

USA
TODAY

Money

SECTION B

MONEY.USATODAY.COM

WEDNESDAY, JUNE 15, 2011

Disclosures of cyberattacks timely

News released as new law is sought

By Byron Acohido
USA TODAY

The recent rash of disclosures about cyberspying comes as the White House is making its third attempt to push through a historic federal cybersecurity law.

The timing is no coincidence, some cybersecurity analysts say. After two previous bills went nowhere, the White House needs to garner public support for a new law that could equip America for cyberwarfare.

"The best way to do that is to get folks worried that we're under attack from some foreign state like China or North Korea," says Ed Adams, CEO of Security Innovation, which integrates security systems for government agencies.

Recent disclosures of cyberattacks against the International Monetary Fund, Google and several defense contractors coincided with an unprecedented pronouncement last week by CIA Director Leon Panetta, who warned a U.S. Senate panel that the U.S. needs to take "defensive measures as well as aggressive measures" to win at cyberwarfare.

The bill is gaining bipartisan support in Congress. It would establish a framework for distributing billions

of dollars for new cybersecurity systems, while placing responsibility for securing cyberspace with the Department of Homeland Security.

In an essay Tuesday in *The Hill*, Rep. Jim Langevin, D-R.I., the bill's chief sponsor, underscored the need to engage Americans "in a continuous dialogue about threats we face and steps taken to protect them."

In that vein, the FBI will help investigate what's believed to be the theft of e-mails and other documents related to the IMF's role in stabilizing currency exchange rates and keeping global trade in balance.

"This is part of a wave of economic espionage putting additional pressure on the U.S. economy," says Alan Paller, research director at SANS In-

stitute, a cybersecurity think tank.

Google recently revealed that hackers pilfered information from the Gmail accounts of hundreds of high-profile individuals, including U.S. government officials. "The dialogue around cybersecurity has definitely become politicized and militarized," says Dave Jevans, chairman of security firm IronKey.

By pinpointing Jinan, China, as the origination point of the Gmail hack, Google "elevated the awareness of the enemy," says Harry Sverdlove, chief technology officer at security firm Bit9. "That could influence both the cybersecurity bill ... (and) the rules of engagement for cyberwarfare being debated by the Pentagon," he says.