Catching Up on the OPM Breach

krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/

I heard from many readers last week who were curious why I had not weighed in on the massive (and apparently still unfolding) data breach at the **U.S. Office of Personnel Management** (OPM). Turns out, the easiest way for a reporter to make sure everything hits the fan from a cybersecurity perspective is to take a two week vacation to the other end of the world. What follows is a timeline that helped me get my head on straight about the events that preceded this breach, followed by some analysis and links to other perspectives on the matter.

July 2014: OPM investigates a breach of its computer networks dating back to March 2014. Authorities trace the intrusion to China. OPM offers employees free credit monitoring and assures employees that no personal data appears to have been stolen.

OPM offices in Washington, DC. Image: Flickr.

Aug. 2014: It emerges that **USIS**, a background check provider for the **U.S. Department of Homeland Security**, was hacked. USIS offers 27,000 DHS employees credit monitoring through **AllClearID** (full disclosure: AllClear is an

advertiser on this blog). Investigators say Chinese are hackers responsible, and that the attackers broke in by exploiting a vulnerability in an enterprise management software product from SAP. OPM soon suspends work with USIS.

November 2014: A report (PDF) by OPM's **Office of the Inspector General** on the agency's compliance with Federal Information Security Management Act finds "significant" deficiencies in the department's IT security. The report found OPM did not maintain a comprehensive inventory of servers, databases and network devices, nor were auditors able to tell if OPM even had a vulnerability scanning program. The audit also found that multi-factor authentication (the use of a token such as a smart card, along with an access code) was not required to access OPM systems. "We believe that the volume and sensitivity of OPM systems that are operating without an active Authorization represents a material weakness in the internal control structure of the agency's IT security program," the report concluded.

Dec. 2014: **KeyPoint**, a company that took over background checks for USIS, suffers breach. OPM states that there is "no conclusive evidence to confirm sensitive information was removed from the system." OPM vows to notify 48,439 federal workers that their information may have been exposed in the attack.

Feb. 2015: Health insurance giant Anthem discloses breach impacting nearly 80 million customers. Experts later trace domains, IP addresses implicated in attack to Chinese hackers. Anthem offers two years of free credit monitoring services through AllClearID.

May 2015: Premera Blue Cross, one of the insurance carriers that participates in the Federal Employees Health Benefits Program, discloses a breach affecting 11 million customers. Federal auditors at OPM warned Premera three weeks prior to the breach that its network security procedures were inadequate. Unlike the Anthem breach, the incident at Premera exposes clinical medical information in addition to personally identifiable information. Premera offers two years of free credit monitoring through **Experian**.

May 2015: Carefirst Blue Cross discloses breach impacting 1.1 million customers. Clues unearthed by researchers point to the same attack infrastructure and methods used in the Anthem and Premera breach. Carefirst offers two years free credit monitoring through Experian.

June 2015: OPM discloses breach affecting up to 4 million federal employees, offers 18 months of free credit monitoring through **CSID**. Follow-up reports indicate that the breach may extend well beyond federal employees to individuals who applied for security clearances with the federal government.

ANALYSIS

As the OPM's Inspector General report put it, "attacks like the ones on Anthem and Premera [and OPM] are likely to increase. In these cases, the risk to Federal employees and their families will probably linger long after the free credit monitoring offered by these companies expires."

That would appear to be the understatement of the year. The OPM runs a little program called e-QIP, which processes applications for security clearances for federal agencies, including top secret and above. This bit, from a July 10, 2014 story in *The Washington Post*, puts the depth and breadth of this breach in better perspective:

> "In those files are huge treasure troves of personal data, including "applicants' financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, and names of neighbors and close friends such as college roommates and co-workers. Employees log in using their Social Security numbers."

That quote aptly explains why a nation like China might wish to hoover up data from the OPM and a network of healthcare providers that serve federal employees: If you were a state and wished to recruit foreign spies or uncover traitors within your own ranks, what sort of goldmine might this data be? Imagine having access to files that include interviews with a target's friends and acquaintances over the years, some of whom could well have shared useful information about that person's character flaws, weaknesses and proclivities.

For its part, China has steadfastly denied involvement. Politico cites a news story from the Chinese news service *Xinhua* which dismissed the U.S. allegations as "obviously another case of Washington's habitual slander against Beijing on cybersecurity."

"It also pointed to the information disclosed by former NSA subcontractor Edward Snowden, saying the U.S. itself is guilty of 'large-scale, organized cyber theft, wiretapping and supervision of political figures, enterprises and individuals of other countries, including China'," **Politico**'s **David Perera** writes.

There are some who would say it is wrong or at least foolhardy to dwell on forensic data and other clues suggesting that hackers closely allied with the Chinese government were involved in these attacks. Indeed, there is a contingent of experts who argue that placing so much emphasis on attribution in these sorts of attacks is a diversion that distracts attention and resources from what really matters: learning from one's mistakes and focusing on better securing and maintaining our critical systems.

As part of my visit to Australia (and then to gorgeous New Zealand) these past few weeks, I was invited to speak at two separate security conferences. At one of them, my talk was preceded by a speech from **Mike Burgess**, chief information security officer at **Telstra**,

Australia's largest telecom provider. Burgess knows a few things about attribution: He is an 18-year veteran of the Australian Signals Directorate (formerly the **Defence Signals Directorate** and the Australian equivalent of the **U.S. National Security Agency**).

In his speech, Burgess railed against media reports about high-profile cyber attacks that created an atmosphere of what he called "attribution distraction" and "threat distraction." A reporter with ZDNet captured Burgess's thoughts with this quote:

> "Don't get me wrong….I'm not saying that attribution isn't important. I'm not saying that issues of source, great technical intelligence, and other forms of intelligence to understand the threat and the intentions of those looking to steal information from you, or disrupt your organisation for some purpose that may be unknown to you, [are not important]."
>
> "But what I observe, what I fear, what I see too much of, is many commentators, many in the industry, and many in media, focus on attribution, with very little focus on the root cause. No-one should lose valuable information where at the root cause there is a known remedy. For me, that is unforgivable in this day and age. And I've got to tell you — my view at least — too much of this distraction around attribution takes away from focusing on what's really important here."

There is, no doubt, a great deal of wisdom in Mr. Burgess's words. After all, OPM clearly could have been doing much more to beef up security around its very sensitive stores of data. But perhaps Burgess was onto something for a different reason: At least as it relates to the United States' tenuous relations with China, having strong indicators of attribution in an attack of this magnitude puts the White House rather publicly between a rock and a hard place.

As *The New York Times* writes, the Obama administration now finds itself under pressure to respond in some way, and is reportedly considering financial sanctions against China. But as *The National Journal* wryly observes, this is a bit of an awkward position for a government that hardly holds the moral high ground when it comes to spying on and hoovering up data from foreign governments.

"That's partially because in the two years since Edward Snowden's leaks about U.S. surveillance, the Obama administration has repeatedly argued that hacking into computer networks to spy on foreigners is completely acceptable behavior," writes Brendan Sasso. "It won't be so easy for the U.S. to express indignant outrage just because it's on the opposite side of the surveillance this time."

If you're affected by these breaches and wondering what you can do to protect yourself besides signing up for credit monitoring services, please see this story.