3-FedScoop-Postal Service hack

Postal Service hack raises new security questions

cyber

Postal Service hack raises new security questions

Share

Written by Jake Williams Nov 20, 2014 | FEDSCOOP

Rep. Stephen Lynch, D-Mass. (Credit: House Oversight Committee)

The Postal Service is still scrambling to assess the impact of a system breach from two months ago that put the personal information of 800,000 employees at risk, an agency executive told lawmakers Wednesday.

“We are still processing the evidence,” *[Rebuild]*Randy Miskanic, the vice president of secure digital solutions at USPS, said at a meeting of the House Oversight & Government Reform Committee’s Subcommittee for the Federal Workforce, U.S. Postal Service and the Census Wednesday. “There is still the possibility of some additional [data] compromise, specifically as it relates to some worker’s compensation files.”

In his written testimony to the committee, Miskanic, who is also in charge of the breach incident response team, reported that the at-risk files come from injury compensation claims data that is still under investigation by the Postal Service.

“Postal Service forensic investigators are conducting a thorough review of the affected databases,” *[Rebuild]* Miskanic wrote. “If the ongoing investigation determines that any additional employee information has been compromised, employees will be notified *[Rebuild]*.”

Information obtained from verbal testimony of Randy Miskanic, USPS' Vice President of Secure Digital Solutions, to the House Oversight and Reform Committee.

Even though the investigation is ongoing, Rep. Stephen Lynch, D-Mass., said the Postal Service's reasoning to wait two months to notify its customers and employees of the intrusion "doesn't fly." *[Anger]*

"The thing for me is that if someone has my Social Security number *[Anger]*, the best defense is for me to know that *[Anger, Worry]*," Lynch said. "If I don't have that information, I'm defenseless *[Worry]*. If we knew that that file had been accessed, like we knew on Sept. 11, 2014, it just raised a red flag to the people who might be vulnerable to that intrusion." *[Anger]*

However, Miskanic said, when the breach was first discovered in September, the agency did not know what data had been compromised *[Diminish]*. It wasn't until fragments of a file were recovered in October, and confirmed in early November, that the agency realized its employees' data had been compromised.

"Through that period of time, we needed to adequately reconstruct what happened to make notice to our employees," *[Diminish]* Miskanic said. "We didn't know if it was one or 800,000 [in October]." *[Diminish]*

The investigation team, which included members of the Department of Homeland Security's U.S. Computer Emergency Readiness Team and members of the FBI, discovered that the data had been taken from the network when they found that the adversary had replaced the stolen file with a new, encrypted version.

According to Miskanic, the adversary was "very sophisticated" and the attack "had been developed specifically to exploit the Postal Service computing environment." *[Diminish]* As more information came to light about the breach, investigators determined Nov. 4 that they needed to "quickly notify employees *[Rebuild]*," of the effect the intrusion would have on them.

Just shy of a week later, Postmaster General Patrick Donahoe announced the breach .

The weekend before, an internal Postal Service network was taken offline. According to spokesman David Partenheimer, by taking the systems offline, the USPS could “counter the intrusion and put new safeguards in place.” *[Disappointment]* Neither Partenheimer nor Miskanic directly said whether the USPS systems were still susceptible to the still-unnamed adversary *[Deny]*.

As of now, USPS has said the breach compromised the personal data of more than 800,000 current and former employees, and the data from more than 2.9 million customers who contacted the USPS call center. About 100 individual servers or workstations were breached — 4 percent of the agency’s total network of about 2,500 servers and more than 220,000 devices.

Although Miskanic noted that no information technology system can be completely invincible to security breaches, the Postal Service would refine its processes to better combat ever developing and high-impact cybersecurity threats *[Rebuild]*.

“This is a transformational moment in the way that the Postal Service addresses IT security,” Miskanic said. “It’s necessary for us to be more actively engaged with these emerging threats that are well-resourced and have a long time period to affect their activities *[Rebuild]*. We must remain vigilant and improve our processes to ensure that it does not [happen again]. *[Rebuild]*”

-In this Story-