Security experts doubt North Korea hacked Sony

December 3 2014, byMartha Mendoza

Sony Pictures Entertainment headquarters in Culver City, Calif. on Tuesday, Dec. 2, 2014. The FBI has confirmed it is investigating a recent hacking attack at Sony Pictures Entertainment, which caused major internal computer problems at the film studio last week. (AP Photo/Nick Ut)

Some cybersecurity experts say it is unlikely North Korea was behind the cyberattack that crippled Sony Pictures' computers and possibly leaked unreleased movies online.

Speculation has been rampant that the hard-line communist state

sponsored last week's hack in anger over the new Sony movie "The Interview," in which Seth Rogen and James Franco play television journalists assigned by the CIA to assassinate North Korean leader Kim Jong Un.

"State-sponsored attackers don't create cool names for themselves like 'Guardians of Peace' and promote their activity to the public," said cybersecurity expert Lucas Zaichkowsky.

He said the details he has seen point instead to hacktivists, who break into computers to make a political point, often one involving the free exchange of information on the Internet. Hacktivists have targeted Sony in the past.

"The Interview" comes out on Christmas. Over the summer, North Korea warned that the release of the comedy would be an "act of war that we will never tolerate." It said the U.S. will face "merciless" retaliation.

FBI spokesman Joshua Campbell would not comment Tuesday on whether North Korea or another country was behind the attack. The FBI is investigating.

It would be unusual if North Korea was behind the breach, said Darren Hayes, director of cybersecurity at Pace University's computer science school.

"However, there are numerous hackers for hire" in some of the shadowy corners of the Internet, he said. "If Kim Jong Un has developed his own rank-and-file cyberattack unit, with sophisticated capabilities, then we should be very concerned."

Cars enter Sony Pictures Entertainment headquarters in Culver City, Calif. on Tuesday, Dec. 2, 2014. The FBI has confirmed it is investigating a recent hacking attack at Sony Pictures Entertainment, which caused major internal computer problems at the film studio last week. (AP Photo/Nick Ut)

Sony Pictures hasn't said how the hackers breached its system. But such attacks often start with "phishing" attempts, a compromised website or a malicious insider, said cybersecurity researcher Craig Young at Tripwire, a security software company that works with such businesses as Visa, Mastercard, Walmart and Starbucks.

Given that the hackers were apparently able to obtain unreleased movies as well as personnel records, Social Security numbers, passport photos, technical documents and other material, Young said it is unlikely they used just a single point of access.

"It's much more likely that attackers were able to exploit a series of

vulnerabilities, misconfigurations and poor network architecture to continuously increase their level of access over time," he said.

A security expert who was part of the South Korean government's investigation into March 2013 cyberattacks blamed on North Korea said there is not enough evidence to point the finger at the North for the Sony incident even though there are similarities.

The expert, who requested anonymity because he wasn't authorized by his employer to speak about the matter, said that when South Korean authorities concluded that Pyongyang was behind the attacks that paralyzed servers at financial institutions and media companies, they had not just malicious computer code but also IP addresses and other evidence.

"We cannot rule out the possibility that some other groups have imitated" North Korea's cyberattacks, he said.

The increased dependence on cloud technology by nearly all major businesses to store their information has made them more vulnerable, said Carson Sweet, CEO of data-protection firm CloudPassage.

Sony workers last week logged on to see a message on their computer screens that said "Hacked by #GOP," which may be the initials of a group calling itself Guardians of Peace, according to Variety.

Some unreleased Sony movies such as "Still Alice," "Annie," "Mr. Turner" and "To Write Love on Her Arms" were later distributed online, along with the still-in-theaters "Fury," though a direct connection to the hacking hasn't been confirmed.

Culver City, California-based Sony Pictures said Monday that it is still dealing with the effects of the cyberattack and is working closely with

law enforcement officials to investigate.

Sony has brought in forensic experts from the Mandiant division of FireEye, a Silicon Valley cybersecurity company, according to a person familiar with the case who spoke on condition of anonymity because the companies have not yet announced the arrangement.

Mandiant helps companies determine the extent of breaches and repair the damage. It has worked on other high-profile computer break-ins, including the one at Target last year.