eBook

Why Embracing Shadow IT is Good for Your Business

CALIAN®

www.calian.com
1.877.225.4264 | 770 Palladium Drive, Ottawa, ON, K2V 1C8

For increased productivity and efficiency, your employees are embracing Shadow IT—unsanctioned and unknown IT projects like cloud services. The concept is simple: corporate assets are leaving the four walls of a company in such a manner that they can't be tracked or seen. Of course, many employees will be unaware that their actions are exposing the organization to attacks by cyber criminals.

Modern businesses move faster today and IT teams cannot keep up. Together with the ability of the average person to instantly spin up everything from simple file sharing, to web hosting, to even servers and virtual workspaces at the click of a button, it is not surprising that many employees opt for Shadow IT. All of which translates to security risks and compliance nightmares.

According to the Cloud Adoption & Risk Report Q2 2015 by Skyhigh Networks (now McAfee), the average organization has employees using 1,083 different cloud services, many having been installed without IT approval—or even known by IT. With sensitive corporate data uploaded to these services, the organization is exposed and at risk of a data breach. These numbers are climbing quickly: in Q2 2014, only 738 cloud services were used by the average company. Thus, over the span of one year, an organization put into operation a new cloud service—nearly every day (as cited in Null, n.d.).

Shadow IT has continued to grow and according to advisory company CEB, it is estimated that 40% of all IT spending at a company is outside the control of the CIO (Groenfeldt, 2013). This growth is in part driven by the quality of applications in the cloud such as social media, collaboration tools, file sharing apps, and enterprise-class Software-as-a-Service (SaaS) applications. And according to a recent McAfee study, 80% of employees admit to using SaaS applications at work without IT approval, and nearly 35% of all SaaS applications used within the company are not approved and are contributing to Shadow IT (infotechlead, 2013).

CALIAN®

The risks of Shadow IT

The growth of Shadow IT is exacerbated by cloud services, such as AWS (Amazon Web Services), Microsoft's Azure, Office 365, Salesforce, Box, and Yammer, making it easy for employees to acquire and deploy SaaS applications without involving the IT department. Furthermore, cloud services are essential productivity tools, delivering cost savings and enhanced flexibility. As such, employees use cloud services to get their jobs done more efficiently and as quickly as possible. Reasons for doing so include cloud services being easier to use and less restrictive than the organization's systems and services, the organization's approved software is more complex and difficult to work with than alternative IT solutions, or the approved software is incompatible with employees' mobile devices.

The unrestricted use of Shadow IT opens the door for cyber criminals to access the company's data, as well as providing a channel for the data to be extracted. Other risks include:

- Data loss
- Hijacked accounts and compromised credentials
- Regulatory compliance violations
- Unpatched vulnerabilities and errors
- User's personal data mined or used without consent
- Delayed diagnosis and resolution of incidents in a complex and dynamic cloud computing environment
- Persistent threats and DoS and DDoS attacks
- Unauthorized user accessing confidential information in a non-production environment

CALIAN®

Danger of third-party services

Another aspect that has to be considered is if multiple employees and departments are all running different third-party services, with many duplicating the functionality of products approved by the IT department, then the organization is bleeding money which negatively affects the bottom line.

Potential loss of revenue

When corporate IT infrastructure operates slower than the business, then business needs are not being met. So employees turn to unsanctioned Shadow IT to build their own functionalities. And to be fair to them, they are focused on their particular environment and on getting their work done as expeditiously and as efficiently as possible. It is ironic, while they focus on meeting their goals and on profitability for the company, they are exposing their company to cyber criminals and to a serious loss of revenue—and reputation.

Minimum encryption and integration

Cloud services are not particularly secure as 90% do not encrypt data at rest and only 15% support multi-factor authentication (as cited in Plant, 2015). Furthermore, as Shadow IT solutions are unauthorized and unknown, they are unlikely to be integrated with existing networks. Basically, these solutions meet the needs of the individual not the organization, resulting in data silos: employees' home computers and the organization's network.

When Shadow IT appears to be the only option

An employee needs to share documents with external teams such as contractors, developers, advertisers, and so on, but their IT department is unable to give the necessary approval. The solution for the employee is to create a Dropbox account to share the documents as needed to complete the project and to meet corporate objectives. Therefore, when IT cannot support business units and goals, Shadow IT becomes the only option.

