[redacted]

Department of Justice Issues Best Practices Guidance on Cyber Incidents

1 Attachment, 350 KB

On Wednesday, April 29, the US Department of Justice released guidance titled "Best Practices for Victim Response and Reporting of Cyber Incidents." (See attached).

The guidance outlines steps companies should take before, during, and after an incident, and includes a summary checklist. The guidance also states the Justice Department's positions on the legal permissibility of a number of monitoring techniques and the impermissibility of many forms of so-called "hacking back."

Before an Incident

The Justice Department's guidance emphasizes the importance of planning before an incident occurs.

Specifically, the guidance states that organizations should:

- identify the company's mission-critical assets, and prioritize those items in risk management and incident response planning;
- have an actionable incident response plan;
- train relevant personnel on the plan, including through the use of regular exercises;
- acquire, install, and test appropriate technology and services;
- ensure that appropriate consent is obtained for network monitoring;
- consult with outside counsel well acquainted with cyber incident response; and
- establish information-sharing relationships.

During an Incident

During an incident, the guidance says, companies should focus on executing their plan. This includes assessing the nature and scope of the incident, preserving relevant forensic images and logs, minimizing continuing damage, maintaining detailed written records of key investigative findings and mitigation/response efforts, enabling additional logging to track ongoing attacks, and notifying relevant law enforcement agencies.

After an Incident

Following an incident, the guidance suggests, companies should remain vigilant, particularly in the event that the attempts to evict the intruder did not eliminate all of the attacker's means of access. Once the victim organization has recovered, it should initiate measures to prevent similar attacks, including a post-incident review of the organization's response to assess the strengths and weaknesses of its performance and its plan.

Implications

While the guidance appears to have been issued with an eye toward maximizing the Justice Department's ability to investigate and prosecute cyber criminals through the collection, preservation, and proper handling of relevant evidence, state and federal regulators (such as the Federal Trade Commission) may look to this guidance as a roadmap for steps companies should take in implementing "reasonable" security practices.

Additionally, the guidance makes the Justice Department's views clear with respect to the federal legal parameters surrounding cybersecurity monitoring and "hacking back."

Specifically:

- With respect to network monitoring, the guidance says that "[r]eal-time monitoring of an organization's own network is typically lawful if consent for such monitoring is obtained from network users," including through the use of log-on banners.
- The guidance further notes that installation of a "sniffer" or other network-monitoring device to record communications during an attack "is typically lawful," but the guidance suggests that companies consult with counsel to ensure monitoring is conducted lawfully.
- With respect to so-called "hacking back," the guidance makes clear that "[a] victimized organization should not attempt to access, damage, or impair another system that may appear to be involved in the intrusion or attack," because "[r]egardless of motive, doing so is likely illegal."

+ + +

Best regards,

Reed

D. Reed Freeman | WilmerHale