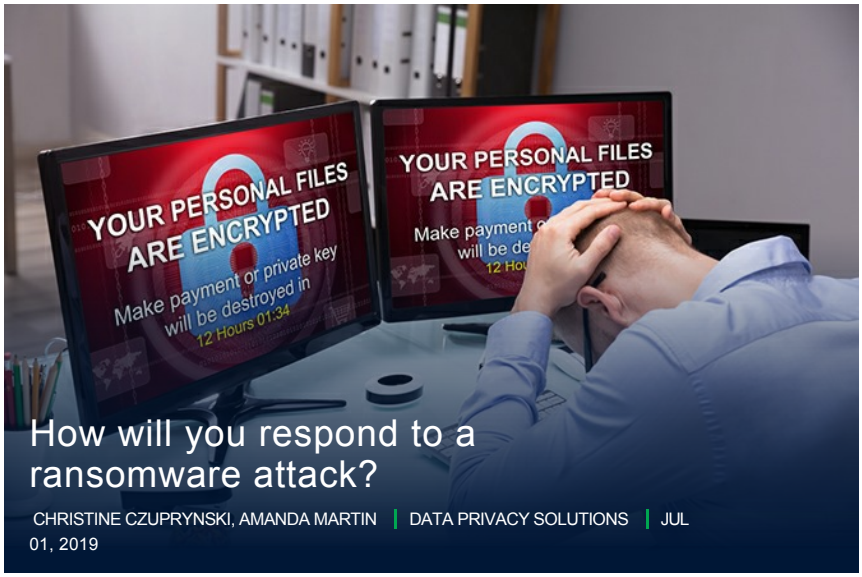

How will you respond to a ransomware attack?

CHRISTINE CZUPRYNSKI, AMANDA MARTIN | DATA PRIVACY SOLUTIONS | JUL 01, 2019

It's Saturday morning and one of your employees has gone to the office to get a jump on the week's work. Instead of being able to get to that work, the employee is faced with locked and inaccessible files, and an onscreen message that the files have been encrypted. The employee alerts IT and the front office. IT confirms what everyone suspects – it is ransomware.

Now what?

Ransomware is one of the most common types of data security incidents, and often unfolds in the same way: after being deployed by attackers, the ransomware encrypts files on a system so that they are inaccessible. A ransom note left by the attackers provides contact information and a promise to provide a decryption key – for a price of course.

There are many different ransomware variants that differ in how they are deployed, the total amount of the ransom demand, and their impact on infected systems. Some of the many variants entities have faced in 2019 include: Dharma, RYUK, Sodinokibi, SamSam, GandCrab, WannaCry, CryptoLocker, and TeslaCrypt. There are likely many more variants waiting in the wings to be deployed. The McDonald Hopkins Data Privacy and Cybersecurity team has handled thousands of ransomware matters covering all of these variants, as well as many others.

A ransom note demands immediate attention, and it can be tempting to respond as quickly as possible to the attackers to get things moving. There is sometimes a countdown within the note, which further elevates the feeling of anxiety and helplessness of the situation. As best you can, do not give in to that anxiety. Instead, take some time to assess the situation before responding. "Some time" is relative, and here, we mean an hour or two. The best approach would be to devise a ransomware response strategy now, before any malware hits your environment.

A ransomware response strategy can include the following, which should all happen within the first few hours of identifying the attack:

- Alert cybersecurity insurance carrier, and legal and forensic experts, to assist.
- Using internal IT and external experts as necessary, terminate any and all unauthorized access into your system(s) and rest passwords to keep the attackers out.
- Assess the viability of back-ups.
- If back-ups are encrypted and/or unavailable, or while the viability of the back-ups is being assessed, have a forensic expert communicate with the attackers to obtain the initial ransom demand and begin negotiations as appropriate. Do not communicate with the attackers yourself, and especially do not communicate with the attackers via a company owned e-mail address.
- Enlist all relevant stakeholders to make the determination whether data will be restored from available back-ups and/or the ransom will be paid with the hope of obtaining the decryption key.

The threat of ransomware is very real. Any and all industry sectors have been victimized by these attacks to varying degrees. If you think that your company is not attractive to these cyber criminals, or is somehow immune from ransomware, the time has come to make a shift.

Taking steps now to prepare a response strategy can save precious minutes when an attack hits.

CHRISTINE CZUPRYNSKI

Read More

AMANDA MARTIN

Read More