CYBERSECURITY & DATA PRIVACY: RANSOMWARE

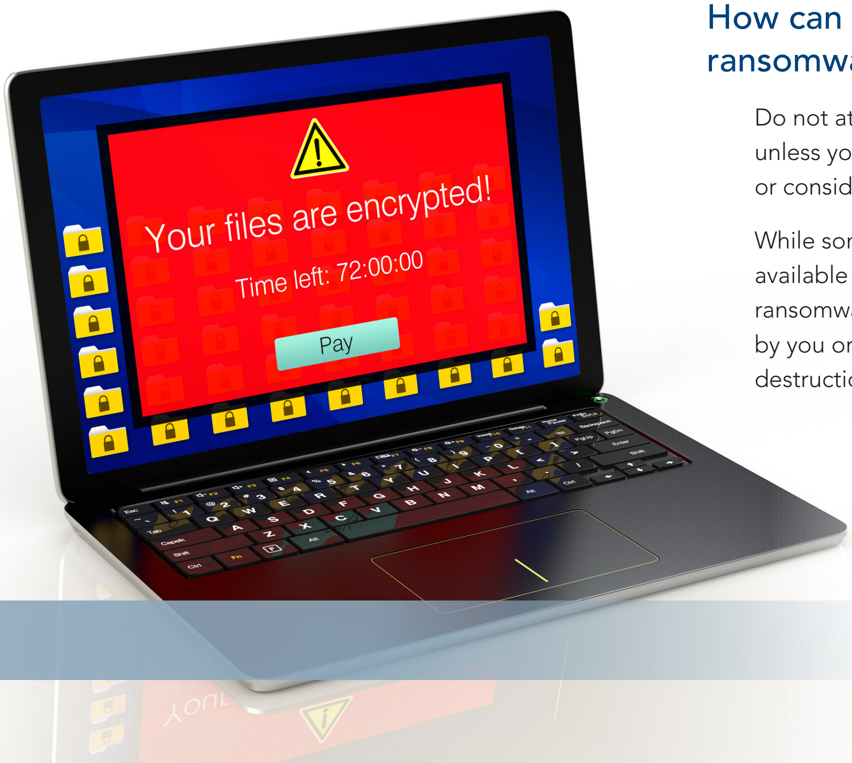
What is "ransomware"?

Ransomware is a malicious program or "malware" that encrypts your data and holds it for ransom. Ransomware will encrypt any files it can access.

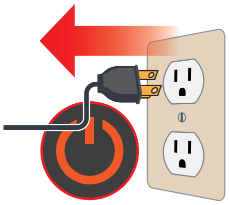
How do I know if ransomware has affected my computer?

Do you experience these symptoms?

- You suddenly cannot open normal files and get errors such as the file is "corrupted" or has the "wrong extension."
- File names have been changed and are unrecognizable.
- You find files in all folders with names such as HOW TO DECRYPT FILES.TXT or DECRYPT_INSTRUCTIONS.HTML or a message with instructions on how to pay to unlock your files.
- A window has opened to a ransomware program and you cannot close it.

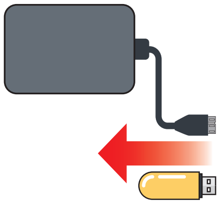


Help, I'm being attacked! What do I do?



UNPLUG! Power off. Your computer could allow the attack to move to other parts of your network. If the files you found were on a server, power off that server to stop the encryption.

Disconnect any mass storage devices, including USB flash drives, external hard drives or other external backup solutions. Unplug any storage devices such as USB or external hard drives.



Call in the experts. An experienced breach coach and forensic investigator will be able to advise you on what to do next.

How can I stop and remove the ransomware? Should I attempt to?

Do not attempt to remove or disable the ransomware unless you have access to a data security professional or consider yourself a highly sophisticated user.

While some decryption solutions are being made available by benevolent hackers, there are hundreds of ransomware variants to account for, and actions taken by you or your IT team could result in a loss of data or destruction of critical evidence.

CYBERSECURITY & DATA PRIVACY: RANSOMWARE

How do I get back to business?

Do you have backups of the encrypted data?

- A recent backup is often the best solution for addressing a ransomware attack. Restoring your files from a backup will ensure the integrity of the data is maintained.
- Inventory devices with impacted files and assess the devices that were connected to the computer or server you know was infected. Ask the following questions: Was the infected computer connected to any other PCs, servers, storage devices or cloud storage? Were any files encrypted on those devices?

Should I pay the ransom?

- While payment of a ransom is not recommended, if you do not have backups of the data and all options to decrypt or recreate the affected files have been exhausted, payment of the ransom may be necessary to continue business operations. Also, there is a chance that payment of the ransom will not restore your files. Remember – you're dealing with a criminal!

Do I have to report this incident?

Are there any reporting requirements?

- Depending on what data was encrypted and how the attack occurred, you may have an obligation to report the incident to individuals whose information is contained in the encrypted documents. Experienced legal counsel will be able to guide you through any regulatory reporting requirements.

What about law enforcement?

- With the guidance of legal counsel, you should strongly consider reporting the incident to law enforcement such as the FBI. The information you have about an attack could be critical to an ongoing investigation.

How do I protect against ransomware attacks?

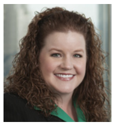
- Back up your most critical data assets and make sure the backups are running successfully and on schedule.
- Train your employees about ransomware attacks, social engineering and other cyber threats.
- Enforce additional credential requirements for access to sensitive and critical company information and consider the necessity of network drive mapping to key data.
- Restrict user account privileges for running executable files and scripts.
- Consider cyber insurance – policies may cover ransom payments and breach response assistance with access to experts.

Talk to a data security professional about other preventive measures.

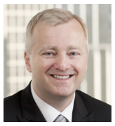
For more information, contact:

Gregory Bautista | Partner
Co-chair, Cybersecurity & Data Privacy Practice
White Plains | 914.872.7839
gregory.bautista@wilsonelser.com

Anjali Das | Partner
Co-chair, Cybersecurity & Data Privacy Practice
Chicago | 312.821.6164
anjali.das@wilsonelser.com



Lindsay Nickle | Partner
Co-chair, Cybersecurity & Data Privacy Practice
Dallas | 214.698.8093
lindsay.nickle@wilsonelser.com



Ian Stewart | Partner
Co-chair, Cybersecurity & Data Privacy Practice
Los Angeles | 213.330.8830
ian.stewart@wilsonelser.com

Cybersecurity Hotline: 877.292.3710