Issued 5/3/18

A Well-trained Staff may be your Best Defense against IoT Cyberattacks

According to Symantec's 2018 Internet Security Threat Report, the total number of Internet of Things (IoT) attacks grew 600% between 2016 and 2017. Increasingly, criminals are using these attacks to install malicious cryptocurrency mining applications on computers and IoT devices. Detection of this niche form of cybersecurity attack increased 8,500% in the fourth quarter of 2017 alone. In many respects, the current cryptocurrency craze is a modern reboot of the Gold Rush era some 150 years ago. The lure of a making a quick fortune by stealing CPU cycles from unsuspecting enterprises is driving cyberattacks and threatening security for organizations everywhere. Traditional security training emphasizes programs and protocols like proper credentials, authorized access, and approved devices. With the widespread adoption of IoT, employees at all levels of the enterprise must now be made aware of an additional set of security vulnerabilities. Devices once considered the domain of the IT department and only the IT department should now be considered part of every employee's security responsibility. This is a major change in focus for most enterprise personnel and is going to require significant changes to training. Any meaningful enterprise-level security awareness and training program must explain where caution must be exercised, identify the appropriate security policies and procedures, and lay out the consequences that can and will occur if the policies are not complied with in full. The only way to make every member of an organization truly accountable for cybersecurity is by creating a well-informed and well-trained workforce.