Fighting Back Against "Shadow IT"

A Guide to Embracing Cloud Services to Become a Trusted Advisor

SUNGARD® AVAILABILITY SERVICES™

Table of Contents

Introduction

Shadow IT involves “information technology devices, software and services outside the ownership or control of a company’s IT organization.”[1] This situation arises when business users avoid formal IT processes and procedures due to demand, outstripping an IT organization’s capacity to supply solutions, as well as a changing technology and services landscape. Today, shadow IT may manifest itself through unauthorized applications, the storing and transferring of sensitive data outside of a secure network, or the spinning up of a virtual machine (VM) in an unsanctioned public cloud.

The advent of powerful and rapidly-evolving mobile devices and associated applications has given shadow IT a boost, as has the availability of cloud services. Partly as a result, analysts forecast that by 2019, more than 75% of all new IT projects will be funded by individual business units directly responsible for generating growth.[2]

While the ease of procuring cloud services has undoubtedly contributed to the growth of shadow IT, the solution lies in governance of its adoption and deployment throughout the organization. If properly managed, cloud services can paradoxically reduce instances of shadow IT and help solve the issues around it. This E-book will explore ways to empower business units in order to achieve the agility they desire, while maintaining the proper governance and control that IT administrators require.

[1] Gartner, “How CIOs Should Deal with Shadow IT,” refreshed June 17, 2014, John Mahoney
[2] Gartner, “CEOs Are Signaling the First Significant Change to IT’s Mission in More Than 20 Years,” April 10, 2014, Ken McGee

Recommended steps to reduce shadow IT include:

- Assess the situation and make better governance a priority for the business.
- Identify and cordon off mission-critical applications.
- Consider rehosting mission-critical applications in the cloud to free up IT staff.
- Build a list of approved cloud service providers.
- Work with each business unit to understand their unique needs.
- Empower development within the IT team and business units.

Following these steps will help shift the IT staff into trusted cloud advisors or brokers among the business units. In turn, this will enable better oversight of cloud services and reduce the instances of shadow IT within the organization.

Today, shadow IT may manifest itself through unauthorized applications, the storing and transferring of sensitive data outside of a secure network, or the spinning up of a virtual machine (VM) in an unsanctioned public cloud.

Assess the Situation

Before outlining a solution, it is important to face reality.

For those tempted to say that shadow IT is not found in their organization, consider such popular cloud-based applications as Dropbox, Evernote and Skype. As of 2014, Dropbox had 300 million users[3] and is a business-focused service available to all corporate users. At the same time, Evernote had over 100 million users across all platforms.[4] Skype had about 300 million users[5], with as many as 80 million online at one time in 2014. In addition to these instances, shadow IT could also include the storage and transfer of sensitive data over unsecure networks, or procurement of applications via software-as-a-service (SaaS) deployment models.

A 2013 survey done for a security technology company found that four out of five workers admitted to using shadow IT; respondents indicated that the most common reasons for turning to a non-approved application were: familiarity with it, a slow IT approval process, and better suitability of the non-approved application for the task at hand.[6] Not surprisingly, IT organizations may have little insight into how much shadow IT is present. Take, for example, the actual usage of cloud services. Surveys done by cloud vendors have shown that the number of applications in use in an organization may be 10 to 16 times the number believed to be in use by IT administrators.[7]

