What Happens When Hospital Data is Held Hostage?

By Leslie Berkoff

Over the past six months, the number of cybersecurity attacks have increased around the globe, many of which have specifically impacted the healthcare industry. In 2016, in the USA alone, 328 health-care firms reported data breaches, up from 268 in prior periods, according to the 2017 Healthcare Breach Report released by data protection company Bitglass. Last May, during GGI's conference in Brussels, one of the largest 'ransomeware' attacks made world headlines when malicious software (aptly named 'WannaCry' 'WCry' or 'Wanna Decryptor') was transmitted via email targeting vulnerabilities in computer systems, in one of the largest 'ransomware' attacks on record. Ransomware is malicious software that infects machines, encrypts their data and then extorts money to let the users back into their own machines.

During this attack, cyber attackers took over computers, encrypted information, then demanded payment of USD 300 worth of online currency Bitcoin per machine from users to unlock the devices. Moreover, the malware did not distinguish between devices; as a result smartphones and medical devices were also impacted. The hacked devices then displayed the warning: 'Ooops, your files have been encrypted' along with a clock counting down to the deletion of the

...next page

Leslie Berkoff

device's data unless payment was made within a delineated time frame.

Some of the world's largest institutions and government agencies were affected, including Britain's National Health Service, where sixteen hospitals were hit as well as hospitals in Scotland. However, the attack did not just target the healthcare industry and all told it impacted seventy-four countries and a wide variety of industries were impacted. Since many of the European hospitals are centralised, the results were crippling. For some reason, perhaps because the hospital systems in the US are less centralised, US hospitals were not significantly impacted by this attack. Over the past year, multiple attacks have specifically addressed various healthcare systems in the US.

The attack apparently exploited a vulnerability purportedly identified for use by the US National Security Agency, which had developed the software, but then lost it to hackers. The hackers subsequently leaked the malware on the Internet and it was distributed by Shadow Brokers, a team of hackers. Microsoft had released a patch that would fix the vulnerability but in many cases the patch had not been installed or certain operating systems were outdated and therefore still vulnerable to attack.

During the May attack, hospitals had no access to computers or phone systems. Wards and emergency rooms were closed and new patients were turned away since no medical or financial records could be accessed to process insurance policies or payments. Moreover, they postponed treatments in order to ensure that people were not receiving improper, contradictory, or fatal treatment, such as prescribing medication

where there are contraindications for adverse interactions with other medications or allergy warnings. Internal phone lines at hospitals became inoperable so medical personal could not consult with one another. Private doctors' practices and pharmacies could not access insurance systems and medical records, forcing them to turn away patients and prescription requests.

The cost to recover from the attack could be exponential. At the National Health Service, teams had to work 24/7 to restore information and scrub files of the malicious malware. Thus, time and dollars that could have been spent elsewhere on medical improvements were lost to repairs and data recovery.

Furthermore, the risks extend beyond the immediate impact. The hackers can use or sell the stolen information to falsely obtain medical procedures. Another risk is that individuals could potentially be blackmailed due to sensitive information contained in health records. Unscrupulous third parties could also utilise healthcare information to falsify prescriptions and sell them on the black market or obtain them for personal use.

Lastly, these attacks may give rise to lawsuits. People who have had their privacy breached, or their personal data hacked, may have a basis to sue the medical facilities for failing to take proper precautions. Healthcare systems have an obligation to take reasonable care to protect private customer information. It is unclear whether any of the entities have specific cybersecurity policies which are designed to address these kinds of attacks. These suits may stress already financially stressed healthcare providers.

Therefore, health systems are gravely concerned about this attack and others. Last year, seventy-five percent of all major health care systems in the US alone had experienced major malware malfunctions. While the concern exists, the cybersecurity protections do not seem to be in place. While healthcare providers are universally switching over to electronic data, the security of this information has not matched its growth. Financial services industries devote in excess of 10% of their annual IT budgets to cybersecurity while the health care industry is less than 5%. Moreover, the cost of mitigating the damage can be astronomical, never mind the potential health hazards which arise during the interim period following the attack.

Given that they often have outdated IT systems and a wealth of confidential patient data, hospitals remain a particularly tempting target. As healthcare budgets shrink, healthcare providers must focus on preparing and protecting against further attacks. While it may not be possible to replace all outdated equipment, some steps can be taken. Consulting with a cybersecurity firm can be productive and could be geared towards a sliding economic scale. Raising awareness among staff and medical professionals of new threats, scams and emails which may contain malware is important. A good firewall and email screening process can provide some measure of protection. Finally, every hospital or healthcare agency should be backing up files and critical data, establishing a plan for an attack, and considering cybersecurity insurance as a way to handle the next WannaCry.

GGI member firm
Moritt Hock & Hamroff LLP
Law Firm Services
Garden City (NY),
New York (NY), USA
T: +1 516 873 2000
W: www.moritthock.com
Leslie A. Berkoff
E: lberkoff@moritthock.com