Hacked US companies to face new reporting requirements

11 March 2022, by Alan Suderman and Eric Tucker

Sen. Gary Peters, D-Mich., speaks at a news conference on Capitol Hill in Washington, Feb. 8, 2022. Companies critical to U.S. national interests will have to report when they're hacked or they pay ransomware. The new rules approved by Congress are part of a broader effort by the Biden administration and Congress to shore up the nation's cyberdefenses after a series of high-profile digital espionage campaigns and disruptive ransomware attacks. Credit: AP Photo/Andrew Harnik, File

Companies critical to U.S. national interests will now have to report when they're hacked or they pay ransomware, according to new rules approved by Congress.

The rules are part of a broader effort by the Biden administration and Congress to shore up the nation's cyberdefenses after a series of high-profile digital espionage campaigns and disruptive ransomware attacks. The reporting will give the federal government much greater visibility into hacking efforts that target private companies, which often have skipped going to the FBI or other agencies for help.

"It's clear we must take bold action to improve our online defenses," Sen. Gary Peters, a Michigan Democrat who leads the Senate Homeland Security and Government Affairs Committee and wrote the legislation, said in a statement on Friday.

The reporting requirement legislation was approved by the House and the Senate on Thursday and is expected to be signed into law by President Joe Biden soon. It requires any entity that's considered part of the nation's critical infrastructure, which includes the finance, transportation and energy sectors, to report any "substantial cyber incident" to the government within three days and any ransomware payment made within 24 hours.

Ransomware attacks, in which criminals hack targets and hold their data hostage through encryption until ransoms have been paid, have flourished in recent years. Attacks last year on the world's largest meat-packing company and the biggest U.S. fuel pipeline—which led to days of gas station shortages on the East Coast—have underscored how gangs of extortionist hackers can disrupt the economy and put lives and livelihoods at risk.

State hackers from Russia and China have had continued success hacking into and spying on U.S. targets, including critical infrastructure targets. The most notable was Russia's SolarWinds cyberespionage campaign, which was discovered at the end of 2020.

FBI Director Christopher Wray speaks at a news conference at the Justice Department in Washington Nov. 8, 2021. Companies critical to U.S. national interests will have to report when they're hacked or they pay ransomware. The new rules approved by Congress are part of a broader effort by the Biden administration and Congress to shore up the nation's cyberdefenses after a series of high-profile digital espionage campaigns and disruptive ransomware attacks. Credit: AP Photo/Andrew Harnik, File

Experts and government officials worry that Russia's war in Ukraine has increased the threat of cyberattacks against U.S. targets, by either state or proxy actors. Many ransomware operators live and work in Russia.

"As our nation rightly supports Ukraine during Russia's illegal unjustifiable assault, I am concerned the threat of Russian cyber and ransomware attacks against U.S. critical infrastructure will increase," said Sen. Rob Portman, a Republican from Ohio.

The legislation designates the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency as the lead agency to receive notices of hacks and ransomware payments. That caused concern at the FBI, which had openly campaigned for tweaks to the bill in an unusually public disagreement over legislation endorsed overall by the White House.

"We want one call to be a call to us all," FBI Director Christopher Wray said last week at a cyber event at the University of Kansas. "What's needed is not a whole bunch of different reporting but real-time access by all the people who need to have it to the same report. So that's what we're talking about—not multiple reporting chains but multiple access, multiple contemporaneous action, to the information."

The FBI also has expressed concern that liability protections that would cover companies that report a breach to CISA would not extend to reporting a breach to the FBI, an issue the bureau believes could unnecessarily complicate law enforcement efforts to respond to hacks and to aid victims.

Lawmakers who helped write the bill have pushed back against the FBI, saying the bureau's concerns about being notified of hacks and liability concerns were adequately addressed in the final version of it.

The new rules also empower CISA to subpoena companies that fail to report hacks or ransomware payments, and those that fail to comply with a subpoena could be referred to the Justice Department for investigation.