APRIL 5, 2022

Legaltech© news

ONLINE

ALM.

Cyberattacks in the Health Care Industry: The Way Forward

BY DANIEL GARRIE AND GAIL ANDLER

What threats does the health care industry face? The health care industry is particularly vulnerable to cybercrime given its dependence on electronic health information and antiquated security systems. Apart from data breaches, health care institutions face a more recent threat in the form of ransomware. This is "a type of malicious software designed to block access to a computer system until a sum of money is paid." Ransomware attacks and its effects put patients' lives at risk.

A cyberattack can happen in the blink of an eye or with the click of a mouse. A mid-level patient records administrator receives an email inquiring about an employment opportunity. Although he is not expecting any applications, and he is not a point of contact for employment inquiries, the administrator opens the résumé anyway. While he is reviewing the applicant's credentials, a cyber-criminal's malware is delivered to the hospital's network. The malware quickly captures the administrator's login credentials, and because he has broad administrative rights to company systems, the malware quickly spreads across the hospital's network and encrypts patient data. The attack is catastrophic. Patient records become unavailable and health care providers are forced to turn new patients away. Law enforcement is called in but they cannot solve the problem. The hospital must pay the ransom.

How then should the health care industry respond to these threats? First and foremost, there must be a change in the culture and a ready acceptance of the absolute importance of cybersecurity as an integrated part of patient care. Secondly, training, backing up, and securing data, and cyber insurance are three important areas that the health care industry should positively explore.

Credit: LeoWolfert/Shutterstock.com

Training: It is vital for health care organizations to make cybersecurity a priority. They can take steps to introduce, maintain and fully implement current and efficient cybersecurity practices. Every employee must know that information security is his personal responsibility, not just the responsibility of behind-the-scenes IT and information security personnel. If proper training is implemented, the scenario described above never would have occurred. This is because when the mid-level patient records administrator received the "suspicious" email, he would have sent it immediately to the IT personnel, who would have promptly detected the threat. Thus, the objective of implementing a training program is to establish the fact that cybersecurity must be the responsibility of every health care professional, from data entry specialists to physicians to board members.

Backing up and securing data: The sophistication of cyberattacks threatens the security of traditional data backups. Company data still faces some risk even when backing up into the cloud. The legal, risk and compliance teams need to work in tandem with the IT and information security groups to understand the nuances of the company's systems. Additionally, they must develop plans that ensure critical data, such as patient records, is both secure and readily accessible in the event of a cyberattack.

Cyber-insurance: Also known as cyber-liability insurance, health care organizations may want to turn to this increasingly popular form of insurance. It will not immediately solve all of their cybersecurity issues nor prevent cyberattacks. Notwithstanding this, the health care industry must ensure that they know exactly what they are signing up for. To successfully buy cyber insurance, what is needed is time, research, and a comprehensive risk assessment. In this regard, lawyers experienced in cyber insurance can be invaluable in assessing the coverage of a particular policy and matching it to the requirements of the company.

What should you do if your security is breached? Cybersecurity is a challenge of technology and tactics. The health care industry can meet the challenge through increased training and vigilance, transparency, and collaboration across the sector. Cybersecurity experts should be able to assist in developing an incident response plan that will prove to be vital in handling a cyberattack.

One step that can be taken to help mitigate legal costs associated with cyber-breach is to employ arbitration as a mechanism for dispute resolution. Accordingly, lawyers can assist health care providers by drafting arbitration clauses related to cyber-claims in patient agreements. This will allow any potential litigants to select an arbitrator with significant technical experience who will be able to advance the resolution of claims. Arbitration is not a silver bullet for dealing with cyberattacks. It is in fact a tool that can be used to save time and cost whilst allowing the health care provider to concentrate quickly on the business saving people's lives.

Additionally, the failure to use adequate measures to safeguard patient records and or personal information from cyber attacks will likely result in class action litigation subjecting the health care provider to large damage awards and harm to reputation. Such litigation has become increasingly common, and for many health care providers the legal fees and business costs alone justify heightened attention to these risks. Experienced mediators can help settle these disputes, but attention to prevention is critical.

Addressing the sophistication of cyberattacks requires a wide, collaborative approach across a myriad of organizations within government and private sector. Positive results will come from a shared commitment to face this challenge. This article has attempted to shed some basic light on how best lawyers and cybersecurity experts together can help health care providers to navigate the minefield created by cybercriminals.

Daniel B. Garrie is the co-founder of Law & Forensics (www.lawandforensics.com), a neutral with JAMS (www.jamsadr.com/garrie), the Editor-in-Chief of the Journal of Law and Cyber Warfare, a Lecturer in Law at the Rutgers School of Law where he teaches cyber warfare, data governance, and cybersecurity law, and a Certified Blockchain Engineer.

Judge Gail A. Andler (Ret.) joined JAMS as a full-time neutral after more than 22 years on the Orange County Superior Court of California, where she served from 2007 to 2017 on the Complex Civil Litigation Panel.