CARLTON FIELDS

White House Issues Strategy Warning of Dangers to U.S. Companies from Hackers

February 21, 2013

The White House warned yesterday that hackers and "hacktivist" groups have the intent and capability to target U.S. companies and steal confidential data. A new executive strategy explains that the threat of corporate espionage and theft of intellectual property via hackers is on the rise and will pose serious threats to the economic well-being of the country unless it is curtailed.

The strategy does not draw discrete distinctions between state-sponsored hacking efforts and those of rogue groups or individuals. It does highlight the fact that foreign competitors of U.S. corporations, some with ties to foreign governments, have increased their efforts to steal trade secret information through the recruitment of current or former employees with the know-how to exploit vulnerabilities in American companies' information systems.

In its analysis, the strategy emphasizes that "there are indications that U.S. companies, law firms, academia, and financial institutions are experiencing [increased] cyber intrusion activity against electronic repositories containing trade secret information."

The White House then lays out several strategic action items to include:

1. Focusing diplomatic efforts to protect trade secrets overseas
2. Promoting voluntary best practices by private industry to protect trade secrets
3. Enhancing and increasing domestic law enforcement efforts
4. Improving domestic legislation
5. Raising public awareness and stakeholder collaboration

The release of this strategy is a significant development in the cyber security space. It clearly

demonstrates that the White House and Congress are laying the groundwork for increased regulation and legislation in this area. U.S. companies should begin to prepare for increased oversight, regulatory requirements, and increased enforcement efforts by the federal government on all matters related to cyber security and information management.

Carlton Fields has the experience and expertise to help our clients develop cyber security and information management policies and practices to meet industry standards and stay ahead of regulation. If you have any questions regarding this alert, please feel free to contact us.

Related Practices

Intellectual Property
Cybersecurity and Privacy

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.