DEPARTMENT OF JUSTICE ISSUES GUIDANCE ON ORGANIZATIONS' RESPONSES TO CYBER INCIDENTS

Date: 12 May 2015

Government Enforcement Alert

By: Theodore L. Kornobis, Jeffrey B. Maletta, Steve Topetzes

On April 29, the Department of Justice's (DOJ) new Cybersecurity Unit within the Criminal Division issued a summary of “Best Practices for Victim Response and Reporting of Cyber Incidents” (“Best Practices”).[1] While created particularly to assist “smaller, less well resourced” organizations prepare a cyber incident response plan, this document offers insights for all organizations about what the government—and federal prosecutors in particular—may come to expect from companies that fall victim to a cyber attack.

A key takeaway is that, although cybersecurity response plans necessarily will differ among companies and should be tailored to specific entities, having a plan in place is essential. As cyber attacks grow more prevalent and online predators continue to develop innovative new ways to breach a company's defenses, entities of all sizes—from major financial institutions to small businesses—with all types of cybersecurity mechanisms should be thinking about the possibility of a breach and what they will do if that unfortunate day comes to pass. As the DOJ notes, “[t]he best time to plan such a response is now, *before* an incident occurs.” The guidance also suggests that the failure to have a plan will likely be viewed unfavorably in the event that the government conducts an inquiry into the breach.

The DOJ offers a detailed outline of actions for companies to consider; some of the key action items identified in the Best Practices summary are as follows:

1. Have an action plan in place that is understood, realistic, and tested. DOJ suggests that the cyber incident response plan should be a subject of regular personnel training and that a company should conduct exercises to identify and correct gaps and deficiencies. When a cyber incident occurs, events will necessarily move quickly. Developing and testing a response plan beforehand can significantly affect how quickly and effectively the company responds to an incident, as well as the possible legal ramifications after a breach.

2. Identify the most sensitive operations at your company (the “crown jewels,” in DOJ's parlance), so you can focus first on aspects of the company's business that need immediate protection and attention when a breach occurs. For some companies, these will be operational (the ability to communicate among employees); for others, it may be protecting the company's intellectual property or reputation (safeguarding client data).

©2005-2026 K&L Gates LLP. All Rights Reserved.

3. Ensure that appropriate technology systems are set up to help your organization mitigate and survive a breach. These will include reasonable measure for data back-up, emergency communication among key personnel and vendors, intrusion detection, and real-time monitoring of internal networks. DOJ also offers some thoughts on what it believes is the necessary legal consent for such monitoring.

4. Be prepared for the legal implications of a cybersecurity incident. Although the company targeted by a cybersecurity breach is usually the "victim" of a crime, it also is correspondingly (and unfortunately) the target of significant scrutiny into its own actions (and inactions), which can have tremendous legal and reputational repercussions. These can include lawsuits by private parties (e.g., the dozens of suits filed against Target and its officers and directors), or the government (including several recent settlements or still-pending actions involving various federal regulators). DOJ identified only a few of the many decisions that the target of a cyber attack might face: "how it interacts with government agents, the types of preventative technologies it can lawfully use, its obligation to report the loss of customer information, and its potential liability for taking specific remedial measures (or failing to do so)." Navigating the data breach laws of 47 different states, as well as applicable federal requirements, is challenging; having experienced legal counsel on hand is essential to allowing an organization to manage and contain the risks associated with any cyber incident.

DOJ also lays out some general actions that companies should take during and after an attack, including assessing the nature and scope of an incident to try to identify its cause, taking measures to minimize continuing damage (for example, by isolating the affected systems), collecting and preserving evidence of the incident (including of continuing activity), and notifying third parties, as appropriate.

Knowledgeable counsel is an important partner in each of these steps. A company should consider whether to evaluate potential responses or to conduct an internal investigation into the cause of the breach with the guidance or under the direction of counsel, securing the protection of the attorney-client privilege and work product doctrine. Counsel may engage cybersecurity consultants to provide an organization with the option of conducting pre- and post-incident assessments and responses in a confidential and privileged manner. A federal district court recently upheld a company's claim of privilege over a technology vendor's work following a cybersecurity breach, relying on the fact that the company hired the vendor through its lawyers to allow counsel to properly assess the situation and provide legal advice to the client.[2]

Similarly, deciding whether and how to notify third parties of a breach—customers, clients, law enforcement, the media—involve difficult questions that may implicate regulatory obligations and potential liability. Depending on the type of breach and the industry in which the company operates, a company may be required to make certain disclosures.

As additional regulators focus on organizations' cybersecurity readiness and offer "guidance" to companies about steps that they should take, it will become increasingly difficult for companies to defend themselves when they experience a cyber incident and do not have a responsible and speedy response. Indeed, DOJ acknowledges in its Best Practices that regulators will be looking into companies after a data breach, and several agencies have brought actions against firms with allegedly defective cybersecurity procedures or publicly announced that cybersecurity defenses and responses will be ongoing areas of attention for them.

©2005-2026 K&L Gates LLP. All Rights Reserved.

The DOJ's guidance is the latest in a series of government statements emphasizing that companies that do not already have a cybersecurity response plan should seriously consider developing one. The DOJ Best Practices document is a helpful starting point that, with the assistance of counsel and technology consultants, can be tailored to an individual business. Please contact your K&L Gates relationship manager or the contacts listed below for assistance in developing an effective cyber response plan or in responding to a cyber incident.

Notes:

[1] Department of Justice, "Best Practices for Victim Response and Reporting of Cyber Incidents," (April 2015).

[2] *See Genesco Inc. v. Visa, Inc.*, No. 3:13-cv-00202 (M.D. Tenn.).

KEY CONTACTS



THEODORE L. KORNOBIS
PARTNER

WASHINGTON, DC
+1.202.778.9180
TED.KORNOBIS@KLGATES.COM



JEFFREY B. MALETTA
GENERAL COUNSEL

WASHINGTON, DC
+1.202.778.9062
JEFFREY.MALETTA@KLGATES.COM



STEVE TOPETZES
PARTNER

WASHINGTON, DC
+1.202.778.9328
STEPHEN.TOPETZES@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.