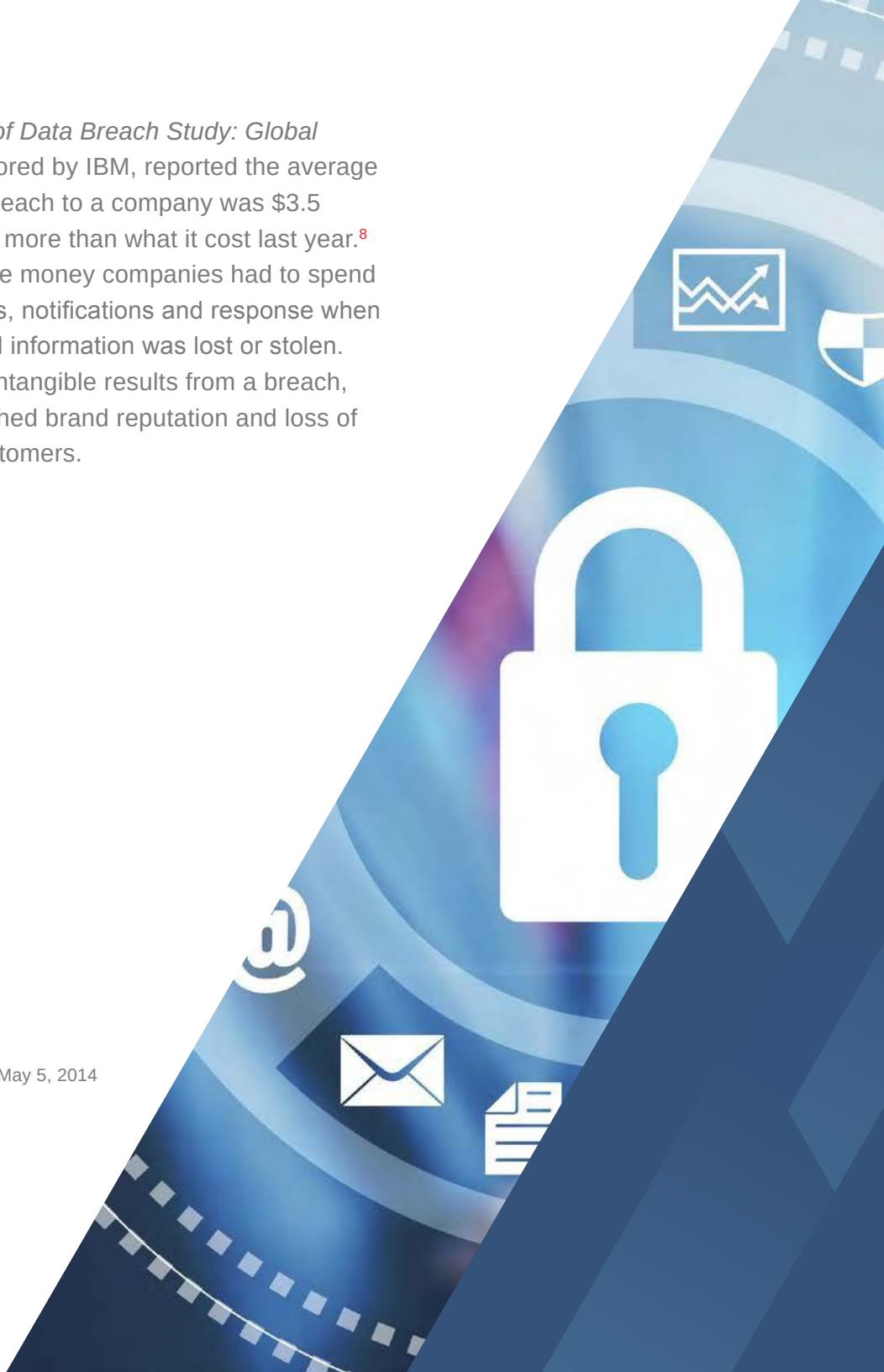
Executing a survey across the business units is one way to better understand the applications that are in use. While implementing this approach, be sure to also ask questions regarding the data being handled and which applications are used to process the data. Also inquire about any integration points with other mission-critical applications.

A 2013 survey done for a security technology company found that four out of five workers admitted to using shadow IT.

[3]The Dropbox Blog, “Thanks for Helping Us Grow,” May 28, 2014
[4]Evernote, “We Have 100 Million People to Thank,” May 13, 2014
[5]TechRadar.Computing, “Microsoft highlights 299M Skype users …,” June 27, 2013
[6]Frost & Sullivan, “The Hidden Truth Behind Shadow IT,” November 2013
[7]CiteWorld, “Workers use ten times more cloud apps than IT thinks,” May 22, 2013

While a survey methodology is a basic starting point, other measures may be required to build a stronger business case for fighting back shadow IT. Penetration tests and external auditors may also be employed to identify issues with particular applications that may be in jeopardy. The findings from these approaches, along with stats that illustrate the costs associated with security breaches and failed compliance audits, should be used to illustrate the importance to the business and the potential negative impacts to the bottom-line from allowing shadow IT to continue.

