OPM and Breach Notifications – A Study in Execution Paralysis

Jul 25, 2015
By Ken Foster

In the continuous barrage of articles about the OPM breach, one theme continues to stand out; how to notify the victims. For those of us who are affected by the much larger second breach, we already know our highly detailed personal histories, fingerprints, and family contacts are in the wind even though we have never received formal notification. The issue that concerns me most is the Execution Paralysis at the OPM regarding this issue. For those whom have not had the pleasure of completing an SF86, it contains rich details on yourself, work histories, family, education, and friends. Since OPM seems to be in full blown Execution Paralysis regarding this issue and is well past the Federal mandated 30 day notification deadline, I submit the following recommendations as a way forward:

1. Establish a registration page for confirmed victims. Registration should require they provide a unique control number that is associated with that victim, thus validating they were impacted. Ensure the unique number is completely randomly generated using an undetectable pattern. Once registered, request they provide a preferred method of contact (e.g. email, USPS, etc…). Reassure those individuals you will keep them notified and that this is the official notification method. For individuals who are not tech savvy or do not have computers, establish a call-in line to assist them with registration. Monitor the registration web site for patterns of attack and indicators of compromise. Please do not lose their data twice!

2. Every individual whom submitted an SF86 was sponsored by an Agency or Contract Entity. Every sponsoring activity has a designed Security Officer for issues regarding background investigations. Send lists identifying impacted individuals to their last designated Security Officer and require they perform the initial notification of their sponsored individuals. Require they report their success or failure by individual within 30 days. The initial notification need only confirm they were impacted, provide the randomly generated control number associated with their record, and give both the web link and alternative toll-free number for registration.

3. For individuals no longer affiliated with originating activity as reported back by the Security Officer, cross-match those individuals via SSN to the IRS database and obtain their last known mailing address. Send those individuals a notification letter; track the success and outsource the notification failures.

4. Open a bi-weekly line of communications with those registered individuals via their identified preferred communication method. Share information on the status of the government's efforts to assist them in protecting their information and identify. Provide them advisories about scams that may be occurring regarding this incident. Provide them a tool-free number to call if they believe their data is being used for illicit means. This is how you repair the trust bridge between the affected and the agency.

5. Determine any long-term services necessary and perform those contracting requirements. Tie the unique registration number associated with the individual to the service registration process thus providing a metric to correlate the impacted to the solution. Require DHS to conduct a network security assessment of the contractor network as a condition of contract award. Require any gross misconfigurations to be fix prior to allowing them to service the impacted.

6. Once a solution is in place, use the notification site mechanism to inform the impacted how to engage the provided services. Follow up with the individuals to ensure they are successful engaging the services provided. Report the metrics regarding the impacted to congress monthly until all impacted individuals are registered, formally decline service, or they are listed as unreachable. In todays connected society, the unreachable list should be extremely small.

If you believe you were impacted by the second OPM breach and concerned that you have not been notified, consider sharing this article. If we're lucky, maybe someone in OPM management will actually read it and implement these steps.

Related Articles: http://www.bankinfosecurity.com/opm-struggles-to-notify-breach-victims-a-8411