U.S. Office of Personnel Management Data Breach: No Routine Hack

CASE STUDY

The U.S. Office of Personnel Management (OPM) is responsible for recruiting and retaining a world-class workforce to serve the American people and is also responsible for background investigations on prospective employees and security clearances. In June 2015, the OPM announced that it had been the target of a data breach targeting the records of as many as 4 million people. In the following months, the number of stolen records was upped to 21.5 million. This was no routine hack. Federal officials believe this data breach is among the largest breaches of government data in U.S. history

Information targeted in the breach included personally identifiable information such as social security numbers as well as names, dates and places of birth, and addresses. Also stolen was detailed security clearance-related background information. This included records of people who had undergone background checks but who were not necessarily current or former government employees.

The data breach is believed to have begun in March 2014 and perhaps earlier, but it was not noticed by the OPM until April 2015, and it is unclear how it was actually discovered. The intrusion occurred before OPM had finished implementing new security procedures that restricted remote access for network administrators and reviewed all Internet connections to the outside world.

U.S. government officials suspect that the breach was the work of Chinese hackers, although there is no proof that it was actually sponsored by the Chinese government. Chinese officials have denied involvement. The attackers had stolen user credentials from contractor KeyPoint Government Solutions to access OPM networks, most likely through social engineering. The hackers then planted malware, which installed itself within OPM's network and established a backdoor for plundering data. From there, attackers escalated their privileges to gain access to a wide range of OPM systems.

The hackers' biggest prize was probably more than 20 years of background check data on the highly sensitive 127-page Standard Forms SF-86 Questionnaire for National Security Positions. SF-86 forms contain information about family members, college roommates, foreign contacts, and psychological information. OPM systems containing information related to the background investigations of current, former, and prospective federal government employees, including U.S. military personnel, and those for whom a federal background investigation was conducted, may have been extracted. Government officials say that the exposure of security clearance information could pose a problem for years.

The Central Intelligence Agency (CIA) does not use the OPM system, and its records were protected during the breach. However, intelligence and congressional officials worried that the hackers or Chinese intelligence operatives could still use the detailed OPM information they did obtain to identify U.S. spies by process of elimination. If they combined the stolen data with other information gathered over time, they could use big data analytics to identify operatives.

The potential exposure of U.S. intelligence officers could prevent many of them from ever being posted abroad again. Adm. Michael S. Rogers, director of the National Security Agency, suggested that the personnel data could also be used to develop "spear phishing" attacks on government officials. In such attacks, victims are duped into clicking on what appear to be e-mails from people they know, allowing malware into their computer networks.

The stolen data also included 5.6 million sets of fingerprints. According to biometrics expert Ramesh Kesanupalli, this could compromise secret agents because they could be identified by their fingerprints even if their names had been changed.

The OPM had been warned multiple times of security vulnerabilities and failings. A March 2015 OPM Office of the Inspector General semiannual report to Congress mentioned persistent deficiencies in OPM's information system security program, including incomplete security authorization packages, weaknesses in testing information security controls, and inaccurate plans of action and milestones.

Security experts have stated that the biggest problem with the breach was not OPM's failure to prevent remote break-ins but the absence of mechanisms to detect outside intrusion and inadequate encryption of sensitive data. Assistant Secretary for Cybersecurity and Communications Andy Ozment pointed out that if someone has the credentials of a user on the network, then he or she can access data even if they are encrypted, so encryption in this instance would not have protected the OPM data.

OPM was saddled with outdated technology and weak management. A DHS Federal Information Security Management Act (FISMA) Audit for fiscal year 2014 and audit of the Office of the Inspector General found serious flaws in OPM's network and the way it was managed. OPM did not maintain an inventory of systems and baseline configurations, with 11 servers operating without valid authorization. The auditors could not independently verify OPM's monthly automated vulnerability scanning program for all servers. There was no senior information security specialist or chief information security officer (CISO) responsible for network security. OPM lacked an effective multifactor authentication strategy and had poor management of user rights, inadequate monitoring of multiple systems, many unpatched computers, and a decentralized and ineffective cybersecurity function. Sensitive data were unencrypted and stored in old database systems that were vulnerable. What's more, OPM used contractors in China to manage some of its databases. These deficiencies had been pointed out to OPM over and over again since a FISMA audit in 2007. OPM had the vulnerabilities, no security-oriented leadership, and a skillful and motivated adversary.

