## CYBER SCENARIO I: Cryptolocker Holds Firm's Data Ransom

A mid-sized corporate law firm that provides M&A consultation to several aerospace engineering firms had its network breached via an email phishing scheme. An unsuspecting legal assistant opened an attachment to an email that contained the "CryptoLocker" virus.

The malware virus encrypted sensitive client files on the firms' servers and the firm was notified that the files will remain locked and will be deleted unless a ransom was paid.

The firm's attorney and insurance carrier engaged their IT forensics vendor and determined that the threat was real and the best course of action was to pay the ransom, and to then assess further exposure and/or loss.

The ransom, IT forensic costs, and legal expenses were covered by the firm's cyber liability insurance policy.

## CYBER SCENARIO II: Attorney's Lost Laptop

A senior attorney at a large law firm brought his work laptop on vacation. The laptop was left on the airplane. The attorney reported the loss to his firm, noting that many files of the class-action case he was working on were on the laptop and were unencrypted.

The case files contained names, social security numbers, addresses, and private health information, as the case involved a regional hospital's emergency room procedures. Due to the sensitive nature of the data, several state and federal agencies were notified of the breach. The firm was required to notify the patients that their personal information may have been exposed.

The firm's costs for breach notification, IT forensics, PR services, and legal fees are covered by their cyber liability insurance. In addition, fines and penalties expected from the Office of Civil Rights for HIPAA violations will be covered.