BRACEWELL

INSIGHTS

Justice Department Provides Cybersecurity Guidance

May 8, 2015

To listen to the podcast, please click ***here***.

In late April, the Department of Justice's Cybersecurity Unit ***provided a set of voluntary best practices*** for companies faced with the prospect of data breaches. The DOJ's best practices were expressly developed with smaller organizations in mind, and incorporate lessons learned from both federal prosecutors and private sector companies who have experienced cyber incidents. In contrast with some of the other guidance from federal regulatory agencies, the two predicates underlying the DOJ's recommendations are preparation and common sense. And because of its accessibility, expect that the DOJ's best practices will become the default standard of care for the private sector.

According to federal law enforcement agencies and regulators, it is not a matter of "if" a particular company will suffer a data breach, but "when." Compounding the issue is the nature of the threat: external hackers are actively working to circumvent a company's cybersecurity, but all too often a company's own employees cause a data breach by careless action. As such, the DOJ's best practices emphasize that the best approach is to begin planning immediately, because "[a] cyber incident is not the time to be creating emergency procedures or considering for the first time how best to respond." The DOJ's recommendations are well-grounded in common sense and should be practical for most organizations to implement and follow.

On the front-end, the key takeaways from the DOJ's guidance are that: (1) companies should identify in advance what mission critical needs they must protect (described in the best practices as their "crown jewels"); (2) companies should have actionable plans in place before intrusions occur; and (3) companies should ensure that they have the right resources – with emphasis on the right people – lined up in advance. Included among those "right people" are counsel who are accustomed to addressing issues associated with data breaches in order to reduce incident response times and leverage pre-existing relationships with forensic providers, media, and law enforcement.

Once a cyber-incident occurs, the appropriate response will always vary based on the nature of the organization, the kind of information it has, and the nature of the incident itself. However, the DOJ recommends a series of practical steps not only to mitigate the harm a cyber-incident can cause to the victim organization and others, but also to aid law enforcement in investigating, and possibly responding to, such an incident.

Each one of the DOJ's best practices may not match every company's needs, resources, or risk profile perfectly -- for example, the DOJ guidance does not reference state notification guidelines. That said, using the DOJ's best practices as a checklist to track a company's own

cybersecurity preparations and to recognize what the federal government, shareholders, and customers may come to expect would be advisable. Prudent companies should afford significant consideration to the DOJ's recommendations where practical, and should have reasoned explanations for why their own cybersecurity preparations differ from the best practices.