SpencerFane®

Five Best Practices the White House Urges all Businesses to Take to Mitigate Risk of Ransomware Attacks

The threat of ransomware attacks against all American businesses is so great that on June 2, 2021, the White House issued a memo to all corporate executives and business leaders with the subject "What We Urge You To Do To Protect Against The Threat of Ransomware." This is the first time such a memo has ever been issued. That is how serious the threat of ransomware attacks is to our nation.

The Memo instructs that in order for businesses to understand their risk, "business executives should immediately convene their leadership teams to discuss the ransomware threat and review corporate security posture and business continuity plans to ensure you have the ability to continue or quickly restore operations."

The Memo then provides five recommended best practices as the first steps to take in mitigating this risk, which are explained in more detail in the document.

Now understand, these steps are not the only things you should be doing, and doing them will not eliminate the risk. These are just the U.S. Government's recommendations that are believed to have the most impact, as a place to begin:

1. Backup your data, system images, and configurations, regularly test them, and keep the backups offline
2. Update and patch systems promptly
3. Test your incident response plan
4. Check your Security Team's work
5. Segment your networks

This blog post was drafted by Shawn Tuma, a Partner in the Plano, TX office of Spencer Fane. For more information, visit www.spencerfane.com.

Additional Resources

- Good Cyber Hygiene Checklist
- Understanding How Cyber Insurance Impacts Your Incident Response Planning
- Digital Extortion Drama: Deconstructing the Ransomware Response Lifecycle (audio)