HOUSTON
BUSINESS JOURNAL
Strictly Houston. Strictly Business.

Week of December 17-23, 2010 houston.bizjournals.com

# WikiLeaks highlights ease of information theft by insiders

Information technology officers in the Pentagon and embassies worldwide are not the only ones moaning and groaning over the WikiLeaks fiasco.

GUEST COMMENTARY

UMESH K. VERMA

CEOs are feeling nervous and fearful in the executive suites and boardrooms of corporate America and beyond. They are worried about the damages if they are WikiLeaked.

Thanks to a self-righteous, low-level Army intelligence analyst, national diplomacy may have been set back a decade, hard-earned reputations destroyed and lives placed at high risk. His determination and an inexpensive memory stick bypassed protection, avoided detection and may well incite information insurrection in every digital corner of the world by like-minded Internet anarchists.

Last month, WikiLeaks, a nonprofit media organization based in London, accommodated the youthful offender by sharing tens of thousands of sensitive and embarrassing embassy cables with obliging newspapers on a global scope.

This still-developing story underlines the vulnerability of corporate assets and reputations, the ease of the theft and the speed of dissemination of the information. It also reinforces the absolute importance of early detection and rapid-response as a core component of a comprehensive loss-prevention program.

Any business or organization that stores confidential data on their network of servers is just as vulnerable as the U.S. government and could be employing insider thieves with easy access to secure data.

Admiral Dennis Blair, former director of national intelligence, told Charlie Rose on Bloomberg Television in late November, "Technology is very penetrable. Currently, the only way to catch a thief is to monitor every keystroke."

So, why the extreme nervousness in C-suites and boardrooms of companies and organizations worldwide? It is the financial and compliance risk from insider theft of data. Banks and credit unions, for example, are vulnerable on the governance side as well as the IT side.

In addition to the potential loss of credibility, loss of customers and loss of competitive advantage, C-level executives, managers and directors can face employment, financial and criminal consequences from a host of regulatory agencies, as well as lengthy and damaging lawsuits related to breaches of privacy and loss of the organizations' assets.

In a June 4 interview, Gigi Hyland, a National Credit Union Administration board member, identified two of today's top information security challenges:

"… First and foremost, … employee theft of data. Unfortunately, the agency is learning of cases where disgruntled former employees pilfer or otherwise corrupt key data …. The second … big area … is employee misuse of data."

The weakest link in any organization's security is its own personnel. When a rogue employee decides to attack the company network or steal information, most of the security defenses erected against outside hacking and intrusion are ineffective.

Stealing information is not typically a one-time act. Rogue employees often research their targets for weeks or months before their first breach.

Information theft is often most successful when performed one small step at a time, stealthily probing and testing the security and response measures of the organization. Then they strike.

The most devastating losses of information assets are those that go undetected for extended periods of time.

Information security personnel and software must continuously monitor and report even the most minor activities on your network for early detection. Every anomaly must be investigated using rich, evidentiary data.

Corporations and organizations need to harden their infrastructure with a view that everyone in their organization is a threat. The more an organization believes that an employee or contractor's position in the company is so minor that he or she would not be a threat, the bigger the threat.

Defenses specific to managing internal threats must include extensive, continuous monitoring and reporting of user activity. Then you can determine if someone is testing the system before stealing the most costly, confidential data. Now, you can catch a thief in the act and not get WikiLeaked.

**UMESH K. VERMA** is founder and CEO of Blue Lance Inc. in Houston, a provider of IT security and data protection solutions, UVerma@bluelance.com.

Reprinted for web use with permission from the ***Houston Business Journal***. ©2010, all rights reserved. Reprinted by Scoop ReprintSource 1-800-767-3263.