

Cyber Reporting Law Offers Broad Safe Harbor

Media Mentions

March 28, 2022 | *SIGNAL Media* | 1 minute read | New York

Bracewell's **Seth DuCharme** told *SIGNAL Media* that a new SEC proposal for mandatory disclosure of cybersecurity incidents by publicly traded companies is the result of a growing realization that the government doesn't have good information about the exact shape and scale of the cyber problem.

US intelligence and law enforcement agencies have grown increasingly concerned about "a very high level of under-reporting" of cyber incidents, DuCharme said.

"It's hard to make policy choices, to adopt a more aggressive posture towards cyber threats, if you don't have good data about the problem," said DuCharme. "It's impossible for the government to have confidence in its strategies ... if it is suffering from an information deficit."

With the Russian invasion of Ukraine ratcheting up the cyber threat, the government was trying to put the country on "nearly a war footing" in cyberspace, he said. But without visibility into the true scope and scale of the attacks being launched, it was effectively operating in the dark. "The victim companies are the ones with the information about what happened, and if they don't come forward, the government won't get the information it needs," added DuCharme.

Attached to the omnibus spending package President Biden signed March 15, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) requires "critical infrastructure operators" to report "substantial cyber incidents" to the Homeland Security Department's Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours, and to report ransomware payments within 24 hours. CISA must now begin a rule-making process to implement the new law.

[Click here to read more from *SIGNAL Media*'s "The CyberEdge."](#)

Related People

Seth D. DuCharme

Partner

NEW YORK

+1.212.508.6165

seth.ducharme@bracewell.com

Related Industries

[Technology](#)

Related Practices

[Government Enforcement &](#)

[Investigations](#)

