LIGHT FOR ALL
THE SUN
www.baltimoresun.com

Obama order allows sharing of data on cyberattacks

By Ian Duncan

February 13, 2015

President Barack Obama, appearing Friday at a summit on computer security, signed an executive order to make it easier for businesses to peer into the government's deep reservoirs of data on cyberattacks — the latest attempt to draw the private and public sectors together against what officials describe as an unrelenting assault on the nation's computer networks.

"This summit is an example of what we need more of," Obama told a gathering of Silicon Valley leaders at Stanford University, "all of us working together to do what none of us can achieve alone."

After the high-profile hack last year of Sony Picture's Entertainment, officials have looked for ways to step up the fight against hackers acting to aid hostile regimes, to make money for criminal gangs or merely for their own amusement.

But there is considerable disagreement about how the government should respond to what has emerged over the past decade as a new kind of threat.

Even simple definitions are in dispute: Obama called the attack on Sony an act of vandalism, but Adm. Michael S. Rogers, head of the National Security Agency, has said the decision to publicly name North Korea as the attack's sponsor came from the nuclear deterrence playbook.

This week, the Obama administration landed somewhere in between, proposing the fight against terrorism after the attacks of Sept. 11, 2001, as a model. Obama announced the formation of a new center to coordinate the government response to cyberattacks, patterned after an agency established after Sept. 11 to coordinate intelligence on terrorism.

"Cybersecurity, like terrorism, requires a sustained effort to meet what is a constantly changing, a constantly evolving enemy," Lisa Monaco, the president's homeland security adviser, said Friday at the Stanford summit.

Federal intelligence and law enforcement agencies have much information that could be useful to protect computer networks, but freeing them to share it with the private businesses often targeted for attack has proved a challenge.

Sherri Ramsay, a former director of the NSA's threat analysis unit at Fort Meade, said it has gained "considerable insight" into risks in cyberspace. And in the past five years, the agency has increasingly been sharing information, Ramsay said in an interview before Obama announced his executive action.

After the Sony attack, Monaco said, the NSA was pushing out information in as little as 24 hours.

"That is a role that the NSA can and should fill," said Ramsay, who now works at the Baltimore security company CyberPoint International.

But the agency still faces legal obstacles to turning over classified information.

The executive order might ease some of those problems, said Julian Sanchez a fellow at the libertarian Cato Institute. But getting secretive government bodies to share more will likely remain a challenge.

"You hoard information," Sanchez said. "That's just baked into the DNA of an intelligence agency."

The White House announced the creation of a cyber information-sharing center earlier this week. Part of the Office of the Director of National Intelligence, the new organization is designed to apply the lessons learned in a decade of fighting al Qaeda to computer security.

Monaco said the government does not currently have a clearinghouse for gathering and analyzing cyber information from across the agencies. The new center — named the Cyber Threat Intelligence Integration Center, or CTIIC — is intended to fill that gap.

The Obama administration is also seeking ways to encourage private companies, which control most of the nation's Internet infrastructure, to share information with the government.

While intelligence agencies have driven the fight against terrorism, their ability to protect computer networks is limited. Monaco acknowledged that when she announced the creation of the new sharing center.

"The private sector plays a more central role in spotting and responding to cyber incidents than it does in the counterterrorism realm," she said.

Some corporations are leery of collaborating with the government after revelations about the NSA's data-collection programs by former contractor Edward J. Snowden. They fear they could face legal action if they turn over records containing customers' personal information.

Privacy groups, meanwhile, warn that closer communication between government and businesses will give the nation's spies a new way to gather more information.

Obama acknowledged those concerns in his speech Friday.

"Grappling with how government protects the American people from adverse events while at the same time making sure the government itself is not abusing its capabilities is hard," he said.

The executive order he signed does not address legal liability for businesses that share customers' information with the government. The White House has proposed legislation that officials say would address liability and privacy.

Some computer security researchers say the attention placed on government action is misplaced.

A recent study by the Online Trust Alliance, a nonprofit group, estimated that 90 percent of data breaches recorded in the first half of last year could have been prevented with basic security measures and education of employees.

Matthew D. Green, a research professor at the Johns Hopkins Information Security Institute, said government initiatives proposed so far are unlikely to help much and could hurt if they undermine encryption tools that scramble sensitive data to protect it.

"We live in a town where everyone is leaving their doors unlocked," said Green, a cryptographer. "The solution is to start locking the doors, not to put together a new government agency to monitor the Internet."