DOD PROMISES TO DEFEND THE NETWORKS THEY FAILED TO DEFEND AFTER 2008

There's something hysterical about the promise a Quantico spokesperson made that DOD would take any threats to its IT networks—in this case, threats made by Anonymous—seriously.

> A Quantico spokesman, Lieutenant Agustin Solivan, said officials had referred the matter to law enforcement and counter-intelligence agencies. "We are aware of the threat and any threats to defence department information systems and networks are taken seriously," he said. "The intent or stating that you are going to commit a crime is a crime in itself," he added.

You see, back in 2008, DOD got badly hit by malware introduced via a thumb drive or some other removable media. And in response, DOD instituted measures that—it said—would clear up the problem.

> 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.

In other words, back in 2008, an enemy force attacked DOD’s IT system using an embarrassing security vulnerability. In response DOD immediately banned all removable media. That ban was supposed to be permanent on classified networks like SIPRNet.

Just over one year later, a low-ranking intelligence analyst in Iraq brought in a Lady Gaga CD, inserted it into his computer attached to SPIRNet, and allegedly downloaded three huge databases of classified information.

Throughout the WikiLeaks scandal, DOD has been the functional equivalent of someone who, just weeks after getting cured of syphilis, went right back to his old ways and—surprise surprise!—got the clap, all the while denying he bore any responsibility for fucking around.

According to Bradley Manning’s description, there was a virtual orgy of IT security problems at his base in Iraq.

> (01:52:30 PM) Manning: funny thing is… we transffered so much data on unmarked CDs…
>
> (01:52:42 PM) Manning: everyone did… videos… movies… music
>
> (01:53:05 PM) Manning: all out in the open

> (01:53:53 PM) Manning: bringing CDs too and from the networks was/is a common phenomeon
>
> (01:54:14 PM) Lamo: is that how you got the cables out?
>
> (01:54:28 PM) Manning: perhaps
>
> (01:54:42 PM) Manning: i would come in with music on a CD-RW
>
> (01:55:21 PM) Manning: labelled with something like “Lady Gaga”… erase the music… then write a compressed split file
>
> (01:55:46 PM) Manning: no-one suspected a thing
>
> (01:55:48 PM) Manning: =L kind of sad
>
> (01:56:04 PM) Lamo: and odds are, they never will
>
> (01:56:07 PM) Manning: i didnt even have to hide anything
>
> (01:56:36 PM) Lamo: from a professional perspective, i’m curious how the server they were on was insecure
>
> (01:57:19 PM) Manning: you had people working 14 hours a day… every single day… no weekends… no recreation…
>
> (01:57:27 PM) Manning: people stopped caring after 3 weeks
>
> (01:57:44 PM) Lamo: i mean, technically speaking
>
> (01:57:51 PM) Lamo: or was it physical
>
> (01:57:52 PM) Manning: >nod<
>
> (01:58:16 PM) Manning: there was no physical security
>
> (01:58:18 PM) Lamo: it was physical access, wasn’t it
>
> (01:58:20 PM) Lamo: hah

> (01:58:33 PM) Manning: it was there, but not really
>
> (01:58:51 PM) Manning: 5 digit cipher lock… but you could knock and the door…
>
> (01:58:55 PM) Manning: *on
>
> (01:59:15 PM) Manning: weapons, but everyone has weapons
>
> (02:00:12 PM) Manning: everyone just sat at their workstations… watching music videos / car chases / buildings exploding… and writing more stuff to CD/DVD… the culture fed opportunities

Incidentally, note that no one has been fired for having left SIPRNet open to the same vulnerability that had already been targeted in a hostile attack? It's all Bradley Manning's fault. Sure, DOD was fucking around. But it can't be held responsible!

So now, weeks after HBGary emails made it clear that DOD and DOJ and CIA were already investigating Anonymous, they're telling us they're investigating. For real now.

And don't you worry! Ain't no way Anonymous can hurt them. Because they know how to defend against such threats.