3-Nextgov-Timeline OPM

By Aliya Sternstein and Jack Moore

June 17, 2015

A recent hearing yielded new details about how hackers were able to make off with data on millions of current and former federal employees.

Updated June 26

After no fewer than five congressional hearings and countless hours of testimony from government officials, we're learning more about the massive breach of sensitive government files at the Office of Personnel Management.

[Disappointment]

We've learned hackers first breached the Office of Personnel Management's networks in late 2013, months before the earlier timeline laid out by officials. Although that intrusion is not believed to have led to the loss of personally identifiable information, it's now believed hackers made off with IT system manuals that, officials say, could have provided a blueprint of sorts into OPM's networks and laid the groundwork for future hacks. *[Worry]*

The timeline below, first published June 17, has been extensively updated and revised. The timeline provides the key events leading up to the disclosure of the OPM mega-hack earlier this month including when intruders first breached government and contractors networks

The timeline is based on media reports, congressional testimony and other public records.

November 2013 — Hackers First Breach OPM

The earliest known malicious activity on OPM networks so far disclosed by government officials dates back to November 2013. Intruders don't make off with any personally identifiable information, but they did steal manuals about OPM IT assets, which officials said acted as a blueprint to OPM networks *[Worry]*. The malicious activity is not detected by OPM until March 2014 *[Disappointment]*.

December 2013 — Hackers First Breach Two Contractors

A month later, officials say hackers first breach two contractors involved in conducting background investigations of national security workers: USIS and KeyPoint Government Solutions. The USIS intrusion may go back even further. Andy Ozment, a top DHS cyber official, told a Senate committee June 25 the malicious activity on USIS networks dates back to April 2013. Intruders had access to both contractors' systems for months before being detected.

March 2014 — OPM First Detects Malicious Activity

OPM officials first become aware of malicious activity on its networks. Intruders didn't access PII, but they did make off with blueprints to OPM's networks. The breach is not disclosed to the public *[Disappointment]*. U.S. officials later tell reporters the attempt was thwarted, because they could not identify the loss of any personally identifiable information. *[Deny]*

May 2014 — OPM Gives USIS a Clean Bill of Health; Separate OPM Security Clearance Hack Begins

In May, OPM IT security personnel conducted a regular security review of USIS systems. The company's information security systems "met or exceeded the requirements imposed by government customers," according to cyber forensics firm Stroz Friedberg, which was retained by USIS.

Meanwhile, government investigators now say in May 2014, hackers breached a second OPM system holding information on federal employees' background checks and other security clearance information. The breach would go undetected for nearly a year *[Disappointment]*.

June 2014 — Contractor Notifies Government of Breach

USIS first detects the breach of its networks (dating back to December 2013) and notifies OPM in early June . The information is not made public *[Deny]*. In congressional testimony this year, OPM officials said the attempted breach of OPM networks and that of USIS happened around the same time.

July 9, 2014 — NY Times First Reveals Attempted OPM Hack

The New York Times publicly reveal for the first time the OPM intrusion detected by the agency in March. The article, " Chinese Hackers Pursue Key Data on U.S. Workers ," is published July 9, 2014.

OPM sent an email to federal workers later that day *[Disappointment]*. "Due to the constant monitoring systems in place at DHS and OPM, we were alerted to a potential intrusion of our network in mid-March *[Reinforce]*," according to the note, which was obtained and published by The Washington Post. OPM officials said there were no indications any employee information had been breached *[Deny]*. Later, however, officials told Congress the hackers stole manuals describing agency IT systems.

August 6, 2014 — USIS Acknowledges Breach; DHS Investigates KeyPoint Breach

Multiple media reports reveal the USIS hack for the first time. In a statement, the company says the attack "has all the markings of a state-sponsored attack *[Reinforce]*." Officials initially said the USIS breach appeared unrelated to the March 2014 attempted intrusion at OPM. Some 27,000 Department of Homeland Security employees were believed to be affected. The number later rises to more than 31,000 and includes employees at the National Geospatial-Intelligence Agency, Immigration and Customs Enforcement and the U.S. Capitol Police. OPM suspends work with USIS and later decides not to renew its contracts with the company.

