

Technology Brief

Large Organizations are Way Behind on IT Risk Management

Date: June 2010 **Author:** Jon Oltsik, Principal Analyst

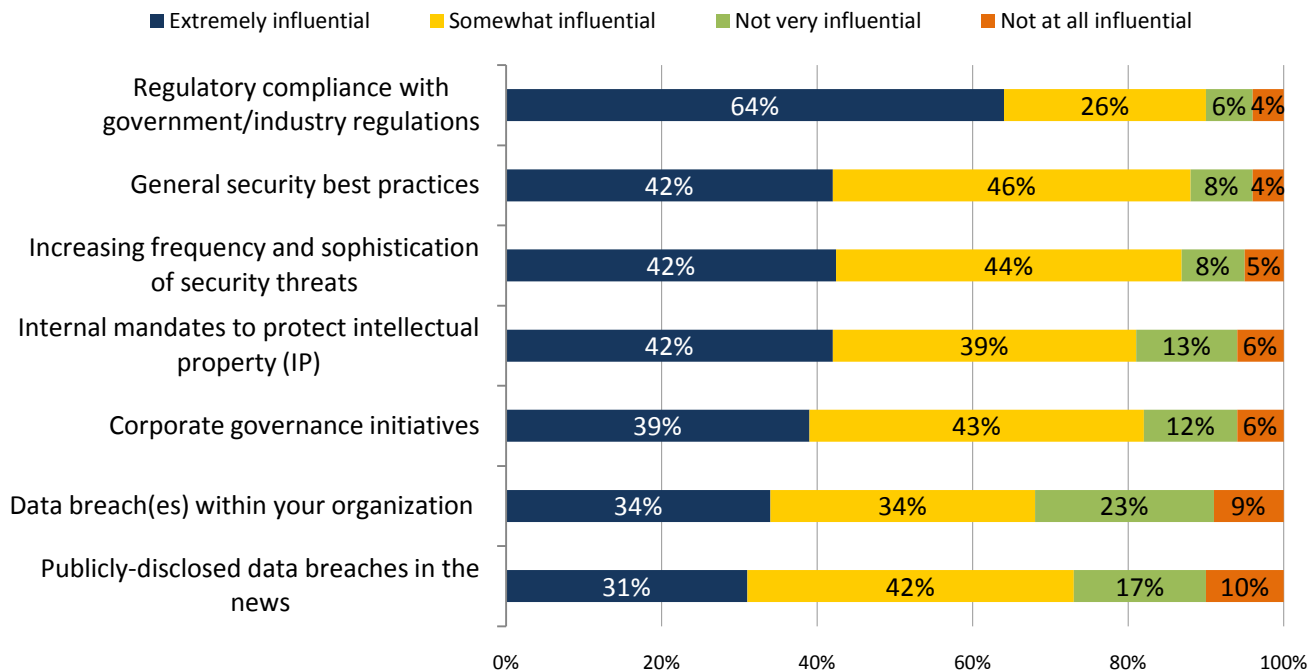
Abstract: Government and industry regulations were supposed to improve information security, yet many holes remain. Why? Many organizations adopted a regulatory “check box” mentality which helped them pass audits, but didn’t address dangerous threats or existing vulnerabilities. ESG believes IT risk management can help and many large organizations concur, but new data from Evalueserve indicates that there is still a lot of work to do. Without rapid IT risk management progress, many organizations remain sitting ducks for cybercrime, industrial espionage, or catastrophic denial of service attacks.

Overview

What’s driving information security at large organizations? In spite of all of the headlines, data breaches, and malicious code exploits, information security remains largely driven by government and industry regulations like FISMA, HIPAA, GLBA, and PCI DSS (see Figure 1).¹

Figure 1. Regulatory Compliance Drives Information Security

How influential have each of the following factors been in your organization’s information security efforts? (Percent of respondents, N=308)



Source: Enterprise Strategy Group, 2009.

Linking information security to regulatory compliance isn’t necessarily a bad thing. After all, regulations like PCI DSS are meant to establish a comprehensive security baseline for organizations handling credit cards and personally identifiable information (PII) and address potential risks to this data. Regulatory compliance is far from a panacea, however. When

¹ Source: ESG Research Report, [Protecting Confidential Data Revisited](#), April 2009.

organizations build an information security plan based upon government or industry regulations alone, the objective is often passing compliance audits rather than addressing the real threats, vulnerabilities, and risks associated with an attack. This “check box” mentality can actually be counter to the real goal of securing people, assets, and data; organizations that pass regulatory compliance audits often unknowingly face pervasive and insidious risks across the enterprise.

What’s Needed?

