10 of 998 DOCUMENTS

Michigan Lawyers Weekly

December 12, 2016 Monday

Ransomware: The rising trend in cyberwarfare that is paralyzing businesses

BYLINE: Norbert F. Kugele and Nathan W. Steed

SECTION: NEWS

LENGTH: 1294 words

A recent government report estimates that, on average, more than 4,000 **ransomware** attacks have occurred daily since January 1, 2016, a 300 percent increase over the approximately 1,000 attacks per day in 2015.

These attacks focus on the healthcare industry primarily, accounting for 88 percent of all **ransomware** detections in the second quarter of 2016. Education and finance industries account for an additional 10 percent of attacks.

Ransomware is a specific type of malware that targets data stored on a computer or computer system. **Ransomware** is usually delivered via email containing a link that directs a web browser to download the malware. Once on a computer, **ransomware** encrypts the hard drive, making use and access impossible. **Ransomware** then instructs the user to pay a certain amount, typically from several hundred dollars to several thousand dollars, to unencrypt the data and regain use and access.

Attackers may demand payment in the form of Bitcoin, Ethereum, Dogecoin or other cryptocurrency. Many **ransomware** attacks also require payment within a short period of time --typically one to three days -- or else risk losing access to the data entirely.

Companies experiencing **ransomware** attacks are in a race against the clock to regain control of their data. In the midst of this process, however, companies must also carefully analyze whether the attack triggers any notification requirements.

Notification requirements stemming from a **ransomware** attack could arise in three contexts:

As a contractual obligation;

As a statutory requirement; and

As a regulatory requirement.

Contractual obligations

Standard confidentiality language appears in many contracts. Parties will typically agree to protect the confidential information of one another and to not disclose it unless it's needed to perform under the contract or as required by law. Many contracts also contain a clause requiring the reporting of security incidents related to confidential information.

Definitions may vary between contracts, but HIPAA provides a good baseline: "the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. "

Under this definition, a **ransomware** attack affecting the confidential information of a third party would likely qualify as a security incident. Depending on the extent of access, the attack may also be a breach of confidentiality. A **ransomware** attack is a successful interference with system operations. Additionally, the attack may have resulted in the disclosure of confidential information to a third party not authorized under the agreement.

A company experiencing a **ransomware** attack should audit its contracts to determine whether it needs to notify business partners that the business partner's confidential information may have been accessed. If there is a silver lining, it's that many **ransomware** attackers do not actually disclose the data. If the **ransomware** attacker did not obtain any unencrypted data as part of the attack, then actual damages to third parties may be limited. This may be cold comfort given other potential notification requirements.

Statutory requirements

Currently, 47 states maintain a data security breach law. While there are some similarities, each state has its own peculiarities. Michigan's Identity Theft Protection Act requires notice to individuals "without unreasonable delay" unless the company determines that "the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to" a resident of the state.

Michigan law defines a security breach as "the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information. "

Assuming the **ransomware** attack targets the relevant information, a company must conduct a risk analysis. A **ransomware** attack likely qualifies as a security incident under Michigan law. But, a company may determine that the attack will not cause substantial loss or injury or identity theft to Michigan residents. That's not to say that it couldn't.

But, the typical **ransomware** attack is limited to a money grab and not a more nefarious data theft. Nevertheless, companies will need to make this determination on a case-by-case basis given the nature of the attack.

Regulatory requirements

Because **ransomware** attacks have overwhelmingly targeted the healthcare industry, we'll focus on HIPAA-specific issues. A **ransomware** attack undoubtedly qualifies as a security incident for HIPAA purposes. Whether or not a **ransomware** attack would qualify as a breach of protected health information (PHI) under HIPAA is a fact-specific determination.

The initial question the organization should ask is whether the PHI was encrypted before the attack. A **ransomware** attack could theoretically further encrypt already encrypted data. Encryption doesn't protect an organization from a **ransomware** attack, but it may mitigate potential HIPAA liability. If PHI is not encrypted, however, the **ransomware** attack is likely a breach because the attack is an unauthorized access or disclosure of PHI.

Unless the organization can demonstrate that there is a low probability that the confidentiality of the PHI has been compromised based on its risk assessment, then the organization will be required to satisfy its notification requirements under HIPAA, including notification to the affected individuals and the Secretary of Health and Human Services.

The more difficult scenario is determining whether it is a reportable breach if PHI encrypted by **ransomware** was

already encrypted prior to the attack. Because breach notification applies to "unsecured PHI," if an organization has encrypted the information in accordance with HIPAA, it typically would not need to conduct a risk assessment to determine if there is a low probably of compromise.

However, the nature of the **ransomware** attack may affect the analysis. For example, if a computer uses full disk encryption and is properly shut down and powered off and then lost or stolen, the data would be secure. But, in a **ransomware** attack, the computer is generally powered on and in use by an authenticated user who then does something to initiate the attack, such as clicking on a link. In this scenario, there could be a breach of PHI because the **ransomware** may now have access to decrypted data. So, while encryption generally is a strong protection from a breach, in a **ransomware** attack the fact that a hard drive uses encryption technology is not the end of the analysis.

Having a plan in place for a potential **ransomware** attack is an organization's first step in protecting itself, its customers and partners. Organizations facing a **ransomware** attack obviously need to move quickly to address the attack. But once the incident has been addressed, the organization can't forget to analyze potential notification duties. Those notification requirements may not always be as obvious as they first appear.

Norbert Kugele and Nate Steed are partners at Warner Norcross & Judd LLP in Grand Rapids. Kugele specializes in employee benefits and privacy and information security law. He is a privacy expert who helps organizations understand and comply with state, federal and international privacy and information security laws, including HIPAA, FTC consumer privacy requirements and breach notification laws. Steed counsels organizations in technology and intellectual property law, health law and privacy and information security law. His specialty involves the acquisition and use of software and hardware and the internet of things.

Click here for more from this resource.

LOAD-DATE: December 16, 2016

LANGUAGE: ENGLISH

DOCUMENT-TYPE: Legal activity (lawsuits etc.)

PUBLICATION-TYPE: Newspaper