

Symantec's High Value Foundation IT Risk Assessment

Date: June 2007

Author: Jon Oltsik, Senior Analyst

Abstract: Many organizations know that they have an unacceptable level of risk associated with their IT infrastructure, but they have no clue how to assess or remediate them. Enter Symantec and its Foundation IT Risk Assessment (FIRA). With FIRA, Symantec can now baseline IT risk and provide CIOs with a business-centric action plan—all in about three weeks.

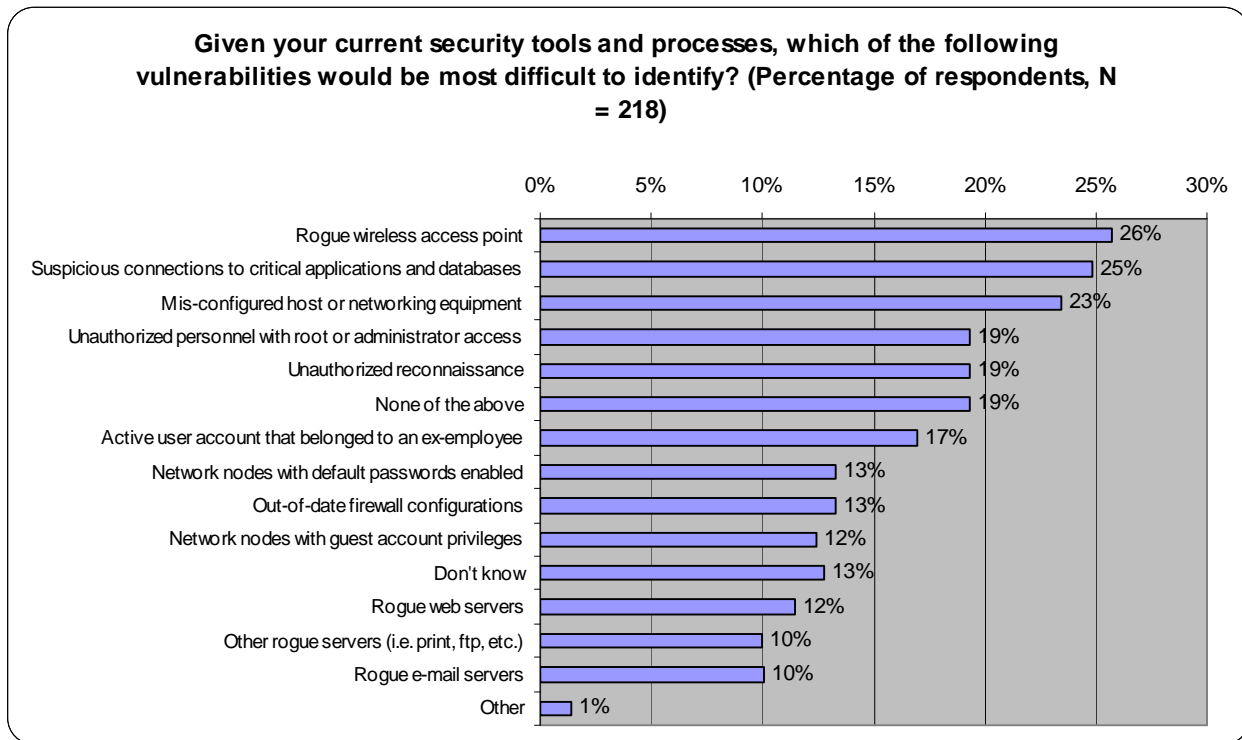
Overview

Regardless of industry, company size or geography, nearly every organization engages in business processes that depend upon IT applications and infrastructure for collaboration, communication or transaction processing. Rather than a debate, CEOs now accept this as a fact.

Unfortunately, this business/IT relationship is governed by Murphy's Law: "anything that can go wrong, will go wrong." In fact, when it comes to IT, Murphy may have been an optimist. Enterprise IT is a complex system in a constant state of moves, additions and changes. Additionally, IT organizations are frequently understaffed or lacking specific skills. These systemic and organizational issues lead inevitably to numerous risks across IT in areas such as:

- **Regulatory Compliance.** Industry regulations such as GLBA, HIPAA, PCI or SOX are driving organizations to bolster processes and technologies across IT. The issue facing organizations here is that industry/government regulations specify business requirements, but not the corresponding IT processes or security safeguards. Unfortunately, this means that IT staff is left to translate legal text in regulatory documents into sound practices aimed at identifying, quantifying and remediating IT risks.
- **System and application performance.** Today's complex multi-tiered applications have become a troubleshooting nightmare. When remote office employees barrage the help desk with performance woes, the entire IT organization is put on call. Is this a network problem? Is some server over utilized? Is the application code itself to blame? Many organizations simply can't afford to hire a team of experts who understand business, application and IT infrastructure behavior.
- **IT availability.** Many firms have processes in place for data recovery, but what about restoring critical applications and business process? How will an organization maintain normal business operations when the data center in Florida is impacted by a Category 3 hurricane? Even the most sophisticated IT organizations need to assess these risks on a perpetual basis.
- **Security.** Security risks remain prevalent, dynamic and difficult to find as evidenced in a recent ESG research project where security professionals defined a number of elusive vulnerabilities (see Figure One). The combination of increasingly sophisticated attacks and IT complexity mean that security risk will become more difficult and obscure in the future.

