CYBER UPDATE

BITNER HENRY
INSURANCE GROUP

Harden Your Cyber Defenses Immediately, White House Warns Private Sector

In a March 21, 2022 statement, President Joe Biden cautioned businesses in the private sector to harden their cyber defenses, reiterating earlier warnings related to potential cyberattacks against U.S. organizations by Russia.

"I have previously warned about the potential that Russia could conduct malicious cyber activity against the United States, including as a response to the unprecedented economic costs we've imposed on Russia alongside our allies and partners," Biden said. "It's part of Russia's playbook. Most of America's critical infrastructure is owned and operated by the private sector, and critical infrastructure owners and operators must accelerate efforts to lock their digital doors."

While there is no evidence of an imminent attack tied to the Russia-Ukraine crisis, Biden's top cybersecurity officer Anne Neuberger noted that the everyday cyber risks businesses face and the potential for Russia-led cyberattacks call for urgency.

"There is no evidence of any specific cyberattack that we're anticipating for," Neuberger said. "There is some preparatory activity that we're seeing, and that is what we shared in a classified context with companies who we thought might be affected."

While declining to offer more detail on the type of preparatory actions seen by threat intelligence researchers, Neuberger said officials are focused on patching known vulnerabilities at all firms that make attacks far easier for attackers than they need to be.

To further assist private sector companies in strengthening their defenses, the Biden Administration issued a fact sheet with specific guidance on protective measures. Specific recommended actions for private sector organizations include:

- Mandating the use of multifactor authentication on systems
- Deploying modern security tools that continuously look for and mitigate threats
- Working with cybersecurity professionals to ensure that organizational systems are patched and protected against all known vulnerabilities
- Changing passwords across networks so previously stolen credentials are useless to malicious actors

- Backing up data and creating offline backups
- Having emergency plans in place and ensuring those plans are practiced regularly so the business can respond quickly following a cyberattack
- Encrypting data
- Educating employees on common cyberattack strategies and encouraging them to report suspicious activity (e.g., slow or poorly behaving laptops)
- Establishing relationships with local FBI field offices or Cybersecurity and Infrastructure Security Agency (CISA) regional offices

Cybersecurity is an ongoing challenge, but organizations aren't alone when it comes to safeguarding their digital assets. Contact Bitner Henry Insurance Group to learn more about potential cyberthreats and risk mitigation tactics.