WannaCry Ransomware Attacks Put Organizations on Alert

By Kristi Fahy, RHIA

A chord of fear has been struck in many organizations—both healthcare and others—after the ransomware attacks that occurred last week that infected more than 200,000 computers across 150 different countries. The ransomware attacks known as "WannaCry" have left many organizations questioning their level of IT security and their system vulnerabilities. According to *Reuters*, the hackers used a tool that the US National Security Agency (NSA) had built. This tool was leaked online in April 2017 and the outcome was significant.

Reuters also stated that the affected organizations received requests from the attackers that they must pay at least $300 in bitcoin, a cryptocurrency that is being used more and more by hackers to make and obtain digital payments online, in order to unlock their infected information.

Organizations were forced to pay the ransom in order to regain access to their sensitive data and information that was critical to business operations. Many healthcare organizations were specifically targeted because of this. Patient care is compromised when providers don't have full access to a patient's clinical record. And consequently, a lack of patient information can lead to poor patient care outcomes. The patient records that were being held hostage left healthcare organizations with no other choice but to pay the ransom.

Although the attacks are in the rearview mirror, IT departments worldwide have their work cut out for them on the road ahead. Sadly, leaked national security information is a vulnerability that organizations must be prepared for in the future. It is important that these IT departments stay current on the latest IT updates and system upgrades. Organization leaders and IT departments will need to assess their current IT capabilities and architectures, and fast. What are the vulnerabilities that these IT systems possess? How can they be addressed? In the event of an attack, can the IT software systems contain the threat? Can the files be restored from backup systems? What is the level of staff awareness on these initiatives? These are questions that need to be asked to ensure effective IT security is in place.

It is events like these that prove that proactive approaches are much more effective than reactive approaches. IT investments can be costly, but the cost of corruption can be so much more… especially in healthcare. Implementing a more proactive IT infrastructure can reduce the risks of compromised patient care, damaged reputation, and the additional costs and labor associated with the breach itself—not to mention the Office for Civil Rights payments required *PER* breached patient record. The costs incurred by breach mitigation are quite substantial and organizations must be readily prepared if they plan on avoiding these sizeable consequences.

Kristi Fahy (kristi.fahy@ahima.org) is an information governance analyst at AHIMA.

Original source:
Fahy, Kristi. "WannaCry Ransomware Attacks Put Organizations on Alert" (Journal of AHIMA website), May 19, 2017.