theoutsourcinginstitute
@outsourcing.com

How to Avoid Being Overrun by Shadow IT

When business users—and sometimes even IT personnel—"go rogue" and deploy unsanctioned equipment and applications, a lot of problems can occur. Here's a guide to the causes, implications and solutions of shadow IT.

By James Avellino
Practice Director - Cloud Services, Pomeroy

POMEROY
infrastructure. optimized.℠

The pressure on IT organizations is enormous and growing every day. IT's role in driving business outcomes has never been more integral, nor has it ever been this challenging in the face of tighter budgets, smaller staffs, more demanding business constituents and rapid changes in technology.

Combine these trends with the reality of an increasingly technically-savvy user base, and it's easy to understand that IT's internal constituents have become more and more anxious about what they perceive to be the slow pace (and perhaps rising cost) of deploying new applications and services. This end-user comfort level of technology is driving increased incidence of what is being termed “shadow IT,” a trend that has important and potentially risky implications for nearly all organizations.

Shadow IT, defined by SearchCloudComputing.com as “hardware or software within an enterprise that is not supported by the organization's central IT department,” is hardly a new phenomenon. It first started to surface in the 1980s as personal computers and other relatively affordable and easily installed equipment and software found its way into businesses. But as technology has continued to evolve and users have become more and more comfortable and confident in deploying or using products without IT's help or involvement, the stakes have been raised tremendously. For instance, instead of users trying to deal with departmental printing queues, organizations are allowing users to deploy their own printers, computers and personally owned or individually contracted cloud-based services.

How pervasive is shadow IT? A recent report from research firm Frost & Sullivan highlighted its growing footprint in businesses: Over 80% of IT and line of business professionals surveyed admit to using unapproved applications accessed through a Software-as-a-Service subscription, adding that more than one-third of SaaS-based applications are purchased and used without oversight.[1] These included increasingly popular and widely used cloud-based applications such as Office 365 and Google Apps.

Other resources frequently sought out include online storage (e.g., Dropbox, Box, Google Drive, SkyDrive), online office tools (e.g., Google Docs, Live Documents), web-based email (e.g., Gmail, Hotmail, Zoho), survey tools (e.g., SurveyMonkey), email marketing (e.g., MailChimp), and CRM tools (e.g., Zoho, Salesforce.com).

This is not to say that those resources should never be used. However, if they are

[1] “The Hidden Truth Behind Shadow IT,” Frost & Sullivan, November 2013

used it should be with the knowledge of the company's IT department.

Causes of Shadow IT

There are numerous trends and factors driving the increase in shadow IT. Some are natural byproducts of rapid technological improvements and an increasingly sophisticated user community, while others are, unfortunately, results of user frustration with their organization's IT department and its perceived inability to meet their needs.

- IT budgets and staff are not growing as fast as in prior years, and especially are not keeping up with the rate of increase in user demands for new applications and additional IT-enabled services.
- IT organizations' tight resources are still being used primarily for “keep the lights on” requirements, such as security patching, help desk inquiries, onboarding new users, rolling out new applications and periodic planned and unplanned service downtime.
- The much-discussed “consumerization of IT” has introduced personal technologies such as tablets, smartphones and consumer applications into the enterprise, largely due to users' increased comfort with deploying and managing technology without IT support.

Of course, many business users are literally taking matters into their own hands as a result of growing frustration with the IT department's inability to give them what they want, when they want it. Other times, however, users are motivated by a more positive goal of reducing the onus on the overworked IT department by handling what they consider to be relatively simple deployments on their own.

Regardless of what may be driving shadow IT, however, it often results in a critical breakdown in communications between business users and the corporate IT department.

It's important to understand that shadow IT isn't just an inconvenience; it's a big and growing problem. For instance, growing awareness and acceptance of cloud computing—especially high-visibility public clouds such as Amazon Web Services (AWS) and Apple iCloud—have resulted in business users easily and quickly setting up cloud environments for key workloads.

The trend of employees using public cloud services without permission is growing due to the ease with which they can attain these services. Subscription-based cloud services offer an attractive alternative for employees to streamline their work activities, collaborate easily with colleagues and be more productive. Cloud services are often easy to adopt; free trials, inexpensive subscriptions, easy-to-cancel policies, all create a situation in which to lower the barrier to adoption of cloud services by employees. Hence, ad hoc adoption of cloud services at all levels in the enterprise is on a very steep rise.

Spinning up dedicated servers in the cloud, however, can come with real risk when the process isn't properly vetted by those familiar with the organization's governance and security policies. A study by research firm Ponemon Institute, noted that 62% of respondents do not agree or are unsure that cloud services are thoroughly vetted before deployment. Ponemon also pointed out, “respondents believe their organizations are relying on functions outside (IT) security to protect data in the cloud.”[2]

The implications of Shadow IT
Shadow IT can exact a serious price on the organization when it is not identified or accounted for. Among the potential challenges organizations can face as a result include:

- Security breaches
- Data leakage/loss
- Disaster recovery/business continuity vulnerabilities
- Compliance/regulatory/privacy issues
- Cost inefficiencies
- Duplication of services
- Impact on increasingly virtual and distributed organizations
    - Remote offices, telecommuters, trading partners, customers
- Inability to get a full assessment of the impact IT is having on business outcomes
- Lack of alignment of IT services and solutions with business goals

Taking proper safeguards
One of the first steps that should be taken by organizations is acknowledging that shadow IT most likely exists to at least some degree within the organization. Avoiding the problem or living in a state of denial will only exacerbate the problem.

