BYOD policies without sacrificing security.