CYBERSECURITY/HEALTHCARE

THE GREY'S ANATOMY / ALLSCRIPTS RANSOMWARE CROSSOVER EVENT: WHEN SCRIPTED TV BECOMES REALITY, THE SCRIPT GOES OUT THE WINDOW

By: Sara H. Jodka and Justin L. Root

For those familiar with the Shonda Rhimes juggernaut, Grey's Anatomy, it is the story of surgical residents, fellows, and attending physicians as they work in the surgical wing of the fictional Grey Sloan Memorial Hospital. In most episodes, the situations in which the doctors find themselves in are entertaining, but not necessarily how they might play out in a real hospital setting.

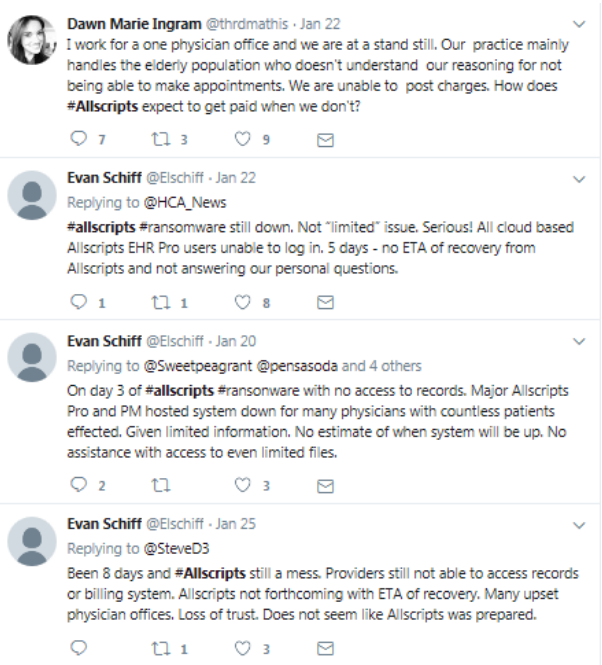
In the show's latest season 14, however, Episodes 8 "Out of Nowhere" and 9 "1-800-799-7233" play out a far too-real situation for those in the healthcare space and demonstrate just what type of damages and disruption cyber hacking can do to a healthcare provider.

In those episodes, the hospital's computer system is infected with ransomware that encrypts and holds hostage all of the hospital's patients' records until a ransom is paid in Bitcoin in an amount equivalent to $20 million USD. The fictional ransomware attack took out not only the hospital's access to electronic patient records, essentially sending the doctors back to the Stone Age in terms of working with paper records and taking notes regarding patient activity, but also rendered inaccessible the hospital's physical systems that were controlled by the now-encrypted computer system, such as the hospital's blood and pharmaceutical supplies. While the eventual solution for Grey Sloan is one of Shondaland fiction (no spoilers here), the attack itself and the initial ramifications and responses to the ransomware attack are entirely realistic.

Exactly how realistic? Well, Episode 8 originally aired on November 16, 2017, and on the exact same day that the second part episode aired on January 18, 2018, Allscripts, an electronic health record (EHR) company that provides healthcare systems cloud-based electronic health record services, suffered an eerily similar attack. The attack resulted in some of the company's applications being taken offline, including its cloud PRO EHR and Electronic Prescriptions for Controlled Substances (EPCS) platforms, which were hit the hardest by the attack.

While the effects on Allscripts were not similar to those at Grey Sloan, the similarities came into effect for the clients to which Allscripts provides its PRO EHR and EPCS cloud-based services. To weigh the scope of the interruptions and impact, Allscripts' client base includes 180,000 physicians across nearly 45,000 ambulatory facilities, 2,500 hospitals and 17,000 post-acute organizations. The attack had many of Allscripts' clients unable to access patient records, electronically prescribe medication, and ultimately, many customers faced severe and crippling operational deficiencies due to the inaccessibility to necessary patient data, forcing some to essentially shut down and wait for Allscripts to provide a solution to the access prohibitions caused by the attack.

Some of the public Tweets using the #AllScripts hashtag provide insight as to the difficulties Allscripts clients were facing as a result of the cyberattack:



The Allscripts ransomware attack came just days after two Indiana hospitals were hit with SamSam ransomware attacks. There, one of the Indiana hospitals paid 4 Bitcoin (approximately $55,000 USD) to recover its systems. The ransomware that infected Allscripts was a new variant unrelated to the version of SamSam that infected the Indiana systems, which has been confirmed by the FBI and the investigating computer forensic companies that were called in by Microsoft and Cisco.

