CONTRIBUTED CONTENT & PRESENTATIONS

Alison Evans publishes article in TerraLex Beacon Alert Regarding WannaCry Ransomware Attacks

MAY 30, 2017

Authors: Alison K. Evans

Arguably the most critical short term action a company should take to protect itself against the WannaCry attack and other similar ransomware attacks is to promptly install critical security patches made available by software vendors. The WannaCry attack targeted systems that had not been updated with a security patch that Microsoft made available nearly two months prior to the attack; if the victims had installed the patch, they likely would have avoided becoming victims altogether. To avoid becoming victimized by a future ransomware attack, companies should aim to employ robust data protection regimes within their organizations that call for frequent and regular data backups, disconnection of data backups from the rest of the company's network, installation of an up-to-date antivirus solution and intrusion prevention software, routine penetration testing, and training of the company's work force on how to avoid falling victim to ransomware attacks and other cybersecurity threats.