Federal Government Data Breach Resulted in Theft of 5.6 Million Fingerprints

September 25, 2015 â€“ The data breach that occurred at the Office of Personnel Management (OPM) earlier this year continues to get worse. Not only did it include data on more than 21 million â€“ thatâ€™s about 7% of the countryâ€™s populatio one data breach â€“ but it also included digitized fingerprints on 5.6 million people. The breach takes the potential of identity theft to an entirely new level.

At this point, you may be asking, â€œWhat can you do with a stolen fingerprint?â€• As it turns out, quite a bit. More importantly, the damage that you can do with stolen fingerprints is probably more significant than with other forms of stolen data. Thatâ€™s because fingerprints are biometric data. That is, they are biological markers that identify an individual and which canâ€™t be changed. Other forms of biometric data include DNA and retinal scans.

Biometric data is considered to be one of the best options when it comes to securing data. Newer cell phones use fingerprints in place of passwords for many of their functions. Secure facilities, such as those used by defense contractors, the Pentagon and various intelligence agencies will use biometric markers such as fingerprints and retinal scans to access high security areas in their facilities. And up until this incident, most people probably considered biometric data to be highly secure. After all, for someone to steal your fingerprint, they would have to either coerce you or cut off your fingers. At least, that was the thought.

But for biometric data to be useful, it needs to be stored somewhere in digital form. Your cell phone needs to have a file to compare your fingerprint to so that it can recognize you. And any digital data can be stolen.

In this case, the fingerprints that OPM was storing included those of people with government security clearances. You donâ€™t need a degree in rocket science to figure out that with these digitized fingerprints, all the hackers need to do is identify which government systems you had access to for them to access those systems without your knowledge.

This mistakeâ€¦ and Iâ€™m being generous here because this breach may actually be a matter of criminal negligenceâ€¦ is goin to be very costly for the US government and for the people whose data was stolen.

For the government, it means having to make significant changes to systems that allow employees and government contractors to access secure systems. Not doing so would leave all of those systems exposed. And it probably means changing the way those systems are accessed for everyone, not just those who are known to have had their data

compromised.

For the people whose data was stolen in the breach, the consequences could be very high. They might include being reassigned in their jobs and restrictions on personal and business travelâ€¦ especially international travel. In some cases, it is likely to mean loss of both their security clearance and their jobs.

Frankly, there is absolutely no excuse for this data breach. The federal government continues to have an absolutely abysmal record for protecting computer systems. Yet that same government chose to store highly sensitive data on virtually every single employee and millions of civilian contractors in a single and apparently insecure database. It will be years before that actual extent of the damage can be assessed.

OPM has insisted on releasing information about the breach slowly. The way that the news has been released is akin to watching OPM management commit a slow suicide. Death by a thousand cuts. Because of this, we fully expect to see more releases of information in the not too distant future. Weâ€™ll keep our readers posted as new information is made public.
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