Allscripts has already been sued by Surfside Non-Surgical Orthopedics on behalf of all of its clients impacted over the ransomware attack and has been accused of failing to secure and audit its systems, which caused the system outage for about a week and allegedly caused "significant business interruption" and "lost revenues" for its clients.

The question, then, becomes: What can an organization do when the information attacked is not within the organization's immediate control but is instead controlled by a third-party cloud service provider who suffers an attack?

For many businesses, cloud computing has been the most efficient and least expensive option for storing and accessing electronic data, including those in the healthcare space. As the security incidents discussed above detail, however, those cloud computing hosts are not 100% secure themselves leaving their clients vulnerable

to their own cybersecurity issues and those of their cloud-services vendor. Businesses therefore need to build a cybersecurity and data accessibility disaster response component into their overarching business continuity plans.

Here are some steps businesses can take to help alleviate some of the stress of a ransomware attack:

- **Back-Up Data:** The key to ransomware attacks is the hackers betting on the target needing the information being held hostage and being willing to pay a pretty penny, or in this case Bitcoin, to recover access. For data that is important for a businesses' operations, like patient data for healthcare providers, that operational-crippling information should be backed up to a physical storage device, such as a USB or a server somewhere, to ensure that there is another source of access for that information. This helps ensure that valuable information is not lost or rendered unobtainable and allows the organization to continue operations, especially in the case of those providing patient services.

- **Incident Response Plan/Team:** Every organization should have an incident response plan and team in place in the event a cyberattack occurs. This written and team-centered plan should include all key players of the organization including, those in the C-Suite with decision-making authority, legal, IT, forensics, and public relations to handle the communications. In the case of ransomware specifically, relationships with Bitcoin-focused entities is also helpful. Some include: "No More Ransom", which helps ransomware victims retrieve encrypted data that could be helpful; reputable Bitcoin exchanges, such as Coinbase, which is the largest Bitcoin company and received its license by the New York Department of Financial Services in meeting the state's consumer protection and cybersecurity standards, Bitpay and Coingate; and Bitcoin brokers to help transfer Bitcoin quickly.

- **Policies and Procedures:** For many organizations, cybersecurity policies and procedures are required. For those in the healthcare space, HIPAA/HITECH requires that covered healthcare organizations comply with the Security Rule and Privacy Rule. Here is U.S. Health Human Services' Ransomware Fact Sheet titled "FACT SHEET: Ransomware and HIPAA". When ransomware first became an issue, it was thought as not to be a breach since the information was merely held hostage and not accessed. That is not necessarily the case anymore, and now a further forensic review of the attack is required to ensure information is not taken during a ransomware attack. If it is, state notification laws could be triggered. For financial institutions, the Gramm-Leach-Bliley Act requires covered entities to comply with its relevant provisions, which include having a written incident response plan. (For more about GLBA compliance, click here.)

- **Vendor Contract:** If the attack is on a third-party vendor, it is important to review the services agreement with the vendor to determine what the contract provides in an attack situation. Better yet, have the vendor contract reviewed in advance of contracting to know exactly what is contractually required to happen in terms of coverage, damages, etc., in the event of an attack. If handled correctly, the review of vendor contracts will be done in conjunction with the formation and work of the Incident Response Team.

- **Insurance:** General liability and cybersecurity insurance go hand in hand. While cybersecurity insurance will likely cover the insured entity if it gets hit with a ransomware attack, it may not cover an attach on a third-party vendor and the resulting damage. This is likely where a general liability insurance policy will fill the gaps. Either way, it is important in this day and age to have both and to have both reviewed by counsel to ensure the company is properly insured regardless of the type of intrusion.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of cybersecurity law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Sara H. Jodka, CIPP-US, is Of Counsel in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.

Justin L. Root, GCFE, is Of Counsel in Dickinson Wright's Columbus office. He can be reached at 614.591.5465 or jroot@dickinsonwright.com.

Sara and Justin co-chair the firm's Data Privacy and Cybersecurity Group (U.S.) and handle data privacy and cybersecurity matters, including policy, response, training, and litigation defense for clients of all sizes.