Figure One. Security Vulnerabilities Can Be Difficult To Find



Pragmatic CIOs certainly recognize these shortcomings, but often struggle with the fundamental question: “Where do I start?” Since it is impossible to cover all bases, should IT executives begin with a security assessment or compliance review? Some IT managers may realize their own limitations and seek outside help, but this also can present a challenge. A security services firm can perform deep penetration testing, but won’t assess the performance of WAN-based applications. Disaster recovery service providers may offer a roadmap to 4 hour RPOs and RTOs, but won’t address security vulnerabilities like stale user accounts on the SSL VPN. A sequential process is also a non-starter due to the constant state of IT change. This leaves CIOs with the same questions: “Where do I start?” and “Who can help?”

Symantec Foundation IT Risk Assessment (FIRA)

IT risk leader Symantec may have an answer to this perpetual IT enigma with the recently announced creation of its Foundation IT Risk Assessment (FIRA). Rather than an extended consulting engagement or a deep technology dive, FIRA can be considered a “wide and shallow” offering focused on IT risks associated with regulatory compliance, performance, availability and security. This “wide and shallow” scope may be the biggest benefit associated with FIRA. In as little as three weeks, Symantec FIRA delivers a:

- **Baseline assessment.** After a few weeks in the IT trenches asking lots of questions, Symantec consultants deliver an executive summary detailing IT risks in all four areas. This baseline can serve as a risk management starting point for measuring the progress of any project or remediation activities henceforth.
- **Granular risk profile.** Based upon a wide array of inputs, Symantec produces a “heat map”—a taxonomy that measures IT compliance, performance, availability and security risks across various categories like “infrastructure and networks,” “organization and culture” and “people and process.” With this report, CIOs may discover IT risk nuances. For example, informal processes may lead to an extremely high level of IT risk in spite of recent investments in a variety of network security

safeguards. In this way, FIRA can help uncover IT risk needles in overwhelming people, process and technology haystacks.

- **To-do list.** With a risk profile in place, Symantec consultants deliver a six month action plan prioritizing IT risks that have the biggest potential impact to the business. The FIRA action plan is written specifically so it can be consumed by both business and IT managers.
- **Help with the business folks.** After FIRA projects are completed, Symantec consultants remain on-call for meetings with executive management or the board of directors. These consulting pros are there to help convert techno-speak into language and metrics that can be easily digested—and acted upon by business leaders.

FIRA isn't for the faint of heart. CIOs should expect a three-week whirlwind of assessment activity, followed by additional periods of intensive meetings between IT and business managers and finally a series of critical IT risk remediation projects. Granted, this isn't the whiz-bang stuff that makes technology so cool, but remember that the CEO cares more about ongoing business operations than multi-core processors, server virtualization, SOA or IPv6.

Why Symantec?

CIOs may recognize the benefits associated with FIRA, but may not realize that this type of high-value service is available from Symantec. Actually, ESG believes that Symantec's service offering is one of its biggest strengths in the market. FIRA is a good match for large organizations because of Symantec's:

- **Worldwide presence.** While Symantec is still equated with PC security, it also has a sizeable services organization. Many IT professionals don't realize that Symantec has a stable of over 4,000 services professionals around the world, 1,100 of which are consultants. Symantec services revenue accounts for approximately 5% of total sales. FIRA marries Symantec's size and subject matter expertise with the right timing and deliverables. This type of service engagements is too broad for local service providers and too focused for large global system integrators.
- **Diverse products and skills.** Symantec product offerings span IT risk areas such as security, storage management, IT operations and application management. Since Symantec has expertise in all of these areas, IT risk management services are a natural extension that takes advantage of its wealth of experience and knowledge.
- **Industry best practices.** Symantec FIRA is a formal process that marries IT governance frameworks such as ITIL and CoBiT with homegrown methodologies. This is important for two reasons: 1) It adds credibility to the Symantec offering, and 2) FIRA reports and action plans can be adapted to fit into existing IT governance processes—a requirement for many large global organizations.

The Bottom Line

It's time that large organizations stop looking at IT stovepipes and start looking at IT Risk Management across the enterprise. This is easier said than done. IT is simply too complex these days to have the internal skills and knowledge to know where to start, let alone come up with a detailed plan of attack.

With growing requirements and lots of confusion around IT Risk management, Symantec FIRA may be the right service at the right time. FIRA delivers a lot of value in a little time and provides CIOs with a detailed plan of action in a business-centric context. ESG believes this makes FIRA a great place to start to address IT Risk Management—sooner rather than later.

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 and is intended only for use by Subscribers or by persons who have purchased it directly from ESG. 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.