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

May 16, 2017

"Oops, your files have been encrypted!" On Friday, May 12, 2017, employees around the world found this message on their computer screens. A massive cyberattack has used variants of the *WannaCry* ransomware program to infect more than 230,000 computers in 150 countries, demanding Bitcoin ransom payments in 28 languages. Across the globe, many factories, hospitals, offices, government agencies and other entities shut down or were seriously affected.

No country was immune, with Russia, Ukraine, China and EU countries hit hardest. Fortunately, the malware contained an inherent "kill switch," coding defects and a non-automatic payment scheme, so that most businesses could remedy the problem, and only about 200 payments totalling $50,000 in ransom had been collected on the three *WannaCry* Bitcoin accounts through Monday afternoon. The danger has not been abated, however, as experts fear new strains of the ransomware will be more robust. For now, *WannaCry* should serve as a wake-up call to all of us.

Legal Concerns. 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. As cyberjournalist Brian Krebs notes, law enforcement or white hat cyber resources may have already worked out a way to break or sidestep the encryption, sometimes posting the keys to unlock the malware online, free of charge. Payment of a ransom on Bitcoin is a unique transaction and is no guarantee the attacker will release the data to you. Further, payment often results in your company finding itself in the crosshairs of other malefactors looking for companies willing to pay. In some cases, however, the stakes may be so high you may want to assume the risk of payment.

Other legal disputes will invariably follow this massive *WannaCry* attack, as parties try to determine responsibility for their related losses and liabilities. If, for example, your business entrusted a vendor or other business with sensitive information, that party may have contractual or other obligations to have prevented or mitigated the ransomware harm. Also, cyber insurance may cover some or all of the damages, depending on policy language and its interpretation.

In addition to restoring your company's access to your data, a ransomware infection may trigger notification or other regulatory obligations under state or federal law. These obligations frequently turn on the nature of the ransomware, the type of information affected (protected health information or personally identifiable information), the method of infection, and the steps you take to mitigate the incident. HHS, responsible for enforcing HIPAA, has published guidance (available here) regarding the potential impact of a ransomware infection on breach notification obligations.

HHS has also provided resources regarding the *WannaCry* ransomware incident through three updates available here, here and here.

What are some of the best defenses to ransomware and similar threats?

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.

Among other things, an information security plan should contain procedures for up-to-date software and a process for timely installing security patches. *WannaCry* targeted computers using Microsoft Windows XP, for which Microsoft has not issued security patches for the last three years (although Microsoft just issued a special security patch). Many businesses have found they had an old PC somewhere running Windows XP, and *WannaCry* found and exploited it.

Ransomware and other malware most 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 flash drive, 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 attorneys listed above.