THE HOMELAND SECURITY *NEWS CLIPS*

PREPARED FOR THE DEPARTMENT OF HOMELAND SECURITY BY BULLETIN NEWS WWW.BULLETINNEWS.COM/DHS

TO: THE SECRETARY AND SENIOR STAFF

DATE: THURSDAY, SEPTEMBER 15, 2011 7:00 AM EDT

TODAY'S EDITION

[redacted]

[redacted]

[redacted]

Financial Industry Especially Vulnerable To Cyberattacks, Analysts Say (NATJO)

By Josh Smith

National Journal Daily, September 15, 2011

Cybercrime is costing the world billions of dollars and current laws aren't enough to stop the loss of money and information, government and industry witnesses told a House subcommittee on Wednesday.

Cyberattacks may not kill people, but officials say there is little doubt about their potential to harm financial and economic systems.

"Cyberattacks have become big business, with extraordinary returns on investment; for example, botnets are both economical and flexible for creating cybereffects at scale, including attacks on financial institutions and their customers, which yield high payouts," Greg Shannon, chief scientist for the computer emergency response team at Carnegie Mellon University, told the House Financial Institutions and Consumer Credit Subcommittee.

Limits in technical protections against cyberattacks have led to the "steady corporatization" of cyberthreats, he said.

Cybercrime costs businesses, governments, and others an estimated $114 billion every year globally, according to Symantec, with billions more lost because of wasted time and other impacts of the attacks.

In a Sept. 2 security bulletin, the Homeland Security Department warned that the hacker group Anonymous has been using social media to ask employees at financial institutions for help gaining access to their networks.

"In the current technological environment, there are growing avenues for cybercrimes against the U.S. financial infrastructure and consumers," Gordon Snow, assistant director of the FBI said in testimony. "Modifications to business and financial-institution security and risk-management practices will directly affect the future of these types of crimes, and the adoption of best practices may be negated by the lack of security-conscious behavior by customers.

He cited the Obama administration's National Strategy for Trusted Identities in Cyberspace, which aims to create more trustworthy credentials for online transactions.

But any efforts to develop authentication for financial transactions have the added risk of gathering and storing even more personal information, said Marc Rotenberg, president of the Electronic Privacy Information Center. Instead of biographical data, such as birth dates or Social Security numbers, financial institutions need to develop more consumer-set passwords, thereby limiting the potential for lost information in addition to lost money, he said.

"In our view, none of the current legal frameworks provide adequate safeguards for consumers, bank customers, depositors, and others who provide personal information to obtain financial services," Rotenberg told the subcommittee.

At a hearing of a House Commerce subcommittee scheduled for Thursday, Chairwoman Mary Bono Mack, R-Calif., plans to examine the relationship between European and U.S. privacy regulations. She has pushed for legislation to limit the impact of data breaches during cyberattacks.

In addition to the money stolen, financial institutions and the larger economy are vulnerable to attacks on infrastructure, which are increasingly linked to global networks, said Greg Schaffer, acting deputy undersecretary at DHS.

"Because financial institutions are critical to the nation's economic security and handle large sums of money, malicious actors find them to be especially attractive targets," Schaffer said. "There are also risk considerations associated with the banking and finance sector's dependencies on other critical infrastructure sectors. In simple terms, financial transactions would be significantly impacted by massive power outages or failures of U.S. communications services."

[redacted]