Stratecast | FROST & SULLIVAN

50 Years of Growth, Innovation and Leadership

The Hidden Truth Behind Shadow IT

Six trends impacting your security posture

An Executive Brief
Sponsored by
McAfee

November 2013

www.frost.com

THE HIDDEN TRUTH BEHIND SHADOW IT

Six trends impacting your security posture

INTRODUCTION

Just a few years ago, the industry was all abuzz about employees who insisted on using their personal iPhones and iPads to access business applications. Within IT circles, the discussion quickly shifted from "how to stop it" (you can't) to "how to protect your business while giving employees the freedom to make choices." Today, many companies report greater productivity and higher employee satisfaction from their Bring Your Own Device, or BYOD, policies.

Are we headed for a similar discussion based around employees' choice of the applications they utilize in business? Are we facing a BYOA (Bring Your Own Application) revolution, in which employees claim the right to choose the tools with which they get their work done, while IT scrambles to protect corporate assets?

The revolution is already here, according to the results of a recent Stratecast survey. Thanks to the ease of access to Software as a Service (SaaS) applications, even non-technical employees feel comfortable and entitled to choose their software—and they are doing so in droves. In many cases, IT departments and security officers are unaware of the extent of "shadow IT," and therefore unprepared to deal with it.

In this paper, we take a look at the state of "shadow IT" in companies worldwide. We reveal some surprising results from the Stratecast survey of IT and Line of Business employees. Finally, we offer tips to IT and business leaders to help them start addressing the risks associated with shadow IT in their own companies.

DEFINING "SHADOW IT"

In this paper, Stratecast broadly defines "shadow IT" as SaaS applications used by employees for business, which have not been approved by the IT department or obtained according to IT policies. The non-approved applications may be adopted by individual employees, or by an entire workgroup or department. Note that we specified that the non-approved applications must be used for work tasks; this study is not about tracking employees' personal Internet usage on company time (e.g., checking sports scores or updating personal Facebook profiles).

The cloud, and particularly the SaaS delivery model, is responsible for the rise of shadow IT in business. In the SaaS model, the software vendor is responsible for hosting and maintaining the application, which users access via a network. For corporate IT

departments, choosing SaaS over traditional licensed software offers a number of benefits. Since the application vendor hosts the software, the enterprise IT department can avoid capital investments in infrastructure. In addition, the vendor is responsible for operational tasks, including infrastructure maintenance, testing, provisioning, upgrades and refreshes, capacity planning, and performance management. Backup and recovery for data and infrastructure is also largely the responsibility of the vendor in a SaaS environment.

The benefits of the SaaS model are not restricted to corporate IT. For users, SaaS is characterized by:

- **Ease of access** – Users can access SaaS apps via the Internet, using their Internet browser, from any Internet-accessible device. In most cases, little or no client-side software is required, which means that the SaaS solution leaves no "footprint" on company-owned devices.
- **Ease of maintenance** – SaaS apps are maintained by the provider. Users have no responsibility for patches or updates.
- **Free or low cost** – Many software providers offer a limited functionality or limited capacity version of their applications at no cost. Other SaaS applications are available at a low monthly fee, payable by credit card (no corporate purchase order required). SaaS subscriptions can often be terminated at any time, with no strings attached.
- **Quick deployment** – SaaS is available on demand, with a click of the "accept" button on the Terms and Conditions page. Users do not have to wait weeks or months for server provisioning and application deployment (assuming the request is approved).

Consumers have embraced SaaS; in fact, a whole generation of users has never loaded software onto a personal computer. It should come as no surprise that those same users carry their experiences and expectations into the workplace.

But, the decisions users make in their personal lives generally affect only themselves. In a business setting, the decisions an employee makes can impact the entire corporation. This is why the stewards of corporate assets (who include not only IT, but also compliance, security, and general business executives) need to understand, assess, and respond to the risks associated with shadow IT.

THE REAL STORY BEHIND SHADOW IT

There seems to be a general industry consensus that shadow IT exists, but little understanding of the details. How pervasive is it? Who are the perpetrators? What is driving them? Do they understand the risks?

