Cyber Briefings 'Scare The Bejeezus' Out Of CEOs

by Tom Gjelten

- May 9, 2012

For the CEOs of companies such as Dell and Hewlett-Packard, talk of cyberweapons and cyberwar could have been abstract. But at a classified security briefing in spring 2010, it suddenly became quite real.

"We can turn your computer into a brick," U.S. officials told the startled executives, according to a participant in the meeting.

The warning came during a discussion of emerging cyberthreats at a secret session hosted by the office of the Director of National Intelligence and the departments of Defense and Homeland Security, along with Gen. Keith Alexander, head of the U.S. military's Cyber Command.

The meeting was part of a public-private partnership dubbed the "Enduring Security Framework" that was launched at the end of 2008. The initiative brings chief executives from top technology and defense companies to Washington, D.C., two or three times a year for classified briefings. The purpose is to share information about the latest developments in cyberwarfare capabilities, highlighting the cyberweapons that could be used against the executives' own companies.

"We scare the bejeezus out of them," says one U.S. government participant.

The hope is that the executives, who are given a special one-day, top-secret security clearance, will go back to their companies and order steps to deal with the vulnerabilities that have been pointed out.

"I personally know of one CEO for whom it was a life-changing experience," says Richard Bejtlich, chief security officer for Mandiant, a cybersecurity firm. "Gen. Alexander sat him down and told him what was going on. This particular CEO, in my opinion, should have known [about the cyberthreats] but did not, and now it has colored everything about the way he thinks about this problem."

The Virtual Tools Of War

Among the computer attack tools discussed during the briefings are some of the cyberweapons developed by the National Security Agency and the Cyber Command for use against U.S. adversaries. Military and intelligence officials are normally loath to discuss U.S. offensive cybercapabilities, but the CEOs have been cleared for some information out of a concern that they need to know what's possible in the fast-evolving world of cyberwarfare.

Alexander himself hinted at the rationale for the briefings during testimony in March, before the Senate Armed Services Committee.

"When we see what our folks are capable of doing, we need to look back and say, 'There are other smart people out there that can do things to this country,' " Alexander said. "We need to look at that and say, 'How are we going to defend [against them]?' "

The fear is that cyberweapons developed by the U.S. military could at some point fall into enemy hands and be turned against a U.S. target.

"There are nation-states, to include the United States, who are building cybertools to prevail in a ... disagreement," Mike McConnell, the former U.S. director of national intelligence, said during a recent cybersecurity conference hosted by Bloomberg. "The worry is, what happens when some of those tools, and there are thousands of them, get released inadvertently, or somebody steals [them] to sell to a terrorist group?"

The 2010 revelation that U.S. cyberwarriors could turn a computer into a "brick" stemmed from research into a design flaw in U.S. computers, according to several sources. It was determined that an adversary could conceivably update computer firmware — the low-level software that dictates how the hardware works — to make the machine useless.

Computer manufacturers had known about the firmware design issue previously, but they had not realized it would be possible for an adversary to exploit the flaw by actually getting into the machine and destroying it.

The manufacturers subsequently ordered a reconfiguration of their computers to fix the flaw, and no damage was done. But two participants in the 2010 meeting say the CEOs were sobered by what they learned there.

Need To Work Together

To government and industry officials alike, such incidents underscore the importance of public-private partnership in the effort to address cyberthreats. But the Enduring Security Framework collaboration remains limited to a select few executives, and much threat information remains secret.

"That's the policy dilemma," McConnell said during the Bloomberg cybersecurity conference. "How do we establish a regime where that information can be shared with corporate America at the unclassified level in real time?"

Proposals to promote greater information sharing between government and industry are a key part of new cybersecurity legislation being considered on Capitol Hill.

To learn more about the NPR iPhone app, go to http://iphone.npr.org/recommendnprnews