SEC SAYS HACKERS LIKE NSA ARE BIGGEST THREAT TO GLOBAL FINANCIAL SYSTEM

Reuters reports that, in the wake of criminals hacking the global financial messaging system SWIFT both via the Bangladesh central and an as-yet unnamed second central bank, SEC Commissioner Mary Jo White identified vulnerability to hackers as the top threat to the global financial system.

> Cyber security is the biggest risk facing the financial system, the chair of the U.S. Securities and Exchange Commission (SEC) said on Tuesday, in one of the frankest assessments yet of the threat to Wall Street from digital attacks.
>
> Banks around the world have been rattled by a $81 million cyber theft from the Bangladesh central bank that was funneled through SWIFT, a member-owned industry cooperative that handles the bulk of cross-border payment instructions between banks.
>
> The SEC, which regulates securities markets, has found some major exchanges, dark pools and clearing houses did not have cyber policies in place that matched the sort of risks they faced, SEC Chair Mary Jo White told the Reuters Financial Regulation Summit in Washington D.C.
>
> “What we found, as a general matter so far, is a lot of preparedness, a lot of awareness but also their policies and procedures are not tailored to their particular risks,” she said.
>
> “As we go out there now, we are pointing

> that out."

Of course, the criminals in Bangladesh were not the first known hackers of SWIFT. The documents leaked by Snowden revealed NSA's elite hacking group, TAO, had targeted SWIFT as well. Given the timing, it appears they did so to prove to the Europeans and SWIFT that the fairly moderate limitations being demanded by the Europeans should not limit their "front door" access.

Targeting SWIFT (and credit card companies) is probably not the only financial hacking NSA has done. One of the most curious recommendations in the President's Review Group, after all, was that "governments" (including the one its report addressed, the US?) might hack financial institutions to change the balances in financial accounts.

> (2) Governments should not use their offensive cyber capabilities to change the amounts held in financial accounts or otherwise manipulate the financial systems;
>
> Second, governments should abstain from penetrating the systems of financial institutions and changing the amounts held in accounts there. The policy of avoiding tampering with account balances in financial institutions is part of a broader US policy of abstaining from manipulation of the financial system. These policies support economic growth by allowing all actors to rely on the accuracy of financial statements without the need for costly re-verification of account balances. This sort of attack could cause damaging uncertainty in financial markets, as well as create a risk of escalating counter-attacks against a nation that began such an effort. The US Government should affirm this policy as an international norm, and incorporate the policy into free

> trade or other international agreements.

After which point, James Clapper started pointing to similar attacks as a major global threat.

I don’t mean to diminish the seriousness of the threat (though I still believe banksters’ own recklessness is a bigger threat to the world financial system). But the NSA should have thought about the norms they were setting and the impact similar attacks done by other actors would have, before they pioneered such hacks in the first place.