Why Did the Feds Rehire a Company Involved in the OPM Data Breach?

January 24, 2017 - It's been about a year and a half since we first reported on the data breach at the Officer of Personnel Management (OPM). The breach was one of the most damaging in American history; not because of its size - 22 million people - but because of the sensitivity of the information. The breach included biometric information on government employees and contractors with security clearances and it is widely believed that the Chinese government was behind it. Today comes word from ZDnet that the federal government has rehired an outside contractor that may have been responsible for causing the breach in the first place. We have to ask, "Why?"

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

A company by the name of Keypoint has been rehired by the federal government to process background investigations for a new government agency; the National Background Investigation Bureau. The problem is that that company has been accused on numerous occasions of exposing a list of user names and passwords which was then used to initiate the hack at OPM.

In congressional hearings to investigate the breach at OPM, the agency's director - Katherine Aruchuleta - testified that Keypoint was hacked and that there was a direct line from that attack to the OPM breach. The information stolen in the breach included 5.6 million records with digitized finger prints.

There is no doubt that the OPM was using substandard security practices for the protection of the personnel data that was being stored. But the fact that one of its private contractors was hacked indicates that their data security practices may also have been substandard. That's more than a little disturbing when you consider that the information they deal with is highly sensitive and used to issue government security clearances. Placed in the hands of a potential adversary, that information could be used to inflict great harm on the United States.

All of this brings up some very uncomfortable questions. The largest of these is, "What has Keypoint done since the OPM breach to ensure that there will be no repeats of that hack?" Unless and until that question is answered, it is our opinion that the federal government's rehiring of the firm is misguided.

byJim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow me on Twitter:

Follow ACCESS