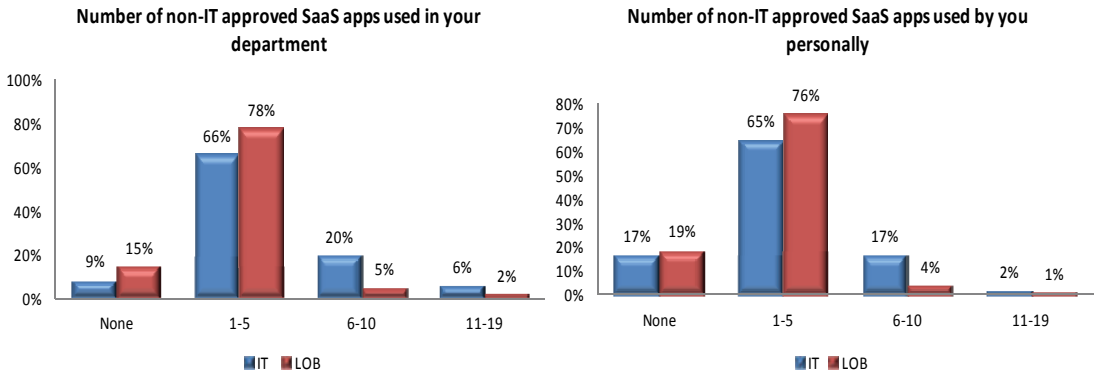
To get to the facts, Stratecast conducted a survey of IT employees and Line of Business (LoB) employees who identified themselves as either "decision-makers" or "influencers" of software purchases in their companies.[1] Some findings conformed to our expectations; many others surprised us. And all provide valuable insight necessary to help companies make the right decisions.

Here are six findings that should change how you approach Shadow IT:

1. Everyone does it.

More than 80 percent of survey respondents admit to using non-approved SaaS applications in their jobs. As shown in Figure 1, only 19 percent of Line of Business employees and 17 percent of IT employees *do not use* any non-approved SaaS applications.

Figure 1: Non-Approved App Usage, LoB vs. IT



Source: Stratecast

Furthermore, non-approved applications represent a sizeable proportion of all SaaS apps used in a company. According to respondents, the average company utilizes around 20 SaaS applications; of these, more than 7 are non-approved. **That means you can expect that upwards of 35 percent of all SaaS apps in your company are purchased and used without oversight.**

The high penetration of non-approved apps argues that such usage is no longer in the shadows, but very open. Furthermore, the similar numbers of departmental and individual users suggests that, while a particular SaaS application may not have been approved by IT, it likely is being overtly or tacitly supported by the employee's own department. This indicates that corporate and departmental policies or practices may clash—with the department winning.

[1] The Stratecast SaaS survey was conducted via the Web in September 2013. Valid responses were returned by 300 IT employees and 300 Line of Business employees of large businesses (1,000 employees or more), representing a range of industries, in three geographic areas (North America, U.K., Australia/New Zealand).

2. We have met the enemy, and he is us.

Another surprising revelation shown in Figure 1 is that IT users are *even more likely* than LoB users to adopt non-approved SaaS. Furthermore, IT employees use a higher number of non-approved SaaS applications than LoB. It appears that, in acting as the guardian of corporate technology, the IT department considers itself exempt. Stratecast suspects that this is a case of IT employees' overconfidence in their ability to assess risks, as well as their greater familiarity with a range of SaaS solutions. Like parents who down a latte and doughnut while admonishing their children to eat a healthy breakfast, it may be a case of "do as I say, not as I do."

The challenge for corporate executives is that such confidence can rarely be justified on such a broad scale; and yet, IT technicians have the tools and administrative rights that make it easy to circumvent any technical solution to the shadow IT problem. As a result, it will be necessary to gain buy-in from IT employees for the corporate SaaS policy.

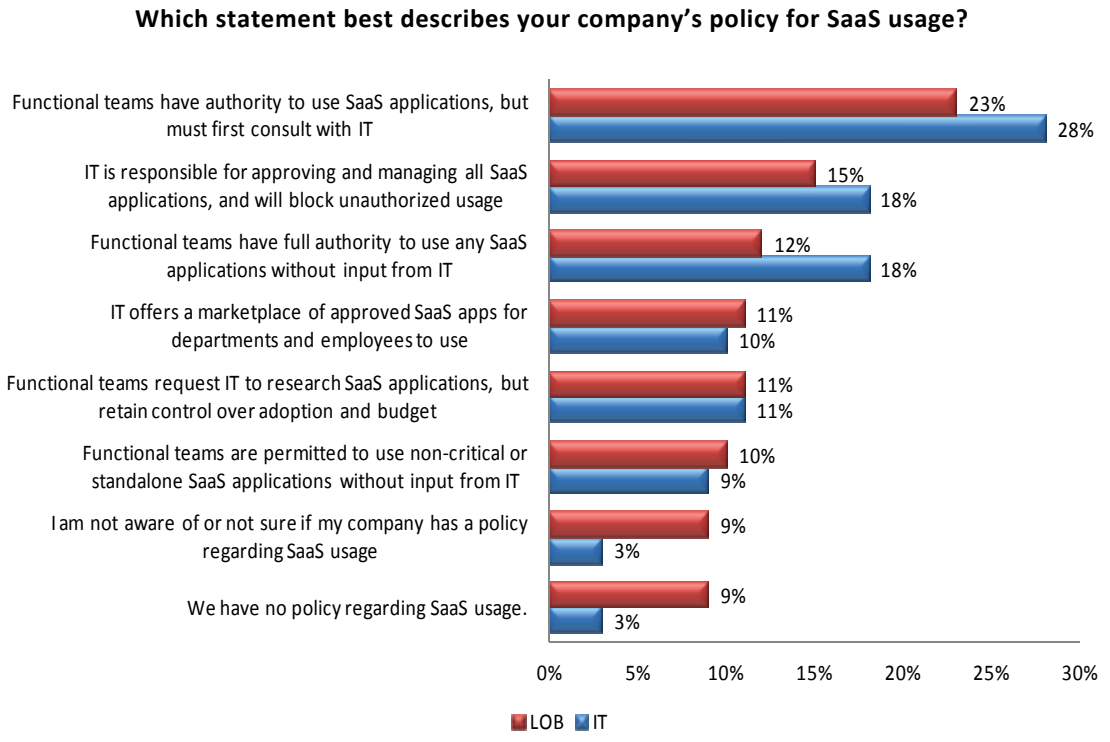
3. Lack of clear consensus and poor communication plague SaaS policies.

