

## THE LAST WATCHDOG on Internet Security by Byron Acohido Information protection in the age of WikiLeaks

<http://lastwatchdog.com/information-protection-world-wikileaks-cloud-computing/>

*Posted on | March 21, 2011*

One big revelation that came out of the 2011 RSA cybersecurity conference last February was that 65% of IT and security professionals do not have a complete grasp of the security implications of using USBs, smartphones and tablet devices to access confidential files.

A survey of 200 pros attending RSA at San Francisco's Moscone Center revealed widespread risky practices by folks you'd expect to know better. For instance, some 77 percent admitted sending payroll, customer data, financial, and other classified information via unsecured email monthly.

Loose security practices enabled the hackers' group Anonymous to expose the disinformation proposals data intelligence firm HB Gary Federal made to the Bank of America and the U.S. Chamber of Commerce. And Anonymous is said to be probing for weaknesses in tech systems of companies controlled by the Koch Brothers of Wisconsin fame.

In this LastWatchdog guest post, Rob Marano, President & CEO of InDorse Technologies, outlines the scope of the corporate world's vulnerability. Marano contends closer monitoring of sensitive company documents could be part of the answer. InDorse supplies systems for document tracking, digital watermarks and advanced file protection.

By Rob Marano

WikiLeaks and Anonymous have dominated the security news landscape in 2011. When you stop to think about the situation, it's no surprise that confidential information from BofA is leaking its way to the headlines. Now that the once mighty enterprise firewall has given way to unrestricted mobility, flash drives, work/home laptops, telecommuting and tablets, there are seemingly limitless ways to steal information without detection.

As we emerge from the great recession, businesses find themselves operating in an increasingly Internet-centric world. During the downturn many organizations turned to IT solutions that would reduced capital and operating costs as well as enabled businesses to operate more effectively. The new flexibility brought forward by the emergence of Web-based services allowed employees to take the enterprise home.

From that point, a shift started regarding privacy concerns in the workplace. Employees increasingly demanded, and needed, the ability to work outside of the firewall. Given the economic climate, the ability to produce results was more important than the threat of a leak. Now that unrestricted mobility

is a reality, we're witnessing and increase in the number of threats like WikiLeaks and state or corporate espionage. Why?

Currently, the industry finds itself in the middle of a shift from traditional, silo-based IT to cloud-based computing systems. This change is happening and will accelerate as rapidly as the Web's first business wave that hit in the 1990s. The bad news is that organizations switching to the cloud are more vulnerable and have not reevaluated their security measures. As such, businesses are constantly struggling to keep sensitive data from leaking outside of their organizations. In many cases, IT professionals are not even sure about the data that is leaving. The fact that 65 percent of IT pros surveyed at the RSA Conference admitted they do not have a handle on the files and data leaving their enterprises does not instill confidence in the security measures currently in place.

Traditional IT security solutions like data loss prevention tools and intrusion prevention systems can slow down the classic sensitive information exfiltration campaigns by malicious users and cyber criminals. Unfortunately, these techniques have lost some punching power since businesses shed their virtual walls. This is mostly due to network-level security's ineffectiveness against monitoring outbound content. Information leaving organizations rarely receives the amount of monitoring needed. As a result, users can attach confidential documents to non-company email, instant messaging and peer-to-peer file sharing with frightening ease.

The reactionary thought to ending these leaks might be to stop cloud implementations. The only way to begin to slow down the ease at which information is shared in a malicious way is NOT to turn away from the flexibility and collaboration that cloud computing has provided. A completely closed enterprise is a thing of the past. The best way to secure outbound information in a security strategy is to provide the ability to maintain enterprise collaboration, and have technology that provides the ability to track and trace files anywhere on the Internet.

BofA can attest that WikiLeaks and Anonymous have created a significant security threat for organizations and agencies. This is especially true for businesses that do not emphasize outside data monitoring in their security strategy. Without the capability of monitoring and controlling company files, both on and off the company's network, this vulnerability can prove disastrous results. Most current approaches fail to counter this threat because it is impossible to stop the flow of information. However, it is possible to return to a state of accountability by monitoring the use of company files and protecting them from misuse through file tagging and tracking.

A 100 percent security solution is a pipedream and halting the cloud transition is not a good financial business decision. By having visibility in the files that have been leaked, organizations can at least create a plan to respond to this situation. Although the information fell into outside hands, a calculated response addressing the information can take some power back from the leak.

**About the author:** *Rob Marano is president and CEO of InDorse Technologies, which he established in 2006. Rob is also a professor at The Cooper Union and NYU*