ND Expert: WikiLeaks points out danger of insider threats to information security

December 7 2010

Even as WikiLeaks faces increasing public outcry over security breaches, potential prosecution of its founder and crippling cyber-attacks, there are probably more information leaks to come, says information security expert John D'Arcy, assistant professor of information technology management at the University of Notre Dame.

The reason has to do with the fact that organizations haven't paid enough attention to their greatest security threats – their employees.

"The recent WikiLeaks incident is no fluke, and certainly points to the increasing insider threat to information security," says D'Arcy. "Although sentiment has begun to shift, organizations have traditionally approached information security with a technological focus through investment in firewalls, network detection systems and monitoring technologies. However, these technologies are useless against the motivated insider who wants to damage the organization by leaking sensitive information."

Even prior to WikiLeaks, studies found that data breaches are costly problems for U.S. companies – about $3.5 billion in opportunity costs and remedial actions for the nearly 500 incidences reported in 2009, according to Ponemon Institute. If consumer losses and an estimate of unreported breaches are figured in, the cost of data breaches ratchets into the tens, if not hundreds of billions of dollars, according to a United Nations report.

Perhaps most surprising, the study also found that three-quarters of all U.S. data breaches are due to insiders at the organization. Only about 24 percent of all breaches studied involved some sort of criminal or other malicious act.

D'Arcy's research examines whether awareness of a company's security policies influences the employee's perceived threat of punishment, and whether this perception in turn reduces incidences of information being used inappropriately.

"In terms of dealing with the insider threat, organizations need to realize that information security is a management issue – not just a technical issue – that requires a coordinated approach," says D'Arcy. "Security experts are now suggesting that IT personnel start working with human resources and other functional areas to look for behavioral signs ahead of time that could prevent insider security incidents."

For example, D'Arcy says, data indicates that a significant number of insider security incidents are perpetrated by disgruntled workers who have publicly expressed their angst via social media (wikis, blogs, Facebook and so on). "I expect to see a rise in employee 'profiling' as a mechanism to combat the insider security threat," he adds.

As a side note, D'Arcy points out that the WikiLeaks incident also underscores the potential damage, beyond financial damage, that can accrue from an information security breach. "For example, the WikiLeaks leaked news that the U.S. government accused the Chinese government of large scale attacks on several U.S. businesses – including Google, Adobe and Intel – last January. To date, the Chinese government has denied this claim; however, the WikiLeaks incident may certainly cause tension between the U.S. and other nations such as China."

D'Arcy's study, "User Awareness of Security Countermeasures and Its

impact on Information Systems Misuse: A Deterrent Approach," co-authored with Anat Hovav of Korea University Business School and Dennis Galletta of the University of Pittsburgh, was published in the March 2009 edition of *Information Systems Research*.

Provided by University of Notre Dame