ABA/FBI Private Industry Notification

New Cyber Alert: Ransomware

The FBI recently sent a private industry notification about ransomware to the American Bar Association, requesting that the ABA share the cyber alert with the legal community. The alert focuses on specific cybersecurity risks and threats targeting law firms, and counsels lawyers to consider the following in trying to prevent ransomware attacks:

- Focus on awareness and training. Since end users are targeted, employees should be made aware of the threat of ransomware, how it is delivered, and trained on information security principles and techniques.
- Patch the operating system, software, and firmware on devices. All endpoints should be patched as vulnerabilities are discovered. This can be made easier through a centralized patch management system.
- Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
- Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary; and they should operate with standard user accounts at all other times.
- Implement least privilege for file, directory, and network share permissions. If a user only needs to read specific files, they should not have write access to those files, directories, or shares. Configure access controls with least privilege in mind.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement software restriction policies (SRP) or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular Internet browsers, or compression/decompression programs, including those located in the AppData/LocalAppData folder.

In addition, the FBI stated that it does not advocate paying a ransom. Paying a ransom does not guarantee that an organization will regain access to its data. In fact, some individuals or organizations were never provided with decryption keys after paying a ransom. While the FBI does not advocate paying a ransom, there is an understanding that individuals and organizations will evaluate all options to protect shareholders, employees, and customers.

To read more about the ABA Cyber Security Initiatives, visit:
http://www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity.html