IT Risk Management

Many large organizations can’t see the forest for the trees—the objective of regulatory compliance is reducing risks, not meeting artificial metrics. ESG believes that CIOs and CISOs must become change agents and lead their organizations to an information security based upon risk management. Just what is risk management? The International Standards Organization (ISO) defines risk management as:

The effect of uncertainty on objectives, (whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

From an information security perspective, risk management is a process of assessing security threats across the organization, determining the vulnerabilities that open the organization to each threat, and then determining how the organization should respond. Potential responses include accepting some risk for unlikely threats (e.g., a physical attack by armed commandos) or addressing the risk with some type of control.

The following definitions are often applied to IT risk management:

- **Threat:** A natural or man-made event that could have a negative consequence to the organization.
- **Vulnerability:** A flaw, loophole, oversight, or error that can be exploited to violate system security policy.
- **Control:** Mechanisms used to restrain, regulate, or reduce vulnerabilities. Controls can be corrective, detective, preventive, or deterrent.

In total, risk management is based on real data, metrics, and measured responses. In this way, risk visibility based upon up-to-the-minute data act as the foundation of risk management processes and potential responses.

How does risk management align with regulatory compliance? Done correctly, risk management actually supports and supplements regulatory compliance. How? By measuring threats and identifying vulnerabilities that may be outside of the scope of compliance mandates or unique to a particular organization. Furthermore, risk management can do something that compliance cannot: help organizations actually identify and respond to measurable risks and truly improve information security protection. Recognizing the compliance “check box” shortcomings, the U.S. Federal Government is in the process of revising the Federal Information Security Management Act of 2002 (FISMA). The plan is to replace the old “report card” system with one focused on addressing real risks.

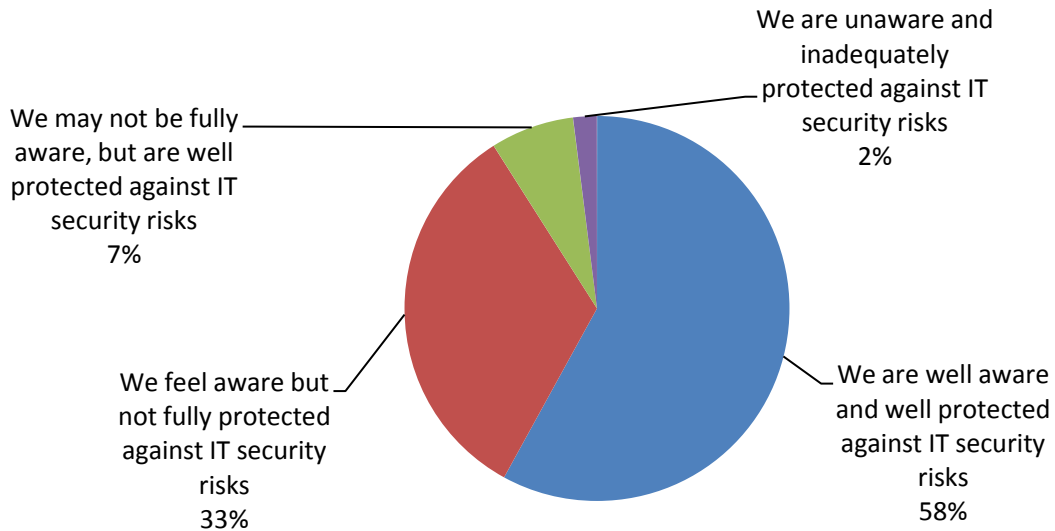
Are We There Yet?

Few CISOs would argue that a comprehensive enterprise-wide risk management strategy could not help any organization improve information security and streamline regulatory compliance. Given this, one would think that enterprises are well along the way toward establishing IT risk management as a standard. Unfortunately, this is not the case. Why? As stated earlier, risk management depends upon end-to-end knowledge of threats and vulnerabilities. Many organizations simply have limited awareness of one or both of these. Without real-time information, it is simply impossible to build adequate controls.

These limitations are illustrated in a recent market research study by Evalueserve. More than 40% of respondents believe that their organization is either unaware of risks or unprotected against them. Awareness without controls represents a real risk. Lack of awareness or controls represents a substantial risk (see Figure 2).

Figure 2. Many Organizations are Unaware of or Inadequately Protected Against IT Risks

Now we would like to ask you a few questions around how your organization manages IT security risks. What would you say is the status of your organization with regard to awareness and protection against information security risks?