In order to confront shadow IT head-on, organizations need to first undertake a thorough audit and analysis of applications and services running on their infrastructure or are contracted through outside services such as cloud service providers or subscription-based applications. Although the IT organization may be willing and able to do this on their own, the IT department's workload and/or lack of experience in spotting shadow IT lurking on the edges of its infrastructure may necessitate working with an experienced third party to conduct the audit and assessment.

It's also important that the risks of shadow IT are communicated to the user base, and to clearly articulate the corporate policy regarding usage of SaaS and other cloud technology; awareness is the first solution key. If you have no policy, start building one.

This is an excellent opportunity to establish a more interactive discussion among business users in order to ensure the IT department hears and understands their needs, and can thus identify ways to improve services. Additionally, the IT group then can create a more comprehensive IT framework that integrates relevant and appropriate IT functions in order to enable employees without putting the organization at undue risk.

Finally, identifying shadow IT instances and sources presents a

[2] Data Breach: The cloud multiplier effect, Ponemon Institute, June 2014

great opportunity to develop modernized policies and put in place management techniques that aren't unnecessarily onerous.

Remember that cloud adoption and usage is part of a much broader transformation of the role IT plays in the organization. IT departments should focus on how the enterprise as a whole uses technology effectively. Additionally, cloud computing enables IT teams to build better bridges to the business, rehash all inputs and develop an equitable go-forward plan. As a result, IT can be positioned as dynamic, thought leading, and business attentive by bringing value to the process and looking at ways to improve the organization's financial footing by cutting costs and creating new revenue opportunities.

Conclusion

Shadow IT may not be a new phenomenon, but it clearly is on the uptick. Even more important, however, is the reality that the implications of shadow IT are more onerous than ever because of issues such as the growing criticality of data security and the need to protect against data loss for compliance, e-discovery and 24/7 data availability.

IT organizations—and their line-of-business colleagues—need to be extremely vigilant in spotting instances of shadow IT and to take proactive steps to mitigate its impact on the organization. At the same time, organizations should take all necessary steps to ensure that shadow IT doesn't crop up in the first place. In this effort, enterprises of all sizes should look to team with experienced, reputable third parties with hands-on expertise in dealing with shadow IT.

How Pomeroy can help

One company with expertise in working with organizations to reduce and even eliminate shadow IT is Pomeroy, a leading IT services organization. Pomeroy's mix of cloud and infrastructure assessment services, managed services, professional services, staffing services and procurement/logistics services has made it a go-to partner for many organizations across a wide swath of industries.

Pomeroy works with companies and public sector organizations to address shadow IT in a methodical, systematic process, starting with a deep and broad assessment of the customer's infrastructure environment. Specifically, Pomeroy's solution architects and systems engineers examine and analyze the information that is extracted from the network via a “collector”. The corporate and rogue applications at play are identified, in addition to identifying and detailing infrastructure anomalies and outlining application and server dependencies. A full report is developed and provided to the organization's business management and IT leadership. Action plans are then worked out to help organizations properly leverage the capabilities of cloud computing without putting the company at risk.

About the Author

Jim Avellino is Pomeroy's cloud practice director. With more than 20 years' experience in managed services and providing solutions in IT outsourcing, Jim has a central role in building and guiding Pomeroy's cloud practice and service portfolio. Jim has worked as a strategic consultant designing IT strategy and roadmaps for Fortune 500 companies and has worked internationally as a chief solutions architect leading large deal infrastructure solutions for a Fortune 500 IT services technology firm. Jim has built infrastructure and cloud solutions leveraging public, private and hybrid cloud models for large ITO engagements and worked for several years as a senior director for several managed services providers.

About Pomeroy

Pomeroy provides high-quality IT infrastructure services from its locations throughout the United States, Canada, Latin America and Western Europe. Pomeroy's portfolio of managed services includes: End User Services, including service desk, hardware and software support, asset management, print management and enterprise mobility management; Network Services, including network monitoring and management, network operations and optimization, unified communications and collaboration and telecom expense management; and Data Center Services, including data center operations and optimization, server, storage, virtualization and cloud hosting services. Pomeroy's staffing services include technical experts for staff augmentation, contract staffing and permanent placement. Pomeroy's procurement and logistics services provide rapid hardware and software procurement, staging, configuration and deployment, as well as depot/repair and asset disposition and end-of-life services.

A recognized leader in the End User Services markets, Pomeroy's ITIL-certified professionals employ a process-centric approach to working with clients, either remotely or on premise, to assess, plan, design, build, test, implement, manage and ultimately optimize each client's IT infrastructure, leading to the creation of tangible business value and return on their IT investments.

theoutsourcinginstitute
@outsourcing.com

The Outsourcing Institute
6800 Jericho Turnpike Suite 120 W Syosset NY 11791
USA
Phone: (516) 279-6850 - 712 Fax: (516) 706-2855
www.outsourcing.com