The *2014 Cost of Data Breach Study: Global Analysis*, sponsored by IBM, reported the average cost of a data breach to a company was $3.5 million and 15% more than what it cost last year.[8] That included the money companies had to spend on investigations, notifications and response when their confidential information was lost or stolen. There are also intangible results from a breach, such as a tarnished brand reputation and loss of trust among customers.



[8]Ponemon Institute, "*Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis,*" May 5, 2014

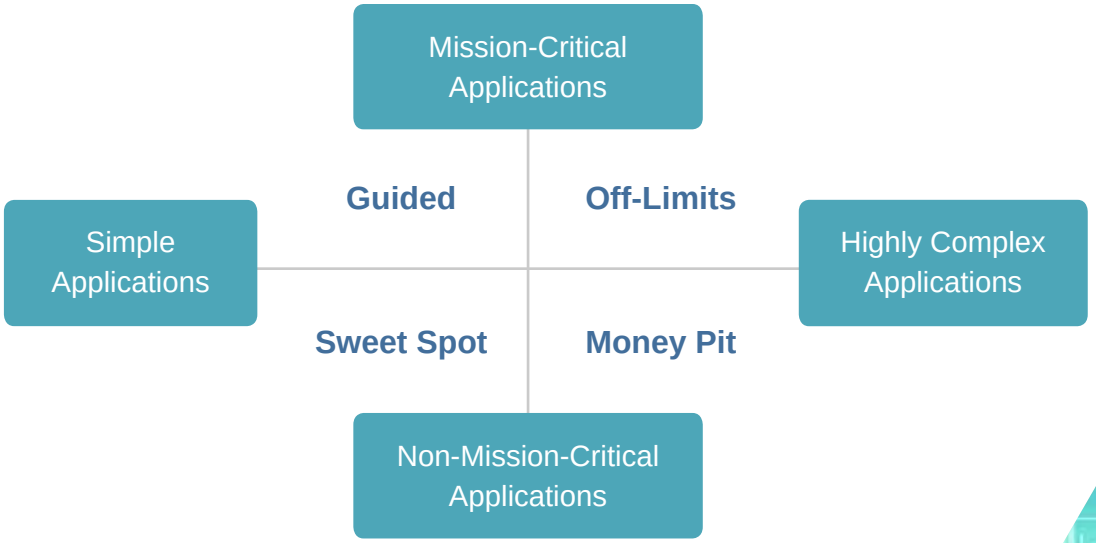
Identify Your Mission-Critical Applications

The second step in controlling this cloud-driven onslaught of shadow IT starts with the acknowledgement that some applications and processes require strict governance and control, while others may only need general oversight. The complexity and sensitivity of the underlying application process should be considered when identifying which applications are mission-critical and which are not.

Customer relationship management (CRM) and enterprise resource planning (ERP) are examples of mission-critical applications with a high degree of complexity. Having either of these unavailable for any length of time is unacceptable. Web conferencing, on the other hand, is an example of a non mission-critical application, as the lack of this capability may be a nuisance, but not catastrophic.

Gartner has provided a matrix (see Figure 1) to help identify the boundaries for shadow IT, illustrating this separation of processes along critical/non-critical and complex/simple axes.

Figure 1. The Boundaries for Shadow IT[9]



[9]Gartner, "Embracing and Creating Value From Shadow IT," May 9, 2014, Simon Mingay

No shadow IT should — or can — be allowed for complex, mission-critical applications and processes, which can be found in the upper right quadrant. Thus, the first step in managing and benefiting from shadow IT lies in defining where it will simply not be permitted.

Having identified the area where shadow IT is not permitted, administrators can then set other boundaries. Opposite of the mission-critical and complex processes resides a region of simple applications and processes that are only an inconvenience if not available.

The two remaining quadrants involve mission-critical, yet simple processes and nice-to-have but complex applications and processes. For all but mission-critical and complex applications, IT organizations must offer guidance. The goal is to have IT administrators function as a cloud advisor or broker when selecting applications and services in these quadrants.

One additional key factor is how much downtime is tolerable. If the answer is none — as might be the case with a customer-facing ecommerce application — then the IT staff should be heavily involved and should drive any decision about integration points and development work supporting the application. If some downtime is acceptable, then service provider metrics — such as recovery plans and service level agreements — become less critical and IT staff involvement can be minimal.

