Compliance Audits: Have a Plan and Tell the Truth!
Habeas Hard Drive | August 5, 2022

Habeas Hard Drive is a blog by Ira Victor of Discovery Technician. Find more postings at HabeasHardDrive.com

If you've been whacked hard for noncompliance, Habeas Hard Drive feels your pain. If you're up for an audit, we hope you take every step to avert the pain.

Calls to our office reflect an enforcement upswing for data security regs, as they apply to critical infrastructure. Also under scrutiny are the contractors who serve these entities. Our experience (and a hard-hitting case linked below) shows that regulators are willing to work with non-compliant parties before they arrive at punitive measures. But the errant parties must do three things – have a compliance plan, stick to the plan, and tell the truth if they deviate from the plan.

Aerojet Rocketdyne Holdings Inc. was fined $9 million after lying to the feds about certain compliance details, according to the Sacramento Bee. The Bee's report [Link: https://www.sacbee.com/news/business/article263300668.html] is only part of the story, which started with a whistleblower lawsuit. For the complete picture, we direct you to a Federal Court's denial of competing motions for summary judgment by both parties. This document [Link: https://casetext.com/case/united-states-ex-rel-markus-v-aerojet-rocketdyne-holdings-inc-6] reveals a long and messy path to the penalty and settlement with the whistleblower who called out the problems. (Many of which, it should be noted, were disputed, were not in evidence, and were omitted from the Court's consideration.)

Meanwhile, Habeas Hard Drive keeps it simple. Here are a few observations based on our work with several small and mid-sized clients facing data security compliance audits. (They are not named. We don't name our clients.)

First – they dread it. Of course they do. It's extra work and expense, to address a threat they view as abstract. Our first task is making our client understand: the threat is abstract until it's in your face. Then it's very real, and the stakes are extremely high. Possibly lethal.

Next, we look at their information governance – that is, their approach to data management. The problems in the Aerojet case sound quite familiar. A Fortune 500 company has a bigger pool of data, with more information silos, more networks, and many more technical tasks to carry out. However, adjusting for scale, the challenges are the same for even the smallest company.

After we survey the client's "inventory of information assets," we start down the path to compliance. Compliance requires regular attention to details. This could mean quarterly, weekly, or even hourly. Some tasks can be automated, but that doesn't let you off the hook. They must be monitored, and perhaps adjusted. Some tasks must be performed by a flesh-and-blood person, now not later. Pushing these to the back burner and letting them pile up – that's a compliance killer.

Overwhelmingly, most compliance officers respond well to disclosure of gaps, so long as there's a plan to close them. Sometimes they're willing to consider alternative methods. Aerojet, in fact, invoked a regulatory provision allowing a certain level of deviation, *so long as it was in writing, and approved in advance.*

Habeas Hard Drive has engaged in productive discussion with compliance officers about everything from deadlines to alternate methods that make sense for a certain kinds of business operations.

Unfortunately, we've also had clients who were too fearful to propose perfectly reasonable alternatives. This is a sad situation. We may propose an alternative because it could meet the requirement and achieve other desirable goals. It's more efficient for the business. Or more likely to prompt employee cooperation. Or because the client can't afford the method described in regulation.

Alternatives are many times not approved, but the conversation helps the regulator understand what you're up against. Honest and timely communication is key to a successful process. Above all, don't try to hide mistakes and omissions. That only makes them mad!

The above referenced case is: United States ex rel. Brian Markus v. Aerojet Rocketdyne Holdings Inc., et al., Case No. 2:15-cv-02245-WBS-AC (E.D.Cal.).