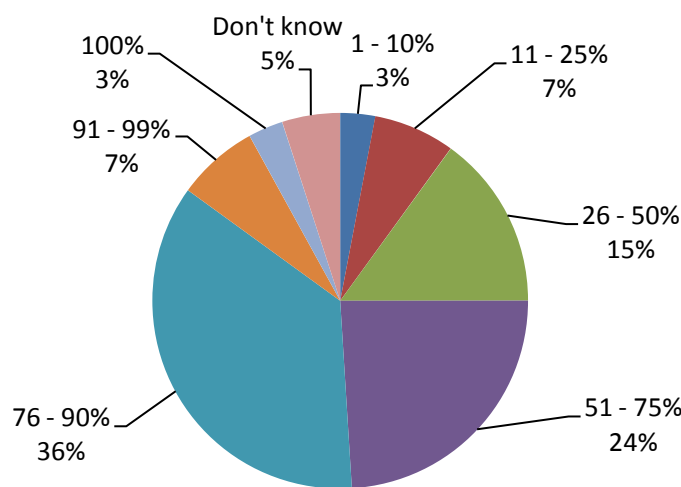


Source: *Evalueserve, 2010.*

The Evalueserve data points to other troubling trends. Note that the majority of organizations responded that they were aware of and protected against security risks. Unfortunately, other data from the survey contradicts these assertions. For example, only 3% of respondents claim that their organization has IT risk visibility into its IT environment. Alarmingly, more than half say that their organization has visibility into less than 75% of its IT environment (see Figure 3). To paraphrase an old management saying, “you can’t secure what you can’t measure.”

Figure 3. Large Organizations do not have Visibility into their Entire IT Environments

In your opinion, what % of visibility do you currently have into the risk posture of your IT environment? (N= 260)



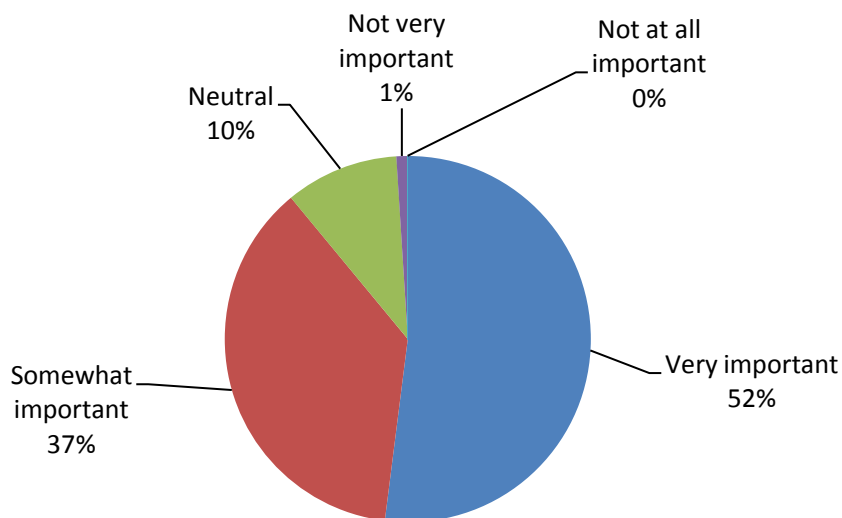
Source: *Evalueserve, 2010.*

In essence, risk management is a formula of inputs (threats and vulnerabilities) that determine outputs (controls). When done correctly, risk management makes the application of controls fairly obvious—unacceptable levels of risk should be

addressed with controls as countermeasures. This formula seems somewhat lost on the Evalueserve respondents, as only 52% of respondents believe it is “very important” to know precisely where to deploy a security product to protect information assets (see Figure 4). Given this, it appears that other organizations are unclear about one of the primary underpinnings of risk management.

Figure 4. Many Organizations do not Believe it is Important to Know Where to Implement Security Controls

How important is it to know precisely when and where you need to deploy a security product to protect your information assets? (N = 273)



Source: Evalueserve, 2010

The Bigger Truth

Information security strategy is a complex struggle between good guys and bad guys. Unfortunately, it is no game; organizations experiencing a security attack can suffer data losses, regulatory compliance breaches, or denial of service attacks. This can result in millions of dollars in losses, loss of goodwill or worse—ESG fully expects to see more devastating consequences like months of business interruption or bankruptcy as a result of sophisticated security attacks in the future.

The Evalueserve data carries some good and bad news. The good news is that most organizations have the right mindset with strong risk management concerns. The bad news is that the majority of firms lack the necessary knowledge about the threats they face, their existing IT vulnerabilities, or the appropriate places to implement security controls. Risk management efforts are commendable, but without a comprehensive program, they are doomed to fail.

So what happens now? ESG believes that organizations must go back to basics. This means establishing processes and implementing tools that provide visibility, data, and metrics on all threats and vulnerabilities. Only then can they apply controls with confidence in their effectiveness and ROI to ultimately establish a meaningful balance between business productivity and the right amount of security.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.