

IT Accountability

Simple IT Blind Spots Can Derail Even the Most Strategic IT Department

As IT departments evolve into larger, more sophisticated and more strategically relevant divisions within organizations, expectations of business alignment and accountability for every IT dollar and decision swell within management ranks. However, this breakneck pace of change can cause even the most savvy IT professional to lose sight of the very fundamentals of accountability that enable strategic-level success in the first place.

Consider this litmus test: Your CFO requests answers to several questions; can you deliver answers in 30 minutes or less?

- Is all of our software legally licensed? If audited by a software vendor, would we be at risk of prosecution?
- Are employees running applications that represent security threats?
- How many of those expensive CRM licenses purchased last year are actually being used?
- Will a migration to Vista require major new investments in hardware?
- If a business unit were wiped out by a flood, how would we know what hardware or software assets were lost?

If you can't confidently answer questions of this nature, your organization is at risk either legally or financially. This is where bad things suddenly happen to good IT people – people who have the strategic interests of the enterprise at heart, but lack the comprehensive insight into the network assets and utilization needed to eliminate critical blind spots and avoid catastrophe.

As with driving an automobile, eliminating the blind spots means adjusting the mirrors and looking at things from a different angle. IT executives must secure resources for IT asset management (ITAM) processes and auto-discovery tools that will provide much-needed visibility—and therefore control—over the inventory and usage of IT assets. With such tools in place, not only can IT departments more effectively avoid nasty surprises, but they can also free up costly overhead associated with routine manual processes and unnecessary fire drills—

devoting more time to mission-critical operations and other strategic projects.

Here are some of the blind spots you can overcome and avoid by achieving a deeper understanding of the desktop environment:

1) Corporate software piracy

According to the Business Software Alliance (BSA), more than 20 percent of installed software in the U.S. is non-compliant. The ramifications of corporate software piracy can be enormous: copyright infringement penalties of up to \$150,000 per infringed-upon title (not including legal fees), business disruption associated with protracted lawsuits and eroded goodwill. In extreme cases, companies have been temporarily shut down for violating their licensing agreements.

ITAM tools enable IT staff to perform automated inventories of all the software and hardware installed across the desktop environment and reconcile that data with purchasing information. This allows organizations to conduct periodic internal compliance audits and take corrective action.

2) Harmful applications on the network

While most IT departments devote extensive resources to averting external security threats, few bother to determine the extent to which employees' use of technology introduces *internal* risks to data security, productivity or network performance. In fact, studies have shown that over half of security breaches—whether malicious or unintentional—occur inside the corporate firewall. Obvious threats include hacking programs and spyware, but even common P2P or chat applications can pose security or regulatory risks if not used appropriately. Furthermore, organizations commonly install applications containing sensitive data on company servers without regard for who's able to access them, making this information extremely vulnerable.

ITAM tools can track both the inventory and usage of software assets, allowing IT professionals to identify exactly what's installed on employees' desktop and network servers; and what's actually being used by employees. Staff can then determine

what programs are potential threats and either uninstall the software or prevent it from launching. ITAM tools can further augment security measures by revealing which computers lack specific software—for example, critical security updates or antivirus applications.

3) Software overspending

IT departments are constantly challenged to eliminate unnecessary spending, yet it's surprising how few monitor the actual use of their investments. According to a Morgan Stanley survey, only 12 percent of CIOs believed they had unused CRM licenses; however, an AMR Research poll revealed that most companies with CRM software had implemented fewer than 50 percent of their licenses. Ironically, efforts to obtain volume licensing discounts and remain compliant often result in purchasing far more software than is actually needed—any volume savings are therefore wiped out by unnecessary support and upgrade fees.

By tracking software usage, IT professionals can determine which applications have not been used over specified timeframes. With this information, purchasing agents can negotiate licensing agreements that more closely match end users' needs—and ultimately save money.

4) Upgrade and migration nightmares

Business strategies often involve distributing new technology to employees. How can IT be accountable for deployment timelines and successful implementations without visibility into which computers can accommodate the new technology and which ones require significant upgrades? This question is particularly relevant with the release of Microsoft Vista and its hefty hardware requirements, as well as its incompatibility with scores of mission-critical applications. Many organizations deal with such challenges on a “one-off” basis, devoting significant resources and overhead to conducting manual inventories of every desktop. Without doubt, this is an extremely time-consuming, error-prone, unscalable practice that drains countless IT hours that could be devoted to the migration itself.

Hardware inventory functionality found within most ITAM solutions allow IT staff to determine whether desktops have the necessary hardware capabilities (such as processor speed, memory, and available disk space) to deploy new technology. Likewise, software inventory information can help IT professionals identify which machines have software known to be incompatible.

5) Widespread computer loss

When computers are lost to disaster, theft or negligence, not only are employees left without the tools they need to perform their jobs, but proprietary data can be lost or, worse yet, fall into the wrong hands. Valuable information regarding what specific applications reside on a particular computer vanishes, leaving IT staff scrambling to file accurate insurance claims and get users back online as quickly as possible. Imagine the difficulty of such tasks without a paper trail documenting the software versions and hardware capabilities, along with their corresponding asset values.

PC inventory data collected by ITAM tools can facilitate quick and organized recoveries by providing comprehensive summaries of what software licenses and files were installed on a computer, its hardware capabilities, and the purchasing data associated with the computer's assets. Furthermore, certain ITAM tools, by recording a “heartbeat” for networked machines and details of each login, can provide critical clues that reveal when the missing computer was last used, and by whom.

As you consider whether your organization is able to satisfactorily steer clear of these blind spots, ask yourself whether your staff is equipped with both the tools and executive support to do so. You'll be surprised at just how simple—and reassuring—it is to empower your department to take responsibility for these critical areas.

Indeed, the era of IT being purely a cost of doing business, a bottleneck, or a black hole is quickly dissolving into a new regime of accountability and contribution to the strategic initiatives of the organization. IT leaders who recognize this shift and organize to accommodate it will find more support for their own initiatives from C-level executives who believe IT and management are kindred spirits pursuing the same goals.

*Kris Barker
CEO of Express Matrix LLC*