Hospital Pays Ransom to Hacker in Response to Malware Attack: An Eye-Opening Reality

By: Daniel Ferhat and Jason Poore
Cyber Law and Data Protection Alert
3.9.16

With the advancement of medical technology and the mandate for electronic health records, hospitals and health care institutions are more reliant on their computer systems than ever before. For hackers, this makes hospitals lucrative targets. Last month, the Hollywood Presbyterian Medical Center paid $17,000 in bitcoins to a hacker who seized control of the hospital's computer systems. The hacker used malware to lock the hospital's computer systems by encrypting files, forcing the hospital to resort to the use of paper medical records. The only way to decrypt the files was to use a decryption key, which only the hacker possessed. The hospital gained full control of its systems with assistance of technology experts, but only after it paid the ransom. Fortunately, neither patient care nor hospital records were compromised.

While these types of "ransomware attacks" are seen in other industries, hospitals are not common targets. This cyber attack demonstrates the importance of securing hospital computer systems and files. Interestingly, Hollywood Presbyterian paid the ransom before reaching out to law enforcement agencies. This demonstrates that not only was the hospital unprepared for such an attack, but those in charge apparently did not have confidence that law enforcement would have been able to achieve a better result. This perspective fails to recognize that law enforcement agencies, including the FBI which is now handling this investigation, have sophisticated agents and resources to address cyber crimes.

So what steps can a hospital take to defend against such cyber attacks? The first step is recognizing that cyber attacks are not just an information technology issue. Cyber attacks can, and do, directly affect patient care and can result in unauthorized access to large volumes of patient records, leading to privacy and HIPAA-compliance issues. Hospital leadership should become involved in ensuring the security of its computer systems and files in light of the significant financial harm and reputational damage a cyber attack can cause.

Additionally, there are concrete practical steps hospitals can take in an effort to defend against cyber attacks. One such step is to have an outside company conduct an overall evaluation of the hospital's security system and protocols in case a breach occurs. These evaluations provide both technical guidance and legal counsel regarding the steps the hospital would need to take in the event of a breach, such as which regulatory bodies need to be notified and how to limit potential liability. Also, as demonstrated in the Hollywood Presbyterian case, it would be optimal to have a quick response system set up in the event of a breach. This could potentially involve a notification system that immediately alerts an outside technology security firm. Hospitals should also consider implementing system redundancy and having off-site back-up systems with separate firewalls in place so that core systems are operable at all times.

These are just some of the approaches hospitals should consider in the new age of cyber ransom. One option that will not work is to ignore this potential threat.

For further information on this matter, please contact Daniel Ferhat (ferhatd@whiteandwilliams.com; 215.864.6297), Jason Poore (poorej@whiteandwilliams.com; 215.864.6806) or a member of our Cyber Law and Data Protection or Healthcare Groups.