FOUR WAYS TO WIN THE GAME WIKILEAKS CHANGED

How to Protect Your Company's Data in an Increasingly Online World

Written by Victor Vital, Robert Failla and Chuki Obiyo

This article contains information regarding the following topics: RISK MANAGEMENT + LEADERSHIP + WORKFORCE

Unexpected volatility of stock prices, reputational damage, and director and officer liability associated with the massive data loss underscore the need to bring information security to the top levels of the company. WikiLeaks has forever changed the way directors and executives need to view information security. In light of WikiLeaks, there are four ways for a company's directors and officers to execute a winning information security strategy that not only protects the company but also insulates its directors and officers from liability: (1) sponsor a winning governance culture that holds executive management accountable; (2) implement a "common language" control framework; (3) evaluate information security as a nondiscretionary cost; and (4) identify and evaluate technical controls appropriate for the organization.

BUSINESS FACT: WikiLeaks was launched in 2006 by Julian Assange.

First, a company must promote a culture of accountability in IT governance. Accountability demonstrates board sponsorship and assures that executive management is not de-prioritizing information security in favor of other executive priorities. IT governance is a framework for making decisions based on risk, and it assures that information-security spending is tied directly to real risk that is recognized at the board level.

Specifically, directors must give information security adequate time and attention on the board's agenda. The board's focus on information security needs to be dedicated to understanding the company's risks, and the board needs to determine the level at which the organization should be mitigating those risks through appropriate controls. Indeed, best practices include the board forming a special committee made up of directors, officers, auditors and information security leaders to specifically address information security. Below the senior management level, managers and other IT personnel should be implementing controls that directors and officers have approved while audit personnel should be assessing and reporting on the effectiveness of these board-approved objectives.

Second, a company should implement a control framework. A control framework provides for a common language within the company culture for addressing information security. This framework allows everyone in the company, from board members to the lowest-ranked workers, to communicate with clarity, focus, and alignment around the company's information security objectives. Such a framework facilitates budgetary decisions that mitigate risk at a minimum cost. Further, the implementation of a control framework substantially reduces the time and effort expended on issues that are insignificant at the board level. The framework becomes the linchpin for all IT risk assessments, compliance inspections, and audit activities.

A popular framework that readily maps to federal, state, or local requirements such as the Sarbanes-Oxley Act is the Control Objectives for Information and related Technologies or COBIT. Implementation of a framework like COBIT involves (1) selecting risk-mitigation controls that are appropriate for a specific organization, and (2) turning the information security objectives into auditable policy and procedure. Implementation of a control framework is a significant step. Consultation with an IT security expert can help a company choose and implement the right controls to mitigate specific risks.

Third, a company needs to re-evaluate how the budget for IT security is determined. It is all too easy to fund the minimum necessary to be in compliance with federal, state, and local regulations or to tie budgeting directly to the actual loss of information. Compliance and information security are not one in the same, however. In other words, compliance alone cannot be expected to mitigate all the significant risks in a company's risk universe. Further, the budget that is tied to actual losses is reactive and will not prevent a WikiLeaks-like situation from occurring. Funding, therefore, needs to be based on assessed risk.

Risk is not evaluated in a vacuum. There is risk to not achieving other company objectives. However, aggregate risk increases when information-security spending is tied to other budgets such as the general information technology budget. We recommend a separate budget line item for IT Security that is (1) tied directly to risk reduction, (2) based on an established control framework, and (3) evaluated in the context of the business as a whole.

> **THE THREATS ON INFORMATION SYSTEMS FROM WIKILEAKS AND OTHER LEAK-FOCUSED ORGANIZATIONS ADD A NEW ARENA OF COMPETITION FOR COMPANIES IN AN ALREADY COMPETITIVE GLOBAL ECONOMY.**

Fourth, controls must be selected that complement each other and that are appropriate for the organization. Physical, administrative, and technical controls all work together to achieve the objective of securing the organization. As an example, a policy regarding authorized network use (administrative control) is of no value if locks and alarms (physical controls) or firewalls (technical controls) do not exist. In the case of WikiLeaks, proper technical controls such as Digital Rights Management (DRM) or Data Leak Protection (DLP) may have been lacking. DRM is a strong tool for enabling companies to protect documents based on several criteria such as "who, when, and how" they are accessed. DLP is a technology that inspects data and can be configured to either set off alarms or reject the traffic altogether. Both DRM and DLP have significant implications to a network and therefore must be implemented purposefully. Alignment with the entire organization is paramount to success.

The significant threats on information systems posed by WikiLeaks and other leak-focused organizations add a new arena of competition for companies in an already competitive global economy. This is now a different game. The risks at play now go well beyond audit compliance requirements especially with regard to certain liabilities. The days of relying on an IT strategy that simply checks off a "compliance to-do list" are over. Because the unauthorized loss and subsequent disclosure of sensitive data can expose the company to significant damage, including reputational damage, triggering suits against directors and officers, a pro-active approach by the board is advisable. Furthermore, without IT governance, there is a greater likelihood that confidential information disclosed about vendors, customers, or competitors may lead to a suit seeking damages associated with the company's failure to prevent the disclosure.

"The vast majority of boards that [are] reviewing privacy and security issues [are] not focusing on key activities that could help protect the organization from high risk areas," according to a report published by CyLabs entitled "Governance of Enterprise Security: CyLab 2010 Report." The aftermath of WikiLeaks underscores this finding. Don't miss your call to action. The benefits of a winning strategy on IT governance can positively impact a company's earnings as well as its reputation by reducing the liability exposure of the company, its directors and officers.

Victor Vital is a Litigation Partner at the international law firm Baker Botts L.L.P. Robert Failla is a 14 year Information Security Veteran and Principal of RJF Investigative Services. Chuki Obiyo is an Executive Advisor and graduate of Northwestern University School of Law.