Cyber Aware

CASE STUDY

> This is crown jewel material...a gold mine for a foreign intelligence service."
>
> Joel Brenner
> *former NSA Senior Counsel*

OFFICE OF PERSONNEL MANAGEMENT

In what appeared to be a coordinated campaign to collect information on government employees, attackers stole the personnel files of 4.2 million former and current government employees and security clearance background investigation information on 21.5 million individuals. Additionally, fingerprint data for 5.6 million of these individuals was stolen. Background investigation information includes some of the most intimate and potentially embarrassing aspects of a person's life, including whether the applicant consulted with a healthcare professional regarding an emotional or mental health condition, used illegal drugs, abused alcohol, or experienced financial problems.

THE OFFICE OF PERSONNEL MANAGEMENT (OPM) is the central human resources planner for the Federal Government. OPM is responsible for the successful management of human capital across every federal agency. OPM assists federal agencies in hiring new employees, providing investigative services for background checks, and creating training programs to develop tomorrow's leaders.

Attackers were able to access OPM systems due to poor security protocols. OPM lacked an effective managerial structure to implement reliable IT security policies and didn't comply with the agency's IT security program. Implementing multi-factor authentication for employees and contractors would have thwarted continued access to the system.

MARCH 2014

The U.S. Department of Homeland Security's (DHS) United States Computer Emergency Response Team notified OPM's Computer Incident Response Team that a third party had reported data exfiltration from OPM's network.

In an effort to better understand the threat posed by the hacker, OPM monitored the adversary's movements.

During this time, the hacker removed manuals and other sensitive materials that provided a roadmap of OPM's IT environment and key users.

May 2014

While OPM monitored the first hacker, a second hacker used a contractor's OPM credentials to log into the OPM system, install malware, and create a backdoor to the network.

Two months later, OPM began monitoring the first hacker, concerned for the safety of security clearance background information. OPM kicked the first hacker off of the system, but was still unaware of the second hacker.

July 2014-March 2015

Security clearance background files, personnel files, and fingerprint data were exfiltrated.

April 2015

OPM became aware of the data breach and began an investigation to identify and isolate all malicious code.

> **[OPM data] remains a treasure trove of information that is available to the Chinese until the people represented by the information age off. There's no fixing it."**
>
> Michael Hayden | *former Director of the CIA*