washingtontimes.com

Capital One data breach tied to cloud computing vulnerability

Dan Boylan

10–13 minutes

Capital One's data breach has turned attention to an often-overlooked vulnerability in securing online information: cloud computing.

Believed to be one of the largest in banking history, the hack exposed personal details of about 106 million individuals in the U.S. and Canada, including 140,000 Social Security numbers and 80,000 bank account details from people applying for Capital One products.

According to authorities, the hacking suspect didn't directly breach the financial institution's networks but exploited a weakness in the firewall of a cloud computing firm used by Capital One to store its vast amounts of data.

The breach, privacy experts say, underscores the delicate balance the cloud computing platforms have struck between security and efficiency.

"The biggest security challenges seem to be that we can't get large corporations to protect against the simple attacks," Marty Puranik,

CEO of cloud services provider Atlantic.net, told The Washington Times.

The largest “clouds” are run by the likes of Amazon, Microsoft and Google, and store data on hard drives. While this increases the free flow of data, it also expands the potential of hackers to loot data.

The evolution of cloud security and data encryption is being driven by some of the industry’s top computer scientists, hired out of the world’s best scientific universities and the National Security Agency.

The federal government’s most secretive agencies also have publicly endorsed cloud technology, including the CIA.

According to Sean Roche, associate deputy director of the CIA’s Digital Innovation Directorate, “the cloud on its weakest day is more secure than a client service solution.”

The Pentagon is fully on board. Defense officials plan to award what is anticipated to be the government’s most expensive information technology procurement — the 10-year, $10 billion Joint Enterprise Defense Infrastructure contract for cloud computing.

But hacks and breaches continue at an alarming rate, with last year seeing what experts believe was the largest cloud data theft. That incident — at Aadhaar, India’s government ID database — compromised the identity and biometric information of roughly 1.1 billion Indians. Cyber investigators found citizens’ personal details being sold online for less than $10.

Other major breaches of late include Marriott hotels, where

hackers accessed the information of an estimated 500 million customers. Google, T-Mobile, Quora, Orbitz, Equifax and Facebook also have dealt with major breaches.

The Capital One incident has turned attention to the massive Amazon Web Services (AWS), which was used to store the bank's sensitive information. Amazon is a finalist for the Pentagon JEDI contract.

So far, Amazon has avoided being implicated as liable, with Capital One admitting the data was stolen via "a misconfigured security firewall."

The FBI on Monday arrested and charged Paige Thompson, 33, with the data hack. Ms. Thompson worked alone, according to a Department of Justice filing.

The hacker, who went by the online alias "erratic" bragged about her exploits in chat rooms, authorities said. She also worked for AWS in Seattle from 2015 to 2016.

That new wrinkle — insider information — is a formidable challenge across the industry.

"Financial Institutions need to take all the normal precautions and now a new one, where an ex-employee of their cloud hosting provider could prove to be a threat," Atlantic.net's Mr. Puranik said. "They know the intricate details of the architecture and how to exploit the small nooks and crannies for any weaknesses."