Cybersecurity and health care: where the concern lies

Over the past six months, cybersecurity attacks have increased around the globe, many of which have specifically impacted the health care industry. According to a 2017 Healthcare Breach Report released by data protection company Bitglass, 328 U.S. health care firms reported data breaches in 2016, up from 268.

This year, the following attacks occurred: (1) In February, Californian Hollywood Presbyterian Medical Center paid cyber attackers $17,000 in Bitcoins to regain control of its systems; (2) a month later, Washington D.C.-based MedStar Health was attacked and paid $19,000 in Bitcoins to restore encrypted files; (3) that same week, Alvaro Hospital Medical Center in San Diego was attacked but refused to pay; (4) additionally, Merck and Pennsylvania's Heritage Valley Health System were attacked; and (5) in July, Caro Community Hospital Medical Clinic and Quick Care (both located in Caro, Michigan) were attacked.

This past May, international headlines were made when one of the largest "ransomware" attacks on records aptly named "WannaCry," "WCry" or "Wanna Decryptor" was transmitted via email targeting vulnerabilities in computer systems. During this attack, cyber attackers took over computers, encrypted information, then demanded payment of $300 of Bitcoin per machine to unlock the devices.

The attack impacted 74 countries and a wide variety of industries. It affected some of the world's largest institutions and government agencies, including the United Kingdom's National Health Service, where 16 hospitals were hit. Since many of the European hospital systems are centralized, the result was crippling. For some reason, perhaps because the hospital systems in the United States are less centralized, U.S. hospitals were not significantly impacted by this attack.

These attacks impacted health systems in a variety of ways, resulting in the inability of hospitals to provide health care to the patients. Among other things, the attacks disabled the facilities and inhibited the ability for doctors to access medical records. Without access to medical records, hospitals could not access health insurance records to confirm coverage, and, more importantly, medical history could not be obtained, doctors could not prescribe new scripts or render services because they could not check for contraindications for adverse interactions or allergies. More minor complications resulted in the doctors' inability to update records or communicate with other doctors.

There are problems that extend beyond the immediate impact. The hackers can use or sell the stolen information to falsely obtain medical procedures. Another potential harm is that individuals could potentially be blackmailed due to sensitive information contained in health records. Health care systems do not just contain medical records; they contain Social Security numbers, bank statements, financial history, driver's licenses and information on spouses and guarantors. Unscrupulous third parties can also use this information to falsify prescriptions, sell the scripts on the black market, or obtain them for personal use.

The financial and operational risks from a cyberattack would be exacerbated in bankruptcy, although to date so far none have occurred post-petition. Moreover, the harms identified above could force an entity to contemplate or file for bankruptcy because of an influx of claims. WannaCry was the indirect result of a failure to perform certain simple upgrades and implement patches. Thus, individuals who have had their privacy breached, or their personal data hacked, or utilized by third parties may have a basis to sue the medical facilities, or their officers or directors, for failing to take proper precautions. Patient injury or death due to compromised devices, systems or technology could lead to a potential rise in class actions and claims against the facilities.

In the bankruptcy case *21st Oncology Holdings*, pending in the Southern District of New York, 17-22770 (RDD), a class action was filed on behalf of over two million current and former patients of the debtor who had their personal information compromised while undergoing cancer treatment at the facility. The claims assert that the loss was due to the company's failure to enforce sufficient security protocols and procedures and that the company did not discover the breach, but rather the FBI informed the company that the information was posted on the Dark Web. The validity of the claims is currently being litigated before the Bankruptcy Court, but the existence of these claims suggests they may have contributed to the bankruptcy filing.

The cost of these suits can be enormous: In the United States, HIPAA settlements totaled over $17 million from breaches of confidential information. In June, Anthem, the largest U.S. health insurance company, settled a multi-district lawsuit after the personal information of 78.8 million people was stolen during a 2015 cyberattack for $115 million.

The concomitant loss of public confidence and trust when these kinds of attacks occur often result in the loss of revenue from the public seeking alternative venues for treatment. Moreover, insurance companies may consider the failure to protect this data a basis to stop reimbursements. Loss of revenue may lead to loss of independent funding. Lenders to the facility may consider any or all of these to be a breach of an underlying loan covenant as a result of disruption of operations and loss of patient information. All of these events may stress an already financially stressed health care provider.

Health care systems have an obligation to take reasonable care to protect private customer information. Focusing on these issues is also part of the responsibility of the officers and directors of a facility. Yet the cybersecurity protections do not seem to be in place.

While health care 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 ten percent of their annual IT budgets to cybersecurity while the health care industry is less than 5 percent. Given that these facilities often have outdated IT systems and a wealth of confidential patient data, hospitals remain a particularly tempting target.

As health care budgets shrink, health care 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. One thing is clear, as these attacks continue to increase, the concomitant risk grows, leading a shaky industry to perhaps tip more into the insolvency zone.

By Leslie A. Berkoff