This approach of dividing process along complex/simple and critical/non-critical axes accomplishes several important goals in managing shadow IT. First, it ensures control over what is vital. Second, by allowing users and lines-of-business leeway elsewhere, it allows IT organizations to see what is going on and how to influence it.

The first step in managing and benefiting from shadow IT lies in defining where it will simply not be permitted.

Consider Rehosting Mission-Critical Applications in the Cloud

Now that you have established the boundaries for mission-critical applications, you should consider whether any of these applications could fit into a cloud deployment model. Not all applications will be appropriate to migrate, but cloud technologies are quickly evolving to meet the high-availability, security, and compliance standards that are expected for mission-critical applications like ERP, business intelligence, finance, and others. There are some significant benefits that can be achieved by rehosting these applications in the cloud.

They include:

- Enabling your current IT staff to focus on business unit needs, because they will not need to address the maintenance of hardware refreshes, OS patches, and other time-consuming tasks to support these applications.
- Gaining cost efficiencies by shifting from a CAPEX to an OPEX cost model.
- Greater agility, as the environment can quickly scale up and down as needed, eliminating the need for capacity planning.
- Maintaining resiliency and high-availability of the application, which is commonly backed by service level agreements (SLAs).
- Some cloud service providers have additional managed services that can be leveraged to supplement current staffing challenges with regards to networking, storage, disaster recovery, security, and compliance expertise.

It is important to recognize there may be a cultural challenge when rehosting these mission-critical applications in the cloud, as IT staff may see the strategy as a threat. To mitigate that reaction, verify that internal IT staff members are on board with this approach. Such support can be nurtured by pointing out that the skills and expertise of the IT staff represent abilities and know-how that are highly transferable to the new role of cloud advisor for the business units.

In establishing the parameters for cloud migration, the IT staff should be deeply involved in vendor selection. They must set overall requirements, ensuring that these properly account for compliance considerations. By doing so, the staff will become knowledgeable about service models, vendors in the marketplace, and other key elements of the cloud arena. This breadth of information will be important during the migration, and such knowledge is vital when acting in an advisor or cloud broker role.

In total, rehosting of mission-critical applications in the cloud can increase the overall agility and scalability, while also freeing up staff to focus on understanding the needs of the business units. It will also make your current staff aware of cloud technologies and provide an opportunity to address any cultural concerns that may impede the strategic shift to an advisory role.

Rehosting of mission-critical applications in the cloud can increase the overall agility and scalability, while also freeing up staff to focus on understanding the needs of the business units.

Build a List of Approved Cloud Service Providers

Whether or not you decide to migrate some of your mission-critical applications to a cloud deployment model, you will want to begin to build out requirements for cloud service selection and establish an approved list of vendors. Before doing so, however, ask and get satisfactory answers to some critical questions. These may include:

- What security certifications do you have and what audits have your cloud platforms undergone? (PCI DSS Certification, SSAE 16 Type 2, ISO 20000-1, etc.)
- What SLAs are provided? How is the guaranteed availability measured?
- What additional managed services are they able to provide beyond just Infrastructure-as-a-Service?
- Does the cloud service provider have the expertise to help satisfy industry specific regulatory requirements (HIPAA, PCI DSS, SOX, etc.)?
- Is there multi-site failover of the cloud environment to protect against natural and man-made disasters?
- Are vulnerability scans and other security tests regularly performed to hedge against breaches?
- What is the policy for commissioning and decommissioning hardware? How are changes communicated?
- What are the security policies followed when hiring, training, monitoring, disciplining or terminating personnel?
- What physical security measures are in place at the data center to control access?

It should be noted that the answers to these and other questions can be critically important and can even override pricing. The cost of a single data breach can run into the millions, possibly swamping any savings that arise from going with a less expensive and less secure provider.

In its role as a trusted advisor, the IT organization should match line-of-business customers with potential cloud vendors. Providers offer differing degrees of managed support, and different business units will require varying degrees of support. Aligning the two will boost the chances for success in migration to and usage of cloud services.

The cost of a single data breach can run into the millions, possibly swamping any savings that arise from going with a less expensive and less secure provider.

Work with Business Units to Understand Their Unique Needs

In all of this, it is vital that the IT organization remain aware of applications and the handling of data, as the data flow among and across virtualized environments must be understood for regulatory or compliance considerations. Inadvertently stumbling into a dangerous situation can then be avoided.

