FRONTLINE IGNORES MOST EMBARRASSING "CAUSE" OF WIKILEAKS LEAK

Greg Mitchell has a preview of the Frontline piece on Bradley Manning today. He points out that the big "scoop" of the story—that Manning's stepmother called the cops in 2006 after Bradley pulled out a knife during a family fight (but then immediately asked if his dad was okay).

The entire story seems to look to Manning's psychology to explain his alleged leak of classified information.

> *Frontline* says it will continue its report in May in a one-hour program which will, again, focus on Manning's personal life and how this "led" to his alleged leak; and his new outbursts, this time in the Army (all reported elsewhere)—and how the Army still gave him access to top-secret documents.
>
> [snip]
>
> The overall tone of tonight's report is sure to spark debate. Consider that *MilitaryTimes* opens its report today with this: "Could the global turmoil sparked by Wikileaks have started started with a son's anger for his father?" NPR's report is headlined: "Home Life Included a 911 Call."

Such spin, in the absence of a larger examination of what "led to" the alleged leak, is irresponsible.

If Manning is found to have leaked the cables, he deserves the bulk of responsibility for the leak (though, as Mitchell points out, to explain it, it'd be well to look at his political views and, I'd add, the disclosure requirements for

crimes like support for torture exposed in WikiLeaks as well).

But one entity that has thus far avoided all responsibility for the leak are the folks in charge of DOD's IT. As I have pointed out, DOD's network security was embarrassingly bad—worse than your average mid-sized corporation. But to make their negligent security even worse, they had already suffered a damaging compromise of their systems when, in 2008, malware was introduced into their system via removable media, the same means by which Manning is alleged to have downloaded the WikiLeaks cables.

> The Defense Department's geeks are spooked by a rapidly spreading worm crawling across their networks. So they've suspended the use of so-called thumb drives, CDs, flash media cards, and all other removable data storage devices from their nets, to try to keep the worm from multiplying any further.
>
> The ban comes from the commander of U.S. Strategic Command, according to an internal Army e-mail. It applies to both the secret SIPR and unclassified NIPR nets. The suspension, which includes everything from external hard drives to "floppy disks," is supposed to take effect "immediately."
>
> [snip]
>
> Servicemembers are supposed to "cease usage of all USB storage media until the USB devices are properly scanned and determined to be free of malware," one e-mail notes.
>
> Eventually, some government-approved drives will be allowed back under certain "mission-critical," but unclassified, circumstances. "Personally owned or non-authorized devices" are "prohibited" from here on out.

Not only did DOD's failure to do what it claimed it would in response to this malware attack expose DOD's networks to the kind of leak Manning is alleged to have committed, but it also exposed DOD's networks to more secret, but potentially more damaging, leaks of targeted information that our enemies would like. The failure to implement the very minimal response to the malware attack is inexcusable.

But, as far as I know, no one is asking anyone be held responsible for that negligence.

None of this excuses what Manning is alleged to have done in the least. But shouldn't the press be asking why DOD persisted with completely inadequate security after having been attacked already?

Update: "Stepmother" fixed.