Technology Brief

Real-Time Risk Management

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

Abstract: *Information security based on regulatory compliance stipulations cannot keep up with today's sophisticated and rapidly changing threat landscape. CISOs need to implement a new discipline that ESG calls, "Real-time Risk Management." Real-time Risk Management addresses the rapidly changing threat landscape with up to the minute information about threats, vulnerabilities, and assets; comprehensive visibility of the entire IT infrastructure; and continuous assessment of existing security controls.*

Overview

Over the past few years, information security policies and controls were guided primarily by regulatory compliance requirements. ESG believes this behavior is now changing. Why? Information security defenses based upon regulations alone can help large organizations pass compliance audits, but they aren't nearly as effective at protecting them against the growing volume of sophisticated threats and targeted cybercrime attacks.

Addressing these new virulent threats demands a new mindset based upon IT risk management rather than regulatory compliance or reactive security alone. Unfortunately, many enterprises have a long way to go to make this transition. Why? Of ESG research respondents:

- Only 58% of organizations claim that they are "well aware and well protected against IT security risks."
- Just 3% of organizations claim to have 100% visibility into the risk posture of their IT environment. Alternatively, more than half of all respondents said that they either had 50% or less visibility into the risk posture of their IT environment or they didn't know.

This data points to an alarming reality: many organizations realize that they are not only inadequately protected against security threats, but they lack the right level of visibility to understand or sufficiently address these risks. Regrettably, many organizations are simply "flying blind" when it comes to risk management.

Risk Management Review

From an information security perspective, risk management is the process of assessing the likelihood of security threats across the organization and determining the vulnerabilities exposing organizations to each threat. With risk management, threats and vulnerabilities are defined as follows:

- **Threat:** A man-made or natural event that could have a negative consequence to the organization. Man-made examples include power failures, but also Web threats, spear phishing, and internal attacks. Examples of natural events include natural disasters like earthquakes, hurricanes, and floods.
- **Vulnerability.** A flaw, loophole, oversight, or error that can expose an organization to a threat. A distribution center on the U.S. Gulf coast is vulnerable to hurricanes and floods. Likewise, a Windows server that has not been patched with the latest operating system updates may be vulnerable to specific types of malware attacks.

With IT risk management, threats and vulnerabilities should be assessed on an asset-by-asset basis. Risk management decisions can then be made depending upon the level of exposure (i.e., threats and vulnerabilities) as well as the asset's value (i.e., the relative significance each asset delivers in overall business operations).

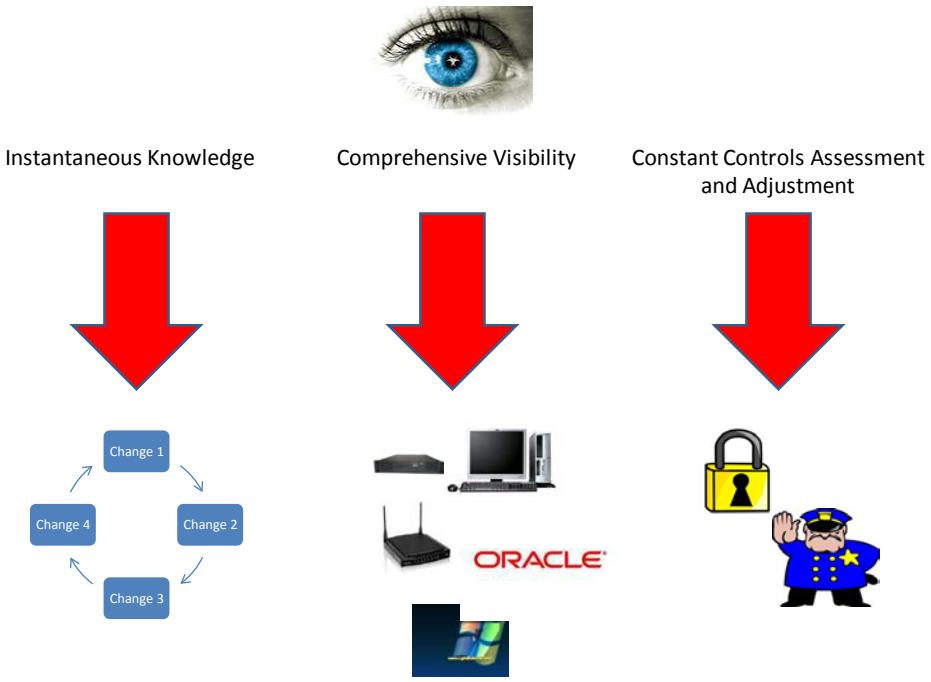
Armed with these metrics, organizations can make qualitative and quantitative risk management decisions such as risk acceptance, risk assignment, or transfer (i.e., transferring potential risk to a third party such as an insurance company) or risk reduction (i.e., mitigating risk by implementing security controls, policies, and procedures). In this case, a control is defined as a mechanism used to restrain, regulate, or reduce vulnerabilities.

