3 Essential Steps For Responding To Ransomware Attacks

Prepared by:
Damon W. Silver
Jackson Lewis P.C.

LORMAN EDUCATION SERVICES
September 2016

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 700 available
- ☑ **Slide Decks -** More than 1700 available
- ☑ **White Papers**
- ☑ **Reports**
- ☑ **Articles**
- ☑ **... and much more!**

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: **www.lorman.com/pass/?s=special20**

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

3 Essential Steps For Responding To Ransomware Attacks

Friday, September 9, 2016

Likely because most victims comply with their demands, the incidence of attacks by ransomware hackers has exploded in 2016. Guidance issued by the U.S. Department of Health and Human Services ("HHS") in July notes that, on average, there have been 4,000 reported ransomware attacks *per day* thus far in 2016, far exceeding the average of 1,000 attacks per day last year.

What Is Ransomware?

Ransomware is a type of malware that denies the affected user access to his or her data, typically by encrypting it. Once the user's data is encrypted, the hacker who launched the ransomware attack notifies him or her that, in order to obtain a key to decrypt the data, he or she must pay a ransom, often in a cryptocurrency such as Bitcoin. Hackers sometimes impersonate government entities – like the IRS or FBI – in their ransom notes.

Can I Just Pay The Ransom And Move On?

While it may be tempting to do so, there are serious risks to this approach. Even if the ransom demanded by a ransomware hacker is not prohibitively expensive, an organization victimized by an attack must bear in mind that simply paying off the hacker is unlikely to make its problems go away.

As an initial matter, there is no guarantee that, upon receipt of the ransom payment, the hacker will provide a fully functional key that enables your organization to regain access to its data. Moreover, your organization must evaluate whether the ransomware attack triggered legal obligations under federal or state privacy laws, or other regulatory or contractual requirements.

What Are My Legal Obligations In The Event Of A Ransomware Attack?

Determining your organization's legal obligations in responding to a ransomware attack requires a fact-specific inquiry. For organizations subject to HIPAA, for example, HHS's guidance indicates that a ransomware attack is ***presumed*** to be a breach triggering HIPAA obligations unless the affected organization can demonstrate that there is a low probability that protected health information ("PHI") has been compromised. This low probability analysis, the HHS instructs, should include consideration of a the following four factors, among others: (1) the nature of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated.

Organizations that are not subject to HIPAA must also assess their legal obligations in the wake of a ransomware attack, such as those imposed by the Gramm-Leach-Bliley Act or under state law. Under the data breach laws of certain states – such as New Jersey, Connecticut, Florida, Kansas, and Louisiana – unauthorized ***access*** to personal information constitutes a breach, even absent evidence that the personal information accessed was

actually acquired. Organizations whose affected employees or consumers work or reside in these states thus face increased risk that a ransomware incident will trigger breach notification obligations.

Additionally, during some ransomware attacks, hackers do not simply block the user's access to its data, but also exfiltrate that data to external locations, and/or destroy or alter it. Accordingly, organizations subject to the data breach laws of any state may be required to take certain actions in the event of a ransomware incident.

What Should I Do After I Discover A Ransomware Attack?

If you believe your organization has been victimized by a ransomware attack, you should proceed as follows, carefully documenting each of the steps laid out below:

ONE: Notify your cyber liability insurer. This step is essential not only to ensure applicable coverage, but also because your insurance contact will likely be able to provide valuable early-stage guidance, such as on retention of qualified data security professionals to investigate the ransomware incident, and implementation of appropriate measures to mitigate existing and future risk.

TWO: Investigate the incident. Your internal or outside data security professionals should immediately launch (and document) an investigation of the incident. This investigation should include, at minimum, analysis of:

- When the incident occurred.
- The methods the hackers used to carry out the attack.
- Which of your systems were affected.

- The nature of the data affected – *e.g.*, was PHI or personal information accessed or acquired. (Most state breach notification laws define personal information as the affected individual's full name, or first initial and last name, in combination with any of the following data elements: (i) social security number; (ii) government identification card number; or (iii) account number or credit / debit card number with any required security code, access code, or password.)
- The states in which the individuals whose data was affected work or reside.
- Whether there is evidence that the affected data was exfiltrated to the attacker's servers, or elsewhere.
- Whether the attack is completed or ongoing; and, if that latter, whether additional systems have been compromised.
- What mitigation measures were and are in place. For example:
    - Were the affected files encrypted and, if so, is there evidence that the hackers successfully decrypted those files.
    - What data backup, disaster recovery, and/or data restoration plans did you have in place.
    - What post-discovery steps did you take to prevent continued or future acquisition, access, use, or disclosure of the compromised data.

THREE: Consult legal counsel. As discussed above, ransomware attacks may trigger obligations under federal and state privacy laws, such as HIPAA, the Gramm-Leach-Bliley Act, and state breach notification laws. They may also require an affected organization to comply with other regulatory and contractual requirements, and to communicate with government agencies like the FBI, U.S. Secret Service, or state attorneys general

offices. Consulting an experienced attorney upon discovery of a ransomware attack will ensure that your organization complies with applicable legal requirements, thereby controlling the costs inflicted by the attack to full extent possible.