Data Privacy & Cybersecurity Alert

PULLMAN & COMLEY

A publication of Pullman & Comley, LLC

Attorneys:

- **Russell F. Anderson**
  randerson@pullcom.com
  203.330.2271
- **Timothy G. Ronan**
  tronan@pullcom.com
  203.674.7933

Prepare to be Ransomed: A Primer on Legal Obligations Before and After Ransomware Strikes

October 30, 2017

by Russell F. Anderson

According to a recent U.S. Government Interagency report, ransomware is the fastest growing malware threat, targeting users of all types. An incredible 51 percent of respondents in a January 2017 study by the Ponemon Institute reported that their organization had suffered a ransomware incident within the past year.

Ransomware is malware that invades a computer's systems – such as through a phishing message or a compromised Internet site – and then encrypts all of the data that it can find. The data is thus rendered unusable until a ransom is paid (usually in Bitcoin) in order to receive the necessary de-encryption key.

This article provides a brief overview of some of the legal considerations that organizations should take into account both before and after ransomware strikes. These requirements will most often flow from sensitive information held by the organization, such as HIPAA-protected health information (PHI) or employee Social Security numbers.

Steps to Take Before Your Data is Gone

The Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services has published in-depth guidance that addresses how businesses that handle PHI must prepare for ransomware. While this guidance is specific to HIPAA, the data security principles under many other federal, state and international laws are similar.

Prepare to be Ransomed: A Primer on Legal Obligations Before and After Ransomware Strikes

HIPAA requires that a covered organization review in writing the potential vulnerabilities to PHI stored by the organization as well as demonstrate that it has undertaken security measures to mitigate those risks and identify any gaps in security it cannot fill. In addition, the HIPAA Security Rule requires a number of specific steps that are relevant to malware attacks, such as:

- Establishing safeguards for guarding against and detecting malicious software;
- Training users to identify malware and report to IT if they believe they have fallen victim; and
- As we've been reminded thanks to the Equifax breach this fall, promptly patching software with known vulnerabilities.

As HIPAA requires not only confidentiality, but also the availability and integrity of the data, regular testing of data backups and business continuity planning are also needed. Data backup especially proves its worth in the context of ransomware. In the Ponemon Institute study, 42% of respondents cited having a full and accurate backup as the primary reason why they did not pay the ransom.

Responding to Ransomware

So, if your systems have been victimized by ransomware, and your data has been encrypted, now what?

From a practical perspective, you have decisions to make, such as whether to pay the ransom and whether to report the incident to law enforcement. Organizations are not prohibited from paying the ransom, although law enforcement generally advises against it (as it increases the incentives for further attacks). According to the Ponemon study, 48% of respondents who suffered a ransomware attack answered that their company paid the ransom and that the average payment was $2,500. In a similar study conducted by IBM's security team, 70% of those that had been struck by ransomware paid to get access to their data back, and 20% of the organizations affected had paid more than $40,000.

There is no guarantee that paying the ransom will, in fact, restore your data, although the odds are apparently not terrible. In the Ponemon Study, 55% of respondents indicated that once the payment was made, the decryption key was actually provided to unlock the data. This determination can be made in part based on knowing the characteristics of the malware. The WannaCry strain that attacked earlier this summer reportedly was more interested in destroying data than generating revenue for its creators.

From a regulatory perspective, reporting the ransomware incident to law enforcement authorities is the highly recommended, if not required, step.

Lastly, in the event of a ransomware attack, you must also consider who must receive notification of the breach under applicable federal, state and international laws and client contracts (such as affected individuals, clients and state Attorney General Offices). What makes ransomware different from other hacks

is that while you know information has been "messed" with, you don't necessarily know that the information has been compromised or stolen. That distinction can potentially matter in the context of whether individual data breach notification requirements are triggered.

If data has been "exfiltrated" – i.e., removed from your systems – then the data breach notification requirements under applicable law and most customer contracts will apply. However, as the OCR guidance notes, while there is a presumption that a breach has occurred, the presumption may be overcome if you are able to show that the information was not actually acquired or viewed by an unauthorized party (e.g., if the data was already encrypted on your systems before the ransomware struck or if the malware did not have the capacity to exfiltrate the data).

Be Prepared

As October is National Cybersecurity Month, there is no time like the present to review your plans for preventing and recovering from ransomware. If despite your best efforts you suffer a ransomware attack, having a battle plan in place for investigating the functionality of the malware and determining whether those characteristics trigger data breach notification requirements will be key to meeting your legal obligations.