Risk Management: What's Needed?

The data cited above demonstrates that IT risk management needs a lot of work. Why? First, IT risk management is relatively new and undeveloped; this will improve over time. But IT risk management faces another challenge beyond immaturity alone. The fact is that IT is a rapidly-evolving system: large organizations are currently in the midst of a massive IT metamorphosis driven by SOA, virtualization, cloud computing, consumerization, and mobility. In this environment, threats, vulnerabilities, and even IT assets change on a daily basis. This situation is exasperated by the rapid rise in threats; the convergence of the two results in a perfect storm for CISOs.

How can CISOs maintain sound risk management practices in an environment of constant change? Today's risk management must be based upon (see Figure 1):

Figure 1. Components of Real-Time Risk Management



Source: Enterprise Strategy Group, 2010.

- **Instantaneous knowledge.** Given the dynamic nature of both IT and the threat landscape, it is no longer adequate to perform risk assessments at predefined internals (i.e., weekly, monthly, quarterly, etc.). Rather, asset changes, vulnerability assessments, and threat data must be available in real-time. Security tools must correlate this information and immediately report on new types or levels of risks. Security practitioners must be trained to digest these inputs, present them to business managers, and expedite risk management mitigation without delay.
- **Comprehensive visibility and coverage.** IT is composed of a multitude of assets like hardware devices, databases, business applications, and virtual appliances. It is no longer enough to understand a sub-segment of the entire IT portfolio alone or adopt a piecemeal view of the entire IT infrastructure through a potpourri of tools. To keep up with assets and their associated vulnerabilities, CIOs need a consistent data, visibility, and alerts across the entire IT spectrum. It's not enough to get a partial picture (remember that more than half of all respondents said that they had 50% or less visibility into the risk posture of their IT environment). Organizations need to understand all of the vulnerabilities that exist and how they impact the environment.
- **Constant controls assessment and adjustment.** Security controls don't fit into the "set-it-and-forget-it" category. Rather, controls need persistent assessment to ensure that they adequately address new or changing risks.

The Rise of Real-Time Risk Management

CISOs should anticipate a new category of security management solutions for "Real-time Risk Management." Real-time Risk Management demands wide (i.e., across the entire IT infrastructure), deep (i.e., strong technical insight into each technology), and constant visibility into threats, vulnerabilities, assets, and controls. The best real-time threat management systems will also be supported by:

- **Threat monitoring intelligence.** To keep up with rapid changes in the threat landscape, real-time risk management platforms will be constantly updated by the latest threat data from leading security researchers, academics, and public organizations. Along this line, security practitioners require vulnerability assessment content that delivers depth and breadth of coverage to ensure proper controls can be dispatched to thwart risks that materialize from the ever-changing/evolving threat landscape. Don't be caught with partial coverage—finding 100% of half of the vulnerabilities still leaves a business highly exposed.
- **Deep security knowledge.** To help security professionals sort through mountains of threat, vulnerability, and asset data, real-time risk management will be instrumented with heuristics, correlation engines, and alerting capabilities. The goal? Help security professionals understand where best to focus security controls.
- **Automation.** Aside from gathering and sorting through information, real-time risk management platforms will also integrate with security controls and enforcement technologies in order to automate risk management responses. When the risk management system detects un-patched laptops on the network, it can prompt security operations teams to begin an immediate patch cycle or other security control.

The Real-Time Truth

Real-time Risk Management is more than a new evolving set of security tools; it is a mindset shift. CISOs should begin with more frequent security assessments, asset discovery, vulnerability scans, and configuration management. It is also worthwhile to implement IT best practice models like ITIL, COBIT, or the NIST-800 series. These guidelines will help lock down error-prone activities such as IT provisioning, configuration management, and change management.

CISOs should also take a pragmatic look at risk management blind spots. How current are asset databases? Do existing tools discover and alert IT when new assets are added to the network? Do vulnerability scanning tools cover all technology elements or just a subset? Do those tools use timely content and cover the spectrum of databases, applications, systems, and devices that define the organization with a comprehensive set of vulnerability checks? Remember that visibility gaps represent security vulnerabilities and should be analyzed and mitigated as such in a risk management context.

Finally, ESG firmly believes that early Real-time Risk Management systems are already available today. Smart CISOs will research available solutions, query vendors on product roadmaps, and evaluate leading solutions as soon as possible. The goal? Deploy Real-time Risk Management tools that can keep up with business-driven IT changes and help establish a Real-time Risk Management discipline throughout IT.