## **WorldNews**

## Experts: DoD Could Have Prevented WikiLeaks Leak

## By WILLIAM MATTHEWS

While senior Pentagon officials resort to bluster in hopes of preventing the WikiLeaks website from posting any more secret Afghan war documents on the Internet, security experts say there is a lot the U.S. military could have done to prevent the classified documents from being leaked in the

Steps range from the sophisticated — installing automated monitoring systems on classified networks - to the mundane disabling CD burners and USB ports on network computers.

The technology is available" to protect highly sensitive information, said Tom Conway, director of federal business development at computer security giant McAfee. "The Defense Department doesn't have it, but it is commercially available. We've got some major commercial clients using it."

Banks, for example, use "host data-loss prevention" software to prevent theft and accidental disclosure of customers' account information, he said. The software also enforces rules on how data is

handled, from which employees can view it to whether it can be copied, printed or transmitted.

By contrast, Conway said, the Army "had someone on a classified network who was burning classified stuff onto a CD or DVD. That could have been blocked by automated security systems - or at least checked by security personnel at the door.

"They've got a problem, that's blatantly obvious," he said.

The leak of 91,000 secret documents has been called the largest intelligence leak in U.S. history.

WikiLeaks has already posted 76,000 documents and says it will soon post 15,000 more. The website describes itself as "a public service designed to protect whistle-blowers, journalists and activists who have sensitive materials to communicate to the public."

U.S. Army Pvt. Bradley Manning, 22, has been identified as "a person of interest" in the leak. He has been arrested and charged with illegally downloading classified information. Although Manning was stationed in Iraq, he was an intelligence analyst with high-level security clearance, and thus had access to classified information about Afghanistan.

Manning is reported to have spent months downloading classified documents and copying them to rewritable music CDs, which he then simply carried out through security checkpoints.

If the reports are accurate, "the Army enabled him to do what he is accused of doing by its own defective security," said Steven Aftergood, who directs the Federation of American Scientists' Project on Government Secrecy. There should have been no CD drives in top-secret terminals. It should not have been physically possible for anyone to download classified records onto transportable media. It was a security failure on the part of the Army that Manning even had the opportunity to do what he [allegedly]

The U.S. Energy Department learned that lesson a decade ago when nuclear weapons secrets were copied onto floppy disks ,which then disappeared. As a result, floppy disk drives in computers in U.S. nuclear labs were sealed. Aftergood said.

Now obsolete, floppy drives



Top Secrets Online: This July 26 photo shows a computer screen displaying an "Afghan War Diary" on the WikiLeaks website

have all but disappeared. The contemporary equivalent would be to disable or remove CD and DVD drives and USB ports that accommodate thumb drives and other external storage devices.

That would make it harder to copy data, but there's another approach to protecting information closely monitoring what is done with it.

"There is an increasing ability to audit every handling of information on networks, and to keep track of each person who access es and manipulates data," said Stewart Baker, former assistant secretary in the Department of Homeland Security.

Digital documents can be stamped with "watermarks" that make it possible to block access by unauthorized users and to review how each document has been handled by approved users. Similar technology is used in the recording and movie industries to prevent unauthorized copying.

"They're not perfect," Baker said, but they make it more difficult to mishandle digital documents without accountability.

Anomaly detection is another se curity step the U.S. military could take. Credit card companies have already developed computer systems that are adept at spotting unusual patterns in transactions.

If you make too many unusual purchases in a short period, Baker said, "the transactions are likely to trigger an alarm at the credit card company and a phone call about whether the purchases were authorized. They have rules that [tell their computers], 'whenever you see this pattern, there's a problem.

If adopted by the military, the technology would alert security officials when computer users download unusual amounts of data, try to copy things that aren't supposed to be copied or even change browsing habits,

See LEAKS, Page 10

a strong call to strengthen

E-mail: wminnick@defensenews.com.

## **LEAKS**

From Page 4

Baker said.

"The government has talked about doing this since [ex-FBI agent Robert] Hanssen" was discovered in 2001 to be a spy, said James Lewis, a cybersecurity expert at the Center for Strategic and International Studies.

Hanssen sold secrets to the Soviets and later the Russians for 22 years before he was caught. He might have been caught earlier if the FBI had monitored its computer systems more closely.

Defense Secretary Robert Gates said the military "is taking action in theater to prevent a repeat of such a breach, to include tightening procedures for accessing and transporting classified information." Neither the Pentagon nor the Cyber Command provided details on the stepped-up security measures.

Gates said an emphasis on information may have made it easier to download and leak data.

"One of the lessons learned from the first Gulf War in 1991 was how little useful intelligence information was being received by battalion and company commanders in the field," Gates said. "So there has been an effort over the last 15 years ... to push information as far forward as possible."

In part, that has meant "putting it in a secret channel that almost everybody" in uniform and many civilians can access, Gates said. "One of the things we're going to have to look at is should we change the way we approach that, or do we continue to take the risk."

It's possible to continue providing access to the information, but still reduce the risk, Lewis said. "You need to do the flip side of information sharing — access control and control of information."

The idea isn't to prevent people from getting the information they need, but to set rules for information use and employ computer systems that ensure the rules are followed.

Software and hardware exists that will alert administrators when cameras, thumb drives or recording devices are plugged into network computers; when forbidden material is downloaded; or when unusual behavior is detected.

"If someone downloads 10,000 pages, it will notify you," Lewis said. "The military relies on its people [not to violate rules]. That's not enough in a digital environment." □

E-mail: wmatthews@defensenews.com.