The employees who responded to our survey came from sizeable companies—two-thirds from companies with 1000-10,000 employees, and one-third from companies with more than 10,000. It can be expected that these companies have a number of well-honed and well-communicated policies in place—for attendance, expense reporting, hiring, and so on. We can also assume that in developing their policies, such businesses adopt best practices in their industries; thus, their policies tend to be very similar across companies.

Not so when it comes to SaaS policies. As shown in Figure 2 below, both IT and LoB respondents indicate a broad range of policies, with the top choice cited by just over 25 percent. This reflects confusion in the market over the best way to approach the issue of shadow IT.

We can also look at the responses in Figure 2 as a gauge to respondents' knowledge and understanding of their corporate SaaS policies. In this case, we see indicators of communication problems. At the bottom of the chart, LoB respondents are more likely than IT respondents to say they are "not sure" if their company has a SaaS policy and to declare "we have no policy." Responsibility for such confusion falls squarely on the company's shoulders: you can't expect employees to adhere to a policy that they are unclear about.

Figure 2: Corporate SaaS Policies



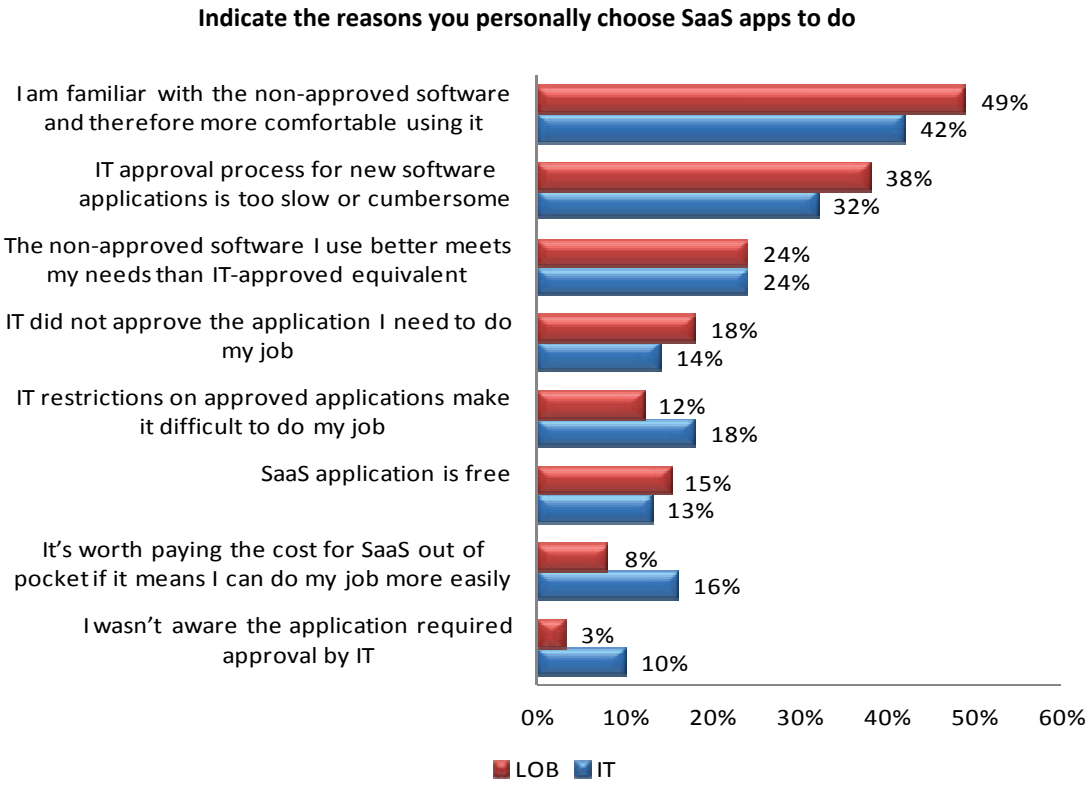
Source: Stratecast

4. Employees just want to do their jobs.

What drives employees to "go rogue"? Is it boredom? Restless energy? A desire to rebel? Alas, the truth is less romantic. It turns out users overwhelmingly turn to non-approved apps for one reason: they need to get their jobs done.

As shown in Figure 3 below, the top drivers cited by both LoB and IT respondents are related to gaining access to the right tools, fast. Nearly half of respondents indicate a comfort level with their preferred software package. While whimsical personal preferences may play a role, it is equally likely that respondents' familiarity with a package means they can avoid a learning curve and thus get their work done more quickly. Users also cite slow approval processes for new software, and inadequacies of "approved" software.