Some security experts see OPM's vulnerabilities as a sign of the times, a reflection of large volumes of data, contemporary network complexity, weak organizational and cultural practices, and a legacy of outdated and poorly written software. As Thomas Bayer, CIO at Standard & Poor's Ratings, explained, until you have a serious data breach like the OPM hack, everyone invests in other things. It's only when a massive data breach occurs that organizations focus on their infrastructure. The expertise and technology for halting or slowing down cyberattacks such as that on OPM are not a mystery, and many companies and some government organizations are effectively defending themselves against most of the risks they face.

OPM lacked leadership and accountability. The prevailing mentality was for everyone to sit and bide their time. The CEO, CIO, and CISO in a private organization would be held accountable by the board of directors.

OPM is a top-heavy organization, with a large management layer of senior advisers to the director. For example, CIO Donna Seymour has 28 staff members under her and four direct reporting organizations, none of which is security-focused. There is no listed CISO function. OPM's director has 62 senior leaders in four groups. Many OPM managers are politically appointed and lack the expertise to make informed decisions about cybersecurity. It's only when managers in an organization understand and appreciate information security risks that they will authorize their IT department to develop an effective set of controls.

Most directors in the U.S. government do not have people in their organizations with the expertise and power to make changes, and many staff members are just not right for the job. OPM director Katherine Archuleta had formerly been the National Political Director for Barak Obama's 2012 presidential reelection campaign. CIO Donna Seymour, who was supposed to advise Archuleta on how to manage risk in IT systems, was a career government employee for more than 34 years. She had some IT and management roles at the Department of Defense and other agencies and has a degree in computer science but no specific expertise in cybersecurity. It is also difficult to bring in experienced managers from the business world because federal government pay scales are so low. A chief information officer (CIO) or chief information security officer (CISO) in the federal government would probably be paid about $168,000 annually, whereas an equivalent position in the private sector would probably have annual compensation of $400,000.

Since the OPM break-in, there has been a massive effort to rectify years of poor IT management. OPM is moving toward more centralized management of security. Information system security officers (ISSOs) report directly to a CISO. These positions are filled by individuals with professional security backgrounds. OPM hired a cybersecurity advisor, Clifton Triplett, and increased its IT modernization budget from $31 million to $87 million, with another $21 million scheduled for 2016.

OPM told current and former federal employees they could have free credit monitoring for 18 months to make sure their identities had not been stolen, but it has been slapped with numerous lawsuits from victims. Seymour faces a lawsuit for her role in failing to protect millions of personal employee data files, and Archuleta had to resign.

The FBI and Department of Homeland Security released a "cyber alert" memo describing lessons learned from the OPM hack. The memo lists generally recommended security practices for OPM to adopt, including encrypting data, activating a personal firewall at agency workstations, monitoring users' online habits, and blocking potentially malicious sites. The Obama administration ordered a 30-day Cybersecurity Sprint across all agencies to try to fix the big problems. Without a strong foundation, this investment could prove futile in the long run. OPM and the federal government as a whole need to invest more in managers with IT security expertise and give those individuals real authority to act.

The Obama administration is trying to determine whether other federal agencies storing sensitive information have weak protection. An audit issued before the Chinese attacks pointed to lax security at the Internal Revenue Service, the Nuclear Regulatory Commission, the Energy Department, the Securities and Exchange Commission, and even the Department of Homeland Security, which is responsible for securing the nation's critical networks and infrastructure. Computer security failure remains across agencies even though the government has spent at least $65 billion on security since 2006.

Sources: Sean Lyngaas, "What DHS and the FBI Learned from the OPM Breach," *FCW*, January 11, 2016; Adam Rice, "Warnings, Neglect and a Massive OPM Breach," SearchSecurity.com, accessed June 15, 2016; Steve Rosenbush, "The Morning Download: Outdated Tech Infrastructure Led to Massive OPM Breach," *Wall Street Journal*, July 10, 2015; Mark Mazzette and David E. Sanger, "U.S. Fears Data Stolen by Chinese Hacker Could Identify Spies," *New York Times*, July 24, 2015; Damian Paletta and Danny Yadron, "OPM Ratches Up Estimate of Hack's Scope" *Wall Street Journal*, July 9, 2015; David E. Sanger, Nicole Perlroth, and Michael D. Shear, "Attack Gave Chinese Hackers Privileged Access to U.S. Systems," *New York Times*, June 20, 2015; and David E. Sanger and Julie Hirschfield, "Hacking Linked to China Exposes Millions of U.S. Workers," *New York Times*, June 4, 2015.

CASE STUDY QUESTIONS

8-13 List and describe the security and control weaknesses at OPM that are discussed in this case.

8-14 What management, organization, and technology factors contributed to these problems? How much was management responsible?

8-15 What was the impact of the OPM hack?

8-16 Is there a solution to this problem? Explain your answer.