republicans-financialservices.house.gov

Cmte Financial Services (R)
Contact:

Republicans Release Report Detailing Cybersecurity Threats in the COVID-19 Era

Washington, Jan 11 -

Today, the Republican leader of the House Financial Services Committee, Patrick McHenry (NC-10), and Republican leader of the Subcommittee on Oversight and Investigations, Andy Barr (KY-06), issued a Republican staff **report** on cybersecurity in the COVID-19 era. The report found that the coronavirus pandemic and related relief programs created an environment ripe for cybercriminal activity, which threatens our financial system and American consumers.

Securing the New Normal: An Examination of Cybersecurity Issues Related to Remote Work and the Transition to a Digital Supervisory Relationship

To better understand and combat the threats cyberattacks pose to the financial system, Ranking Member McHenry introduced H.R. 4458, the Cybersecurity and Financial System Resilience Act, in September of 2019 to ensure regulators are prioritizing cybersecurity efforts. The President signed the measure into law on Dec. 27, 2020. This detailed analysis on banking regulators' efforts to protect against cyberattacks is needed now more than ever as cybercriminals continue to exploit the COVID-19 pandemic.

Read the report's Executive Summary.

The Proliferation of Malicious Cyberactivity since March 2020: Malicious actors adapted their tactics to leverage the uncertainty caused by the COVID-19 pandemic to attack individuals. Cybercrime, however, was not strictly limited to non-state actors motivated by financial interests.

In the spring of 2020, as the federal government mobilized its response to the dual health and economic crisis caused by the COVID-19 pandemic, a Russian-backed group launched what would become "one of the most sophisticated, and perhaps among the largest, attacks on federal systems in the past five years." The

extraordinary proliferation of attacks on systems with a nexus to the financial industry raised questions about how those targets were responding, and those questions remain important in light of the scope and breadth of the 2020 cyberattack on sensitive public and private sector networks. On January 5, 2021, the U.S. intelligence and cybersecurity communities stated jointly that the attack was "likely Russian in origin" and estimated approximately 18,000 public and private sector entities were compromised.

An Expedited Shift to Remote Work in the Private Sector: COVID-19 forced many private sector entities to rapidly adapt to a digital workplace. By one estimate, 31 percent of workers who were employed in early March had switched to working at home by the first week of April.

Federal Agencies Follow Suit: As the financial services industry transitioned toward a model that allowed for remote work and virtual interactions, federal regulators needed to do the same. In many cases, federal financial regulators needed a new and modernized digital infrastructure for efficient and secure digital operations. Congress should consider reforms to address the need for federal regulators to modernize their operations to accommodate what may be a permanent transition toward digital interactions.

The Ranking Member's Requests for Information: On April 17, 2020, Ranking Member McHenry issues requests to federal financial regulators and large financial institutions for documents and information pertaining to: attacks on third-party service providers; attacks on remote workers; malware attacks; denial of service activities; efforts to infiltrate, disrupt, or exfiltrate information and communications technology systems or networks; and other efforts to undermine cybersecurity. Ranking Member McHenry also sought information on steps regulators took to modernize internal and external processes, specifically with the transition to a new at-home work environment brought on by the pandemic.

The documents and information obtained by the Ranking Member show regulators and financial institutions moved quickly to implement new digitization and cybersecurity protocols; and that cybercriminals are indeed attempting to leverage the pandemic, and COVID-related phishing and hacking schemes are ongoing.

Read the Conclusion and Recommendations of the report.

Conclusion: Congress must prioritize cybersecurity oversight as remote work and virtual interactions will continue permanently in some form. The reports the Committee receives pursuant to H.R. 4458 in the summer of 2021 should form the basis for hearings and oversight initiatives throughout the 117th Congress.

The Committee should also seek testimony and information from other key stakeholders, including the community of relevant inspectors general and the private sector. Congress can use this information to strengthen the cybersecurity platforms of financial regulators and institutions in order to better protect the consumers they serve.

Read the full report.

###