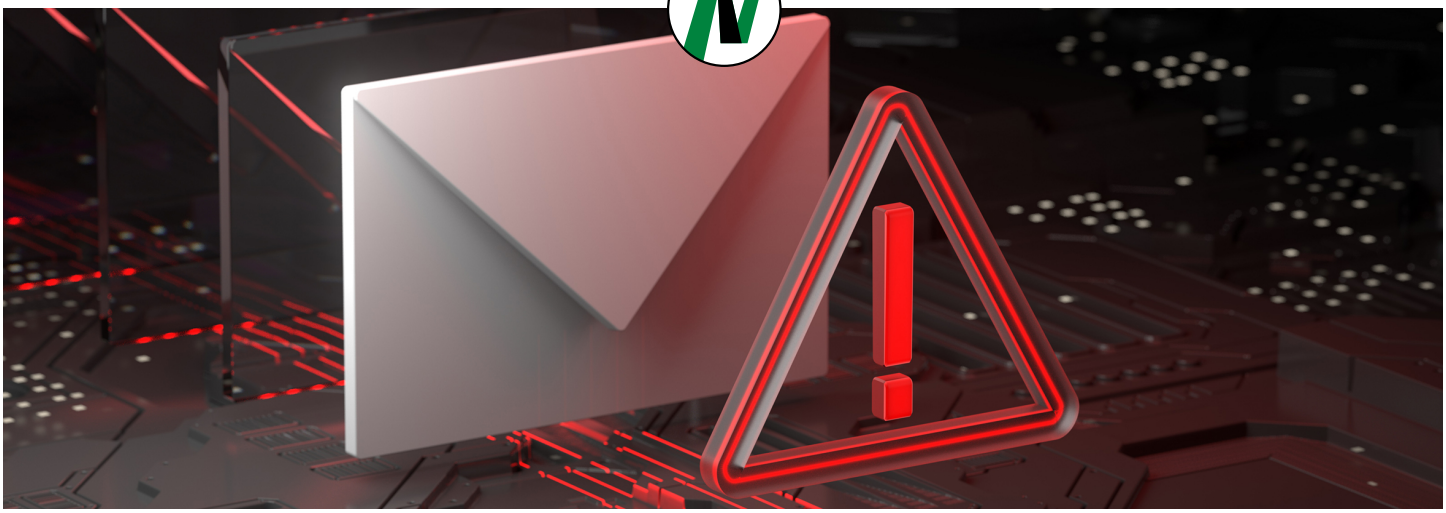

This Time They Mean "IT"!

03.11.2022 | By Hon. Chris Carney, D. Michael Stroud Jr.

In 2010, Congress held hearings that sought to understand how the Department of Homeland Security (DHS) was enforcing cybersecurity regulations on "covered" critical infrastructure (CI) providers. Congress learned that DHS was applying a rather soft touch when it came to enforcing cybersecurity regulations, preferring to "partner" with critical infrastructure providers rather than to punish noncompliance. DHS hoped compliance would be voluntary. It wasn't – at least to the extent needed to stem the tide of cyberattacks on our nation's critical infrastructure. However, in response to the multitude of ransomware attacks on CI, Congress has toughened its posture.

On March 11, 2022, the Senate voted to pass the $1.5 trillion Omnibus Spending bill, which included some of the strongest cybersecurity legislation in recent history. Division Y, the *Cyber Incident Reporting for Critical Infrastructure Act of 2022* of the Omnibus bill, creates cyberattack reporting requirements for those CI operators suffering an attack.

Assuming President Biden signs the bill into law, critical infrastructure operators will be required to report a cybersecurity event within 72 hours and a ransomware payment within 24 hours. Upon Mr. Biden's signature, the Cyber & Infrastructure Security Agency (CISA) will have no more than 24 months to publish a notice of proposed rulemaking in the Federal Register. However, most believe that because of the multitude of ransomware and other cyberattacks already occurring on CI, along with probable cyberattacks by Russia in response to the West's sanctions on Moscow over its invasion of Ukraine, CISA will begin to promulgate rules much sooner than 24 months.

Congress is Serious About Protecting National Critical Infrastructure

The legislation, which was part of the larger Strengthening American Cybersecurity Act of 2022 (SACA) package passed by the Senate, includes a number of specific provisions. For example, not only does the legislation spell out the requirements for reporting a cyberattack on CI, it also outlines the penalties for noncompliance. Essentially, if the victim of a ransomware attack pays the ransom, the victim must report the

payment to CISA within 24 hours regardless if the payment was for a covered attack. If after 72 hours there is no report, or an inadequate report, the CISA Director can issue a subpoena to compel disclosure of the attack to determine if there is a threat to economic and national security or public safety and health. If the subpoena is ignored, CISA may further refer the matter to the U.S. Attorney General where the offending entity could face civil action. But that's not all...noncompliant entities could also face debarment from federal contracts and other financial penalties as well.

This legislation also builds on the Biden administration's push to fortify the United States' supply chain. The bill contains language about the reporting of cyber incidents that impact supply chain information systems. Combined with the recent announcement of proposed disclosure changes by the U.S. Securities and Exchange Commission regarding cyber incidents, the ".com" portion of the United States marketplace will have ample reporting obligations to help focus the efforts on creating better and more secure cyber systems and supply chains.

However, because of the window of time that CISA is allowed for rulemaking and promulgation, critical infrastructure operators have an opportunity to help shape those rules.