Simpson Thacher

Memorandum

The Department of Justice Issues Guidance on Best Practices for Cybersecurity Preparedness

May 14, 2015

On April 29, 2015, the newly-formed Cybersecurity Unit of the Criminal Division of the Department of Justice ("DOJ") issued guidance on best practices for organizations to protect against and respond to data breaches and other cybersecurity risks.[1] As announced by Assistant Attorney General Leslie R. Caldwell at an inaugural invitation-only industry roundtable in Washington, D.C. that day, the publication will be a living document updated over time as part of the DOJ's efforts to "elevate cybersecurity efforts" and "build better channels of communication with law enforcement."[2]

The publication, titled "Best Practices for Victim Response and Reporting of Cyber Incidents," is the DOJ's first published guidance on cybersecurity. While it was drafted with smaller organizations in mind, its lessons apply to companies of all sizes. The bulk of the DOJ's guidance focuses on developing an appropriate incident response plan and executing that plan when a data breach or other cybersecurity incident occurs.[3] The DOJ also gives helpful tips on what *not* to do following a breach and exhorts companies to remain vigilant after an attack to prevent similar occurrences in the future.

---

[1] *See* Cybersecurity Unit, Computer Crime & Intellectual Property Section, Criminal Division, U.S. Dept. of Justice, *Best Practices for Victim Response and Reporting of Cyber Incidents* (April 2015). The Cybersecurity Unit was formed in December 2014 "to serve as a central hub for expert advice and legal guidance regarding how the criminal electronic surveillance and computer fraud and abuse statutes impact cybersecurity." U.S. Dept. of Justice, Cybersecurity Unit (accessed May 8, 2015).

[2] Office of Public Affairs, U.S. Dept. of Justice, *Assistant Attorney General Leslie R. Caldwell Delivers Remarks at the Criminal Division's Cybersecurity Industry Roundtable* (April 29, 2015).

[3] As explained in the Verizon 2015 Data Breach Investigations Report, a cybersecurity incident is "any event that compromises the confidentiality, integrity, or availability of an information asset," while a "data breach" is "any incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party."

I. What to Do Before a Breach Occurs

The DOJ advises organizations to develop an incident response plan now, *before* a cybersecurity incident occurs. Citing the "excellent guidance" of the Cybersecurity Framework published by the National Institute of Standards and Technology,[4] the DOJ recommends that an organization:

- Identify its "crown jewels"—its data, assets or services that merit the most protection;
- Develop, test and keep up-to-date an *actionable* incident response plan that describes specific, concrete steps the organization will take in response to a cybersecurity incident or data breach;
- Have in place (or keep readily available) the technology and tools necessary to respond to a cybersecurity incident, including data back-ups, intrusion detection capabilities and data loss prevention and filtering services;
- Monitor systems communications after obtaining users' prior consent, such as through network warnings, workplace policies or other written acknowledgements;
- Ensure it has legal counsel on hand that is well-acquainted with technology and knowledgeable about relevant privacy and cybersecurity laws;
- Maintain proper personnel and information technology ("IT") policies to minimize the risk of "insider threats";
- Establish a point-of-contact at a local federal law enforcement office, such as a Federal Bureau of Investigation ("FBI") field office; and
- Form relationships with applicable cyber information sharing organizations, such as the Information Sharing and Analysis Centers for companies engaged in sectors of critical infrastructure.

II. How to Respond to a Breach: Putting the Incident Response Plan Into Action

As detailed in the DOJ's publication, an effective incident response plan not only lays out the procedures for managing a breach, but also provides how the organization will continue to operate while responding to such breach. Once an intrusion occurs, the victim organization should:

- Assess the nature of the incident and determine whether it is a malicious act or simply a system glitch;
- Take steps to minimize ongoing damage, such as by rerouting and/or blocking network traffic and isolating some or all of the compromised network;

[4] *See* National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (February 12, 2014).

- Collect information and evidence regarding the cybersecurity incident, including making an exact copy (or "forensic image") of the affected hard disk, preserving logs of network activity, recording ongoing malicious activity and keeping detailed records of all response measures taken by the organization; and
- Notify:
  - relevant internal personnel, including senior management, IT personnel, public affairs officers and counsel;
  - law enforcement, including the FBI, Secret Service and/or the Department of Homeland Security, if criminal activity is suspected;
  - customers, in accordance with state data breach notification laws; and
  - other potential victims, such as another company whose data was also stored on the compromised network.

III. What *Not* to Do After a Breach

The DOJ counsels organizations to avoid using the compromised security network as much as possible. If an organizations must use the system, the DOJ suggests that it encrypt its communications. Finally, the victim organization should not respond to a data breach in kind by attempting to access or damage another system it suspects was involved the cyber attack.

IV. Stay Vigilant After a Breach

Lastly, the DOJ's guidance urges organizations to continue monitoring their computer systems for anomalous activity even after a cybersecurity incident seems to be under control. In addition, the DOJ recommends that a victim organization conduct a post-incident review of its response to the incident, and address any deficiencies the incident uncovered.

Conclusion

As Attorney General Loretta Lynch remarked at the April 29 roundtable, the government and private industry have "a mutual and compelling interest in developing comprehensive strategies for confronting this threat [of theft of consumer information and valuable intellectual property,] and it is imperative that our strategies evolve along with those of the hackers searching for new areas of weakness."[5] The DOJ's guidance confirms that one of the first steps in addressing these challenges is developing, maintaining and testing an incident response plan that will allow organizations to appropriately respond—and evolve—in line with

[5] Office of Public Affairs, U.S. Dept. of Justice, *Attorney General Loretta E. Lynch Delivers Remarks at the Criminal Division's Cybersecurity Industry Roundtable* (April 29, 2015).

cybersecurity threats. Moreover, an incident response plan enables an organization to respond to a potential data breach quickly, efficiently and calmly and could mitigate the impact of a breach on the company's business, including its legal exposure and reputation.

If you have any questions or would like additional information, please do not hesitate to contact any member of the Firm's Privacy and Cybersecurity Practice.

Simpson Thacher Worldwide

UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
600 Travis Street, Suite 5400
Houston, TX 77002
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
1155 F Street, N.W.
Washington, D.C. 20004
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3919 China World Tower
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Seoul
West Tower, Mirae Asset Center 1
26 Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
+82-2-6030-3800

Tokyo
Ark Hills Sengokuyama Mori Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000