COSMOS
Navigate the Compliance Universe

CEP Magazine - May 2022
Boost ransomware risk management with the NIST cybersecurity framework

By Michael P. Barry


Michael P. Barry

Michael P. Barry (mbarry@connexionpoint.com) is Director of Compliance & Corporate Counsel for Connexion Point in Sandy, Utah, USA.

In May 2021, Colonial Pipeline was hit by a cyberattack that affected its gasoline, jet fuel, and home heating oil pipeline to the East Coast. The attack affected Colonial Pipeline's computerized equipment that managed its systems and effectively shut the pipeline down for several days. The hackers demanded that Colonial Pipeline pay a $4.4 million "ransom" to have its operations restored. Colonial Pipeline paid the amount to the hackers, who then sent Colonial a software application, in the form of a decryption key, to restore its network. (Note that the U.S. Federal Bureau of Investigation does not encourage paying ransom in response to a ransomware attack, as payment doesn't guarantee retrieval of the stolen data, and it encourages perpetrators to target more victims). Because the cyberattack involved critical infrastructure, President Biden declared the Colonial Pipeline cyberattack as a national security threat.[1]

This ransomware attack was not unique to Colonial Pipeline. Ransomware is a type of malicious software (or "malware") that encrypts an organization's data and demands payment as a condition of restoring access to that data. Sometimes ransomware may also steal a company's information and demand an additional payment in return for not disclosing the data to authorities, the public, or competitors. Hospitals and healthcare organizations in particular face a growing threat from cyberattacks and ransomware. According to a 2020 survey of IT professionals, 1 in 3 healthcare organizations reported being hit by ransomware that year.[2] And *HealthITSecurity*, a trade publication, recently reported that since November 2020, the sector has experienced a 45% surge in the frequency of cyberattacks.[3]

In 2021 the National Institute of Standards and Technology (NIST) issued an initial draft of its *Cybersecurity Framework Profile for Ransomware Risk Management*.[4] NIST issued the framework "as a guide to managing the risk of ransomware events," and to help gauge "an organization's level of readiness to mitigate ransomware threats and to react to the potential impact of events."[5] This framework will assist any organization in developing the best posture when hackers attempt to hijack a company's computer infrastructure.