Officials from the U.S. Computer Emergency Readiness Team scan networks at both USIS and KeyPoint Government Solutions. Officials detect what have been characterized as two separate breaches at KeyPoint.

One breach is estimated to affect as many 390,000 current and former DHS employees, contractors and even job applicants, who may have had their personal information exposed. It's unclear when the hackers first entered KeyPoint systems, and this breach is not disclosed to the public until a June 15 AP article . Notification letters about the breach were mailed to employees beginning in April.

[Rebuild]

August or September 2014 — Previously Undisclosed Hack at KeyPoint Contractor

Separately, another KeyPoint breach is also detected by US-CERT in either August or September 2014. Officials have offered both dates. This breach — which is the one officials can trace back to December 2013 — may have exposed the data of more than 48,000 DHS employees. Despite the similarity in timing between the two KeyPoint breaches, DHS officials have maintained that the two are separate.

October 2014 — Hackers Breach Interior Data Center

Malicious activity in OPM systems maintained in an Interior Department shared-services data centers begins. The activity is not detected until April of the following year *[Disappointment]*. This is the beginning of the breach of more than 4.2 million federal employees' personnel files.

December 2014 — OPM Alerts Employees about One of the KeyPoint Breaches

On Dec. 18, OPM alerts more than 48,000 federal employees about the potential exposure of personal information related to one of the KeyPoint breaches *[Rebuild]*. OPM officials said there wasn't conclusive evidence that hackers had made off with personally identifiable information.

April 2015 — OPM Detects Hack of Personnel Files

At some point in April, OPM officials detected the cyber intrusion of personnel files stored at the Interior Department, now believed to have begun in October. The discovery came as the agency made cybersecurity improvements, officials said. OPM officials contacted DHS and the FBI. In early May, OPM learned employees’ personal records had in fact been exfiltrated from government systems.

On April 22, government officials testified before the House Oversight and Government Reform Committee about the 2014 USIS hack. OPM CIO Donna Seymour acknowledged both USIS and OPM were attacked by hackers around the same time in March 2014, but OPM thwarted the attack and was able to “put mitigations in place to better protect the information,” she testified.

May 2015 — OPM Learns Background Check Data At Risk

In early May, an incident response team made up of DHS, the FBI and others inform OPM employees’ personal records, stored in an Interior Department shared-services data center, had in fact been exfiltrated from government systems starting in December.

Later, the investigation revealed additional systems covering background investigation data on current, former and prospective federal employees had also been breached.

June 4, 2015 — OPM Announces Massive Breach of Personnel Files

OPM publicly announces data breach of personnel data systems affecting as many as 4.2 million current and former federal employees. Some officials say those estimates undercount the true scope of the attack.

June 12, 2015 — OPM Confirms Related Breach of Background Check Files

Officials confirm a second OPM breach snared security clearance files of current, former and prospective federal employees. The data included “SF-86” forms, containing intimate details on their contacts, families and themselves. The number of people affected by the second intrusion remains unclear, officials said.

June 16, 2015 — OPM Blames Lax Security on Outdated Technology

OPM officials face a grilling at a House Oversight and Government Reform Committee hearing. OPM Director Katherine Archuleta said employees' Social Security numbers stored by OPM were not encrypted because it couldn't be done feasibly with the agency's antiquated systems.

[Anger, Disappointment, Reinforce]

Unconfirmed estimates of those affected by the data breach grew to as many as 14 million, though officials at the hearing declined to provide updated estimates and answers in open session about whether the data included information on military service members or intelligence community employees.

June 23, 2015 — OPM Says Hackers Used Contractor Credential

Amid an onslaught of congressional hearings about the breach, Archuleta reveals that hackers leveraged a compromised KeyPoint user credential to gain access to OPM's network. It's unclear how intruders netted the KeyPoint user's credential and also uncertain which breach of OPM systems the credential was subsequently used in.

Aliya Sternstein and Jack Moore contributed to this report.

Share This: