

Leveraging Technology

ITAM and Information Security

In a world where cyber-crime is becoming an ever-increasing threat and corporate governance has come under more intense public scrutiny organizations have begun placing a great deal of new-found emphasis on information technology security. Some organizations have begun to discover the financial benefits of implementing enterprise-wide information IT asset management (ITAM) programs – often recouping their initial ITAM investment relatively quickly through software license harvesting, lower support costs, and other cost saving benefits. Historically, tracking and reporting IT assets has typically been viewed as a burdensome task required by financial audit requirements. What is often overlooked is the synergy that exists between ITAM and Infosec. One consideration for leveraging the two domains is the use of a common management framework – an infrastructure management framework such as ITIL, or a control-oriented framework like CobiT. These frameworks can provide a common reference landscape in which asset and security practitioners can operate collaboratively.

From a security perspective, information technology organizations have been primarily concerned with securing the perimeter of their technology infrastructure. Indeed until the proliferation of the Internet into almost every aspect of our lives,

most organizations concerned themselves with deploying corporate firewalls to protect their internal networks. Now intranet, extranets, coupled with recent data that shows greater than 50 percent of corporate attacks come from sources internal to the target organizations staff has led. To more emphasis being placed internal audit and compliance As if these challenges weren't enough continuing vulnerabilities of Microsoft-based operating systems have made enterprise configuration management a high priority with today's security professionals. This is one key area where ITAM and Information Security overlap.

More importantly, a new asset-centric view to security is emerging that places the emphasis on intellectual property protection as the primary goal. Key to this effort is a sound strategy that incorporates the people, processes and technology that comprise the foundation of any ITAM program.

ITAM needs to have organizational sponsorship at a level that recognizes the need for dedicated roles in key ITAM functions. With today's focus on lean IT organizations managers can explore sharing ITAM roles with security management roles. For example, and single individual could have a shared role as an Asset Analyst and Configuration Analyst since these roles share similar responsibilities across the ITAM and Infosec domains.

From a process perspective, ITAM and Infosec have shared processes, such as configuration management property accounting, asset disposal and a variety of entitlements support processes. Fundamentally, a set of overall operational management processes that are common to both ITAM and Infosec are needed to establish and maintain the management infrastructure within which the other ITAM processes can be implemented.

There are a variety of tools and technology, whose costs can be rationalized across both organizational needs. For example, it is widely recognized that automated discovery tools can be very effective with identifying those systems that are susceptible to a given set of security vulnerabilities. However, these same tools are critical to the support of any ITAM program.



In fact, it is impossible to implement an effective ITAM process without the successful design, development, implementation and maintenance of accurate ITAM databases, *automatically* updated from the live infrastructure through the use of discovery tools⁽²⁾. Many ITAM technology vendors provide a wide variety of process automation functions in their products that automate key internal controls processes and can simplify demonstrating compliance, help identify technology compliance areas, assign standard roles and responsibilities, alert managers to reporting policy breaches, and facilitate accurate, reconcilable reports. The benefits of utilizing these tools span both ITAM and Infosec domains by:

- Providing pre-built best practices for automating key workflow processes and definitions of roles and responsibilities
- Providing repeatable, measurable and auditable processes necessary to demonstrate compliance with various regulatory mandates
- Empowering lifecycle asset management by developing repeatable and measurable processes that create accountability, efficiency and economy of organizational effort

Ultimately, knowing what systems are in use, those that should be retired or made inactive, as well as what types of applications and software configurations are resident on those systems is a primary component of IT system security. It is vital for an organization to know the configuration of each system in the organization, which systems have not logged onto the network for an unusual period, and hence may be missing, what systems are operating without the most current version of the selected anti-virus software, and which systems have software unauthorized for their use or clearance level.

An appropriately configured IT asset management system will provide management with the information needed to recognize these, and other, situations. Utilizing these systems organizations can determine the level of usage for certain applications and make business and risk decisions on whether to de-install applications which can save licensing fees and lessen the exposure of certain security exploits which might attack a particularly system through the vulnerability inherent in these applications. The author remembers one organization that was hit very hard by a worm that took advantage of security vulnerabilities in Microsoft Internet Information Server. Although only a small percentage of the hundreds on computers actually had a valid business need to have this application installed, the IT department had inadvertently installed

the application in a standard desktop image that was used to install new systems after they were purchased and delivered to the company. Consequently, when the worm hit there were hundreds of additional systems that helped spread the worm that could have been avoided by the installation and use of a very basic IT asset management system.

Ultimately, clearly synergistic links exist between ITAM and Information Security efforts. Unfortunately, barriers do exist in many organizations to get the staff involved in managing corporate assets from an accounting perspective and those that manage them from an information security perspective to work together effectively. However, smart managers will continue to look to find ways to provide incentives for these two groups to work together and leverage the technology that can be shared by both functions.

Steve Gerick is an ITAM expert at Siemens Business Services

