Petya Global Ransomware Attack Shows Why Businesses Should Prepare for Loss or Unwanted Encryption of Key Data

June 29, 2017

What is it? This new variation of *Petya* ("Little Peter" in Russian) is more robust ransomware than last month's North Korean *WannaCry* ransomware. It has no kill switch, and it encrypts entire hard drives, not just individual files. Like *WannaCry*, it targets Windows XP, an older software. It also steals administrative credentials, giving it control over Microsoft system management tools and with it, the potential to instruct other system computers to run the malware, even if those computers have received Microsoft software patches to thwart it.

What has been the effect so far? The new ransomware has targeted about 2,000 businesses in 65 countries so far, including the United States. On Tuesday, prior to Ukraine's national holiday recognizing its 1996 break from Russia, the first Ukrainian computers were infected. Next were global companies such as DLA Piper in legal, Merck in pharma, Maersk in shipping, Cadbury in chocolate and Deutsche Bahn, the German railway. Given *Petya's* failure to improve much upon *WannaCry's* ill-conceived ransom payment process, experts believe the attackers' goal may be disruption of business, rather than collection of ransom. Regardless of the attackers' motives, businesses no longer have the luxury of ignoring the risk of a ransomware attack.

What if our company is infected? A company facing a ransom demand is in a quandary, and should consult with computer experts and legal counsel on the pros and cons of paying a ransom. Most do not pay, but some will choose to do so, considering the operational and financial risk of losing key unsaved data forever. Businesses that lose the data of others to ransomware may have to explain what they could have done to prevent or mitigate the ransomware harm. Cyberinsurance may cover some or all of the damages, depending on policy language and its interpretation.

How can we learn more? On August 29, 2017, Lathrop Gage will host its Third Annual Cybersecurity and Data Privacy Summit, focused upon Ransomware. During this half-day program geared to company executives, general counsel and information security and privacy officers, attendees will hear from the Secret Service, Lathrop Gage attorneys, computer forensics professionals and others about responding to this growing cyber-epidemic. Click here to RSVP.

In the meantime, here are some ransomware mitigation strategies from our May, 2017 *WannaCry* alert:

An Information Security Plan. Adopt and maintain one. It should serve as your guidebook for data security and practices. An information security plan should not be for the exclusive use of the IT department, although they will use it most often. It should contain summaries and directions that non-IT employees can follow. Also, an information security plan should contain procedures for up-to-date software and a process for timely installing security patches.

Ransomware and other malware typically enter a company's system through "phishing" emails, upon which employees unwittingly click and download the infiltrating program. Anti-phishing programs and software are out there, but none are perfect. By training your workforce and adopting a culture of computer hygiene and threat awareness, you can reduce your exposure. Make these and other good practices part of your Information Security Plan.

An Incident Response Plan. If you have an Incident Response Plan and Team as part of your overall business recovery strategy, you will not be starting from square one when you become the victim of a breach or malware attack. In the process of adopting a plan, companies often realize existing, previously unknown, vulnerabilities.

As part of a comprehensive Incident Response Plan, you should have an up-to-date inventory of your key data, as well as the backup status for all your systems. By testing the recovery of data from backup in different scenarios, you will have a preview of time and success/failure rates for the various threats.

In developing the response plan, you may have different personnel, vendors and other resources in place for different threats, whether it is a Dedicated Denial of Service Attack upon your website, a lost or stolen laptop or flashdrive, or ransomware.

At Lathrop Gage, our Cybersecurity and Data Privacy team can assist you with all aspects of planning, prevention and response. If you have questions regarding this alert, please contact your Lathrop Gage attorney or the attorney listed above.