Companies beware: The next big leak could be yours

December 2 2010, By JORDAN ROBERTSON , AP Technology Writer

The Internet homepage of Wikileaks is shown in this photo taken in New York, Wednesday, Dec. 1, 2010. WikiLeaks' release of secret government communications should serve as a warning to the nation's biggest businesses: You're next. (AP Photo/Richard Drew)

(AP) -- WikiLeaks' release of secret government communications should serve as a warning to the world's biggest companies: You're next.

Computer experts have warned for years about the threat posed by disgruntled insiders and by poorly crafted security policies, which give too much access to confidential data. And there is nothing about WikiLeaks' release of U.S. diplomatic documents to suggest that the group can't - or won't - use the same methods to reveal the secrets of powerful corporations.

And as WikiLeaks claims it has incriminating documents from a major U.S. bank, possibly Bank of America, there's new urgency to addressing information security inside corporations and a reminder of its limits when confronted with a determined insider.

At risk are companies' innermost secrets - e-mails, documents, databases and internal websites that are thought locked to the outside world. Companies create records of every decision they make, whether it's rolling out new products, pursuing acquisitions, fighting legislation, foiling rivals or allowing executives to sell stock.

Although it's easy technologically to limit who in a company sees specific types of information, many companies leave access far too open. And despite the best of intentions, mistakes happen and settings can become inadvertently broad, especially as networks grow more complex with reorganizations and acquisitions.

And even when security technology is doing its job, it's a poor match if someone with legitimate access decides to go rogue.

With the right access, a cheap thumb drive and a vendetta are the only ingredients an insider needs to obtain and leak secrets. By contrast, outside attackers often have to compromise personal computers at the bottom of the food chain, then use their skills and guile in hopes of working their way up.

Employees go rogue all the time - for ego, to expose hypocrisy, to exact revenge or simply for greed.

A former analyst with mortgage lender Countrywide Financial Corp., now owned by Bank of America, is awaiting trial on charges he downloaded data on potentially 2 million customers over two years, charging $500 for each batch of 20,000 profiles. Prosecutors say the

analyst worked secretly on Sundays, using an unsecured Countrywide computer that allowed downloads to personal thumb drives. Other home loan companies bought the customer profiles, including Social Security numbers, for new sales leads, according to authorities.

Also, an employee with Certegy Check Services Inc., a check authorization service, was accused of stealing information on more than 8 million people and selling it to telemarketers for a haul of $580,000. The worker was sentenced in 2008 to nearly five years in prison.

Despite the repeated warnings, many large companies lack clear policies on who should have access to certain data, said Christopher Glyer, a manager with the Mandiant Corp., an Alexandria, Va.-based security firm that investigates computer intrusions.

WikiLeaks argues that revealing details of companies and governments behaving badly, no matter how the information is obtained, is good for democracy.

Julian Assange, WikiLeaks' founder, told Forbes magazine that the number of leaks his site gets has been increasing "exponentially" as the site has gotten more publicity. He said it sometimes numbers in the thousands per day.

Assange told Forbes that half the unpublished material his organization has is about the private sector, including a "megaleak" involving a bank. He would not name the bank, but he said last year in an interview with Computerworld that he has several gigabytes of data from a Bank of America executive's hard drive.

Assange also told Forbes that Wikileaks has "lots" of information on BP PLC, the London-based oil company under fire for the massive Gulf of Mexico oil spill. Assange said his organization is trying to figure out if

its information on BP is unique.

WikiLeaks previously published confidential documents from the Swiss bank Julius Baer and the Kaupthing Bank in Iceland. The site also published an operation manual for the U.S. prison in Guantanamo Bay, Cuba.

WikiLeaks' most recent leaks exposed frank and sometimes embarrassing communications from diplomats and world leaders. They included inflammatory assessments of their counterparts and international hot spots such as Iran and North Korea.

The prime suspect in the diplomatic leaks, Army Pfc. Bradley Manning, is being held in a maximum-security military brig at Quantico, Va., charged in connection with an earlier WikiLeaks release: video of a 2007 U.S. Apache helicopter attack in Baghdad that killed a Reuters news photographer and his driver.

Military investigators say Manning is a person of interest in the leak of nearly 77,000 Afghan war records WikiLeaks published online in July. Though Manning has not been charged in the latest release of internal U.S. government documents, WikiLeaks has hailed him as a hero.

Manning boasted to a hacker confidant that security was so flimsy he was able to bring a homemade music CD into work, delete its contents and fill it with secrets, according to a log of the exchange posted by Wired.com.

Experts said a key flaw in the military's security was that Manning may not have even had to look all that hard for the data, as it was apparently available for many people to see. The Defense Department says it has bolstered its computer security since the leaks.

Companies have many options technologically to protect themselves.

Alfred Huger, vice president of engineering for security firm Immunet Corp. in Palo Alto, said companies could simply configure their e-mail servers to restrict who certain people can send documents to.

Other measures include prohibiting certain people from copying and pasting from documents, blocking downloads to thumb drives and CD-ROMs, and deploying technologies that check if executives' e-mail messages are being checked too often - a sign that an automated program is copying the contents.

But the more companies control information, the more difficult it is for employees to access documents they are authorized to view. That lowers productivity and increases costs in the form of the additional help from technicians.

"You run the risk of creating an environment that's so rigid that people can't do their jobs," Huger said. "You have to find that balance. Unfortunately, there's no panacea against it."