U.S.News & WORLD REPORT NEWS

New Agency to Aid in Battle Against Hackers

The creation of a new cybersecurity-centered government agency echoes post-9/11 efforts to fight terrorism.

President Barack Obama speaks at a cybersecurity coordination center in January in Arlington, Va. A new government agency will work with the private sector on cybersecurity issues, the Obama administration announced Tuesday.

By Tom Risen Feb. 10, 2015 | 4:25 p.m. EST

The Obama administration on Tuesday announced a new agency tasked with coordinating the response to cybersecurity threats, aiming to take a stronger approach to combating hackers in a move similar to efforts to battle terrorism after the Sept. 11 attacks.

Data breaches suffered by companies including JPMorgan Chase, Target and Sony – as well as the most recent attack, against health insurer Anthem – have spurred President Barack Obama to call for stricter cybersecurity measures, including higher legal penalties for hackers and legislation that would facilitate the better sharing of threat information between companies and government.

The effectiveness of the new Cyber Threat Intelligence Integration Center, however, will depend on assistance from the private sector and overseas law enforcement, Lisa Monaco, assistant to the president for homeland security and counterterrorism, said Tuesday at the Woodrow Wilson International Center for Scholars in the nation's capital.

“To truly safeguard Americans online … we are going to have to work in lockstep with the private sector,” Monaco said.

The new agency will report to the Office of the Director of National Intelligence, like the National Counterterrorism Center after which it is modeled. The NCTC, formed after the attacks of 2001, is an integration and analysis center built to study terrorism-related intelligence. The new cybersecurity center will apply this same focus by reviewing intelligence collected from entities like the National Security Agency, the FBI and foreign law enforcement agencies, Monaco said.

The new agency also will bolster efforts to aid the private sector after a network attack, as the government did by sharing malware threat data with companies within 24 hours of the November attack on Sony Pictures Entertainment, Monaco said.

But businesses must still take steps to defend themselves, she said, calling for “better cyberhygiene” in corporate culture. Typical steps businesses can take to protect user data and trade secrets include encouraging employees to avoid links in suspicious emails and to create stronger passwords.

“The private sector cannot and should not rely on the government to solve all its cybersecurity problems,” Monaco said.

A lack of network vigilance by companies is a major gap in America’s cyberthreat defenses. PricewaterhouseCoopers’ 2014 U.S. State of Cybercrime Survey revealed that many American companies had not taken important steps to protect themselves. What's more, nearly half of U.S. adults had personal information stolen during late 2013 and early 2014, according to a separate study by cybersecurity research firm the Ponemon Institute.

Better information-sharing between companies and the government about online attacks and network defenses is a concept that has the support of both Congress and the Obama administration, but bills on the topic in recent years have failed in part due to privacy concerns regarding company data that could wind up in the hands of government intelligence agencies.

“We need to share information more broadly … [and] respond more quickly to threats,” Monaco said, adding that “we have to do so consistent with fundamental values” like privacy and civil liberties.

Obama will further address the need to balance security and privacy Friday during a White House summit on cybersecurity and consumer protection held at Stanford University in California.

Some cybersecurity analysts called the new agency an overdue bureaucratic change. The primary purpose of the center “is to make sure we have a more complete picture of what is going on” when a major U.S. network is hacked, says Jim Lewis, a cybersecurity researcher at the Center for Strategic and International Studies.

“When the White House picks up the phone and wants to know the latest on a hack, they know who to call,” Lewis says.

The existing U.S. Cyber Command protects Defense Department networks, but “that cyber defense only fences off a portion of our society,” says Patrick Cronin, a senior adviser at the Center for a New American Security.

The new agency will be a positive change to help protect civilian systems, although expanding the government often raises questions about whether more bureaucracy is the answer, Cronin observes.

"We will learn more about whether the new center is effective, how it works within our existing bureaucratic arena, how it works with allies and partners overseas, how it balances security with domestic laws and rights, and how well it spends public money," Cronin says.

While recognizing the need for privacy and encryption efforts at tech companies like Apple and Google, Monaco also reasserted Obama’s call for a conversation among the American people on how the government can use as much data as possible to track and arrest hackers.

Google and Apple each said last year that they would encrypt their smartphones so they could not be compelled by law enforcement to unlock information stored on the devices, raising concerns from both FBI Director James Comey and Obama about whether that would hinder law enforcement investigations.

“Those who would do us harm should know that they can be found and they will be held to account,” Monaco said.

http://www.usnews.com/news/articles/2015/02/10/new-cybersecurity-agency-to-aid-in-battle-against-hackers?int=9e2d08