Recent Attack on the US Office of Personnel Management

[Name of the Student]

[Name of the Institution]

# Recent Attack on the US Office of Personnel Management

**Introduction**

The United States Office of Personnel Management holds confidential information of the civilian workers of the country. The notorious cyberattack on the personal files kept in the office was one of the most dangerous threats to national security and privacy of workers. China was linked with the attack based on some weak justification. This incident pushed the agency to update its security system as per the best solutions possible.

**Discussion**

The US Office of Personnel Management (OPM) is an agency that operates independently under the US Federal Government and is responsible for managing the civilian workforce of the country. It is the major human resource agency that makes policies and manages issues related to the country’s civilian workforce. In April 2015, the United States OPM found that their data related to personnel files had been breached. The data files attacked by the hackers included very sensitive, confidential information related to the personnel. That information had been gathered through extensive background checks concerning people who had been looking for security clearances by the government. The data also included fingerprint records of millions of people. The data breach targeted records of more than twenty-one and a half million people whose privacy was at stake. A few reliable sources reported that the possible suspect behind the attack is China and certain government officials were cited as well. (Harvey & Evans, 2016). The hack was the worst threat to national security. Congress had to involve in the investigation. Top management executives resigned after the attack. The implications were unpredictable, unclear, and far-reaching.

Uncertainties were present in the cyber-attack on the US OPM and many facts could not be identified until the end. It could not be made clear if the attackers were from the same group or belonged to diverse backgrounds. Moreover, it could not be identified precisely how the attackers gained access to the US OPM networks. The breach has been, however, agreeably attributed to the poor security practices of the agency before the incident (Lin, 2018). Investigation showed that the agency failed to carry out important security measures. The OPM was supposed to create alerts on incoming threats of intrusion, which they did not make, being overly confident of the capability of their security systems. The two-factor authentication needed for users to access their account information had not been introduced until the attack. The hackers, regardless of the matter of how they got access to the OPM accounts, further obtained access down to the root level by using an escalation technique. They inflicted malware into the OPM’s systems which subsequently gave them remote access to the OPM’s systems. The attackers navigated through the OPM systems and stole confidential data from their servers.

China was suspected to be involved in the attack because Chinese-speaking hackers had been associated with the use of PlugX, which was installed on the OPM’s systems as a backdoor tool. However, it was merely a guess that could be falsified for lack of evidence and possible provision of counter facts. The OPM cyber-attack triggered a wide-spread debate on the credibility of the agency’s security measures (Gootman, 2016). As a result of the criticism and data loss, the agency made improvements in the system in 2015. Those improvements include double-layered security checks before log-in by customers, enabling security alerts in the systems, establishing a resource center for online security of users, and providing comprehensive protection services for applicants and non-applicants of background investigation.

**Conclusion**

The cyber-security attack on the US Office of Personnel Management was an eye-opener for the agency as well as the Federal Government. It caused the organization to revise the security measures adopted for the protection of confidential data of civilian workers. Suspecting China to have been involved in this incident has no sufficient evidence to support the claim.

References

Gootman, S. (2016). OPM hack: The most dangerous threat to the federal government today. *Journal of Applied Security Research*, *11*(4), 517–525.

Harvey, S., & Evans, D. (2016). Defending against cyber espionage: The us office of personnel management hack as a case study in information assurance. *2016 NCUR*.

Lin, Z. (2018). *“Success Is Invisible, But Failure Is Public”: Examining The US Office Of Personnel Management Data Records Breach*.