HOW DOES DUTY TO WARN EXTEND TO CYBERATTACKS?

Steve Aftergood has posted a new directive from James Clapper mandating that Intelligence Community members warn individuals (be they corporate or natural persons) of a threat of death of seriously bodily harm.

> This Directive establishes in policy a consistent, coordinated approach for how the Intelligence Community (IC) will provide warning regarding threats to specific individuals or groups of intentional killing, serious bodily injury, and kidnapping.

The fine print on it is quite interesting. For example, if you're a drug dealer, someone involved in violent crime, or you're at risk solely because you're involved in an insurgency, the IC is not obliged to give you notice. Remember, the FBI did not alert members of Occupy Wall Street someone was plotting to assassinate them. Did they (then) not do so because they considered Occupy an "insurgency"? Would they consider them as one going forward?

But I'm most interested in what this should mean for hacking.

Here's how the directive defines "seriously bodily harm."

> Serious Bodily Injury means an injury which creates a substantial risk of death or which causes serious, permanent disfigurement or impairment.

As I have noted, NSA has secretly defined "serious bodily harm" to include threat to property — that is, threats to property constitute threats of bodily harm.

If so, a serious hack would represent a threat of bodily harm (and under NSA's minimization procedures they could share this data). While much of the rest of the Directive talks about how to accomplish this bureaucratically (and the sources and methods excuses for not giving notice), this should suggest that if a company like Sony is at risk of a major hack, NSA would have to tell it (and the Directive states that the obligation applies for US persons and non-US persons, though Sony is in this context a US person).

So shouldn't this amount to a mandate for cybersharing, all without the legal immunity offered corporations under CISA?