To see how easily problems can arise, consider the case of a call center. Sensitive data, such as credit card numbers, which might be collected during customer interactions and stored in an application that does not properly account for the sensitivity of the data. This information can then be transmitted unencrypted. Failure to understand how data is handled from a people, process, and technology standpoint could result in compliance audit failure or compromised customer data.

While surveying business units will provide insights on where to focus your efforts, it is of particular interest that Gartner says the CMO's budget likely will outstrip the CIO's IT budget within a few years, and impact the IT organization.[10] Marketing departments typically leverage a high degree of digital tools when developing applications, and frequently customize APIs to integrate SaaS marketing tools with other applications throughout the business.

[10] Gartner, "Mobilization is Forcing a Role Change for IT," November 27, 2013, Van L. Bakar

More often than not, marketing organizations outsource the development to work agencies without any direction from the IT organization. Once the applications are developed, only then is the IT organization approached to deploy, host, and maintain the application(s). This can present real problems as the IT team may not be able to support languages and frameworks used to develop such applications.

Therefore, engagement with the CMO can be a good place to start building the trusted advisor relationship among business units. This will allow the IT organization to influence the selection of third-party vendors to ensure development work, SaaS cloud deployments and integration with other critical applications is complementary and sustainable. This is just a suggested starting point and the relationship that is established should be carried across the various business units.

Failure to understand how data is handled from a people, process, and technology standpoint could result in compliance audit failure or compromised customer data.

Empower Developers While Maintaining Oversight

As cloud-native applications continue to evolve, so too are the skill sets of your IT staff, as well as members in the business units. Open-source cloud platforms are making it easier to set up test and development environments to customize applications for the unique needs of the business. With this in mind, the final step in managing shadow IT is to provide tools for testing, development, and proof-of-concept work. Here, a self-service public cloud can prove invaluable.

Cloud service providers have made it increasingly easy for developers to establish a public cloud environment. In many cases, this can be done quickly by simply having a credit card and Internet-enabled device. Consequently, it is easy for IT administrators to lose control and oversight of the development work being carried out by the IT team and/or business unit.

To hedge against this, a self-service public cloud should be implemented and development work should be concentrated there. User management controls should be in place to establish workspaces and assign budgets for individual teams and/or projects. Implementing and encouraging development to take place within a single cloud environment will increase oversight into the work being carried out, as well as easing migration of the development work to other stages of the application lifecycle.

The nature of this cloud-enabled process offers two big benefits, both of which help control shadow IT. The first is that it provides a platform for expedited development work, making it less likely that users and lines-of-business will turn to non-sanctioned methods. The second advantage is that the development work itself provides intelligence into the needs of users and lines-of-business. An approved list of vendors makes it possible to gather such information as an organic result of normal activity.

Open-source cloud platforms are making it easier to set up test and development environments to customize applications for the unique needs of the business.

Conclusion

A decade or so ago, the internal IT of a business organization often had a goal of controlling every application and device. This is no longer possible — or even desirable. The advent of cloud services has made shadow IT more prevalent, but the same technology also offers a solution. Implementation of cloud services can be controlled by assessing the situation and making better governance a priority for the business, cordoning off mission-critical applications, rehosting applications in the cloud to free up IT staff, establishing a list of approved cloud vendors, working with the business units to understand their needs, and empowering development work.

While every business faces unique challenges, these recommendations are intended to further increase agility, while maintaining control and governance across a variety of applications and cloud service providers. Business unit budgets are only projected to increase, and shadow IT instances will undoubtedly increase as well if the IT department does not take an advisory role in the selection of cloud services.

SUNGARD® AVAILABILITY SERVICES™

Sungard Availability Services
650 E. Swedesford Road
Wayne, PA 19087

About Sungard Availability Services

Sungard Availability Services provides managed IT services, information availability consulting services, business continuity management software, and disaster recovery services.

To learn more, visit www.sungardas.com or call 1-888-270-3657

Trademark information

Sungard Availability Services is a trademark of SunGard Data Systems Inc. or its affiliate used under license. The Sungard Availability Services logo by itself is a trademark of Sungard Availability Services Capital, Inc. or its affiliate. All other trade names are trademarks or registered trademarks of their respective holders.