CARLTON FIELDS

Cyber Update: What Businesses Must Know about the New Presidential Policy Directive

August 26, 2016

Last month the White House disclosed how the federal government will coordinate incident response activities in the event of a large-scale cyber incident. While the policy directive is worth reading in its entirety, this update will focus on the most important policies for private companies that face significant cyber risks. The Presidential Policy Directive on United States Cyber Incident Coordination (the "Directive") was rolled out with four documents:

1. The Directive itself;
2. A Fact Sheet, which is only slightly shorter than the Directive, that summarizes the Directive and places it in context;
3. A single-page Cyber Incident Severity Schema, to establish a common framework with the government to assess the severity of a cyber incident (which uses color codes similar to those of the now-abandoned terrorism alert system); and

4. An Annex, which provides detailed architecture for federal government coordination for significant cyber incidents, including identifying which agencies have responsibility for which "critical infrastructure sectors," or, industries.

The Administration uses such "Presidential Policy Directives" to promulgate Presidential decisions on national security matters. This Directive, number 41, is therefore intended to help identity and coordinate the response to cyber incidents with a national scope. The Directive outlines certain principles to this end, and two of them offer important clarifications to companies facing significant cyber risk. The first, "Respecting Affected Entities" states that the federal government responders to a private sector breach will "safeguard details of the incident, as well as . . . sensitive private sector information." This continues at least the Justice Department's policy, as stated over the past two years or so, that companies that are the victims of hacks will be seen as just that – victims first. Citation to this policy at the outset of a government investigation of a private sector hack could help encourage the appropriate understanding on the access and use of proprietary data and, if litigation ensures, maximize the chances of a protective order being entered. The second, "Enabling Restoration and Recovery," states that response activities will be conducted in such a way as to help the entity recover, balancing the investigation and national security interests against "the need to return to normal operations as quickly as possible." Again, while this has been part of the general practice of federal law enforcement, this Directive gives concrete, written assurance that investigation priorities will not override the affected business's need to remain operational. One instance in which this principle could prove useful to a business might be when law enforcement has asked to image an entire customer-facing server. In this vein, as explained in the Fact Sheet, the government also recognizes the importance to a private sector entity of maintaining "business or operational continuity in the event of a cyber incident" and the various response activities that a company must undertake to that end, including "communications with customers and the workforce" and "engagement with stakeholders, regulators, and oversight bodies." Under the policy, "the Federal government typically will not play a role in this line of effort, but will remain cognizant of the victim's response activities consistent with these principles and coordinate with the victim." For large cyber incidents, the Directive carves up "threat response" and "asset response" activities. "Threat response" is the law enforcement investigation, including the collection of evidence, and the FBI has been given lead responsibility in that area. The Department of Homeland Security (DHS), on the other hand, will lead "asset response," which includes, critically for a private-sector victim, "furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents." DHS will operate in this role through the National Cybersecurity and Communications Integration Center (NCCIC), which is an entity familiar to many private sector cybersecurity specialists as a source of many valuable, free resources, including those of US-CERT. The Annex, for its part, also incorporates some private-sector best practices. It requires federal agencies to conduct "cyber incident response exercises" within 180 days of the Directive, and then to conduct them "at a frequency necessary to ensure Federal agencies are prepared." It also requires that inter-agency working groups that have formed in response to an incident to afterward review the response and prepare "a report based on that review" for a presidential

committee. If a private-sector organization is not conducting such “exercises” and is not preparing post-incident reports for its leadership, it would do well to borrow from these suggestions. Read as a whole, the Directive provides important assurances for companies that have a national and international footprint and comprises an important “rules of the road” for public-private cooperation during a breach. Companies should review their data breach response plans in light of the Directive.

Authored By

John E. Clabby

Related Practices

Cybersecurity and Privacy
Intellectual Property
Technology
White Collar Crime & Government Investigations

Related Industries

Technology