When addressing the widespread use of Shadow IT within the organization, what actions can a CIO take to reduce the use of Shadow IT while maintaining productivity, security and compliance with such regulations as PCI (Payment Card Industry), HIPPA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation), or SOX (Sarbanes–Oxley)?

The only solution is to adopt and embrace Shadow IT. Let's look at how this can be accomplished:

1 Create a Shadow IT and Cloud Application Control Strategy

Identify the cloud applications employees are using, monitor the most prevalent apps and associated risks, list those services that support organizational objectives and that meet the risk threshold. Ban those services that are high risk, and adopt those that are safe and useful to the company.

2 Support and guide employees

Employees need the support and guidance of senior management to understand the potential risks inherent in using Shadow IT. They might also require legal assistance to understand the terms and conditions of the cloud services they are using. Building trust between employees, the security and technology teams and business leaders is critical to establish a sense of shared responsibility as the goals of all parties are identical: to build the business and to increase profitability. An understanding of how that is put at risk through the use of unsanctioned cloud services, will help to reduce the prevalence of Shadow IT within the organization. This is essential to ensure employees migrate toward sanctioned cloud services.

3 Give employees the tools they need

Providing a list of approved cloud services will give employees the ability to get their jobs done more efficiently and as quickly as possible—while using only IT pre-approved solutions. This will work as long as the approved apps are those that were once unsanctioned, but are good for the company and accepted by the end user. Therefore, by embracing Shadow IT, end users have the tools they need which will motivate them to work within the system instead of outside the system. This approach lessens the burden on IT, enabling it to focus more on mission-critical projects.

4 Restrict access to corporate data

As many cloud services are not secured with strong encryption, access to corporate data should be controlled to minimize the risk of access for unauthorized purposes. Monitoring the network for company-issued and personal devices will help to compile a complete list of devices within the corporate structure. Every wireless device connected to the network should have an authorized configuration and security profile, and there should be a hierarchy of access based on job roles. If there are new or unknown devices, it will enable Shadow IT to be identified.

5 Implement CASB and DLP technologies

By embracing such technologies as Cloud Access Security Broker (CASB), and implementing smart solutions as they relate to Data Loss Prevention (DLP), amongst other measures—what was once a forbidden practice will become commonplace and well secured. CASB delivers four primary security services: visibility, compliance, data security, and threat protection. It also protects cloud-hosted data and delivers enterprise-class security controls so that organizations can incorporate SaaS and Infrastructure-as-a-Service (IaaS) into their existing security architecture. And DLP prevents or protects users from sending sensitive information or critical information outside the corporate network.

6 Protect data with new technologies

These include data-marking tools that can be tied to trusted-party authentication technology; digital watermarks enabling data to be tracked; and data hashing that creates a hash, or specific code, to identify a given dataset (Plant, 2015).

Benefits of embracing Shadow IT

Amazing as it sounds, after assessing the risks, there are benefits to embracing Shadow IT:

- Enables employees to create their own solutions using pre-approved applications and services—which were once in the domain of Shadow IT.
- Reduces calls on the IT department so it can focus on other mission-critical tasks.
- Increases productivity and efficiency without the actual use of Shadow IT, reducing the risk of a cyber attack and enhancing data security.
- Aligns solutions with business needs and ensures data is integrated into existing corporate networks.

The bottom line is it is a continuous balancing act. The majority of employees today grew up with technology and have a greater understanding of technology and what it can do for them. They have little patience with the traditional mandate from IT of what to use and what not to use to meet their job responsibilities. Hence, the widespread and growing use of Shadow IT—a McAfee 2013 survey revealed that over 80% of corporate workers store company data in unsanctioned apps (as cited in Brisco, 2018).

Shadow IT is an offshoot of the latest generation taking advantage of all the technology tools available—even when they are not approved by the company. They are a generation that will not adapt to technology that does not work for them, but will seek out technology that does and that enables them to work efficiently and effectively.

Businesses do not have a choice: It is embrace Shadow IT and create a collaborative environment between employees, IT, security, and business leaders. What other choice is there?

Contact us for a **free consultation or to receive a free Cloud Security Audit** to assess the effectiveness of your current cyber security initiatives.

1.877.225.4264

www.calian.com

CALIAN®