IF A TBTF BANK LOST ITS QUANT CODE TO CHINESE HACKERS AND NO ONE KNEW, WOULD WE STILL HAVE A FUNCTIONING MARKET?

Bloomberg has an excellent catch from the HB Gary emails, revealing that Morgan Stanley was one of the 20-200 companies targeted by the Chinese-based Aurora hack in 2009.

> Morgan Stanley experienced a “very sensitive” break-in to its network by the same China-based hackers who attacked Google Inc.’s computers more than a year ago, according to e-mails stolen from a cyber-security company working for the bank.
>
> The e-mails from the Sacramento, California-based computer security firm HBGary Inc., which identify the first financial institution targeted in the series of attacks, said the bank considered details of the intrusion a closely guarded secret.
>
> “They were hit hard by the real Aurora attacks (not the crap in the news),” wrote Phil Wallisch, a senior security engineer at HBGary, who said he read an internal Morgan Stanley report detailing the so-called Operation Aurora attacks.

As McAfee made clear when it first announced the hack, the hackers were after the targets’ intellectual property (though note the understanding of the timing of the hack has changed).

> Similar to the ATM heist of 2009, Operation Aurora looks to be a

> coordinated attack on many high profile companies targeting their intellectual property. Like an army of mules withdrawing funds from an ATM, this malware enabled the attackers to quietly suck the crown jewels out of many companies while people were off enjoying their December holidays.

Now, Bloomberg—with backing from an FBI officer and a reminder that Morgan Stanley is the world's larger mergers and acquisitions adviser—seems to be most concerned about what the hackers learned about impending M&A.

> FBI Deputy Assistant Director Steven Chabinsky said that hackers have increasingly targeted information related to mergers and acquisitions, data that can give companies involved an advantage in negotiations.

But the description of the targeted information as IP immediately made me think about quant code, the algorithms that banks use to conduct high frequency trading. When Sergey Aleynikov attempted to sell Goldman Sachs' high frequency trading code, the Goldman and the government treated it like a capital offense. For good reason, because if another firm got that code, it would be able to game out Goldman's moves. So how do we know that these hackers didn't steal MS' quant code?

In any case, the hack seems to raise real questions about disclosure. Should Morgan Stanley have had to reveal this to its stockholders and potential M&A clients (remember that MS led GM's IPO last year, though hopefully long enough after this hack for the merger not to be exposed by it). Should MS have had to reveal this—with the potential implications for markets—to Congress? Did it?

I just can't help but think that the Aurora hackers may well have gotten the same kind of

information that Congressional oversight committees have requested from the Fed, but were refused.