Figure 3: Drivers for Adoption of Non-Approved SaaS



Source: Stratecast

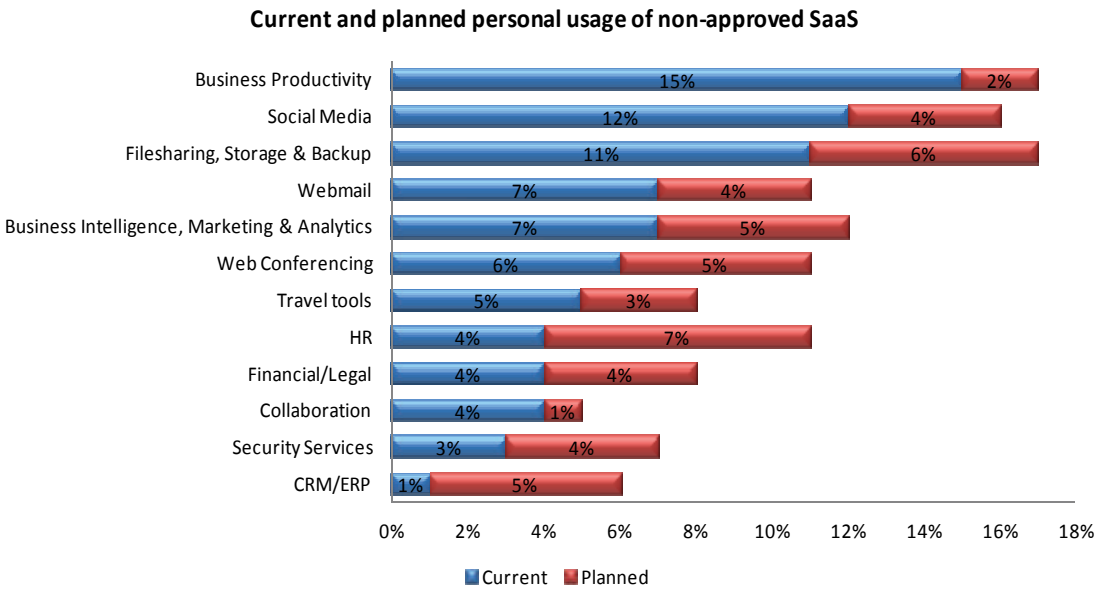
This points to a conflict that falls on the company's leadership team. In a hypercompetitive global business environment, in which companies are looking to increase tight margins, employees are increasingly being measured on results—in some cases, with their jobs at risk. So, they will do whatever it takes to meet their job objectives, which presumably contribute to the company's own business objectives. If that means taking some shortcuts with burdensome company processes, then the tradeoff appears to be a smart business decision. In fact, in many companies, those who attain stellar results are often praised for their willingness to take risks and "think out of the box."

The solution is for the company to develop policies that strike the right balance between flexibility and control. IT and business leaders need to work together to create and support policies that enable employees to use the apps they need to be productive, with controls in place to protect data and minimize corporate risk.

5. Non-approved SaaS usage extends across all application types.

It's not just Facebook that your employees are accessing, without approval, to do their work. As shown in Figure 4, non-approved SaaS encompasses every category. Business productivity (e.g., word processing, spreadsheets) is the top category, with a whopping 15 percent of all employees admitting to utilizing applications such as Microsoft Office 365 and Google Apps. Social media applications, led by LinkedIn and Facebook, are used by 12 percent of respondents, without official approval; and Filesharing, Storage, and Backup applications (including Dropbox and Apple iCloud) follow at 11 percent.

Figure 4: Application Categories of Non-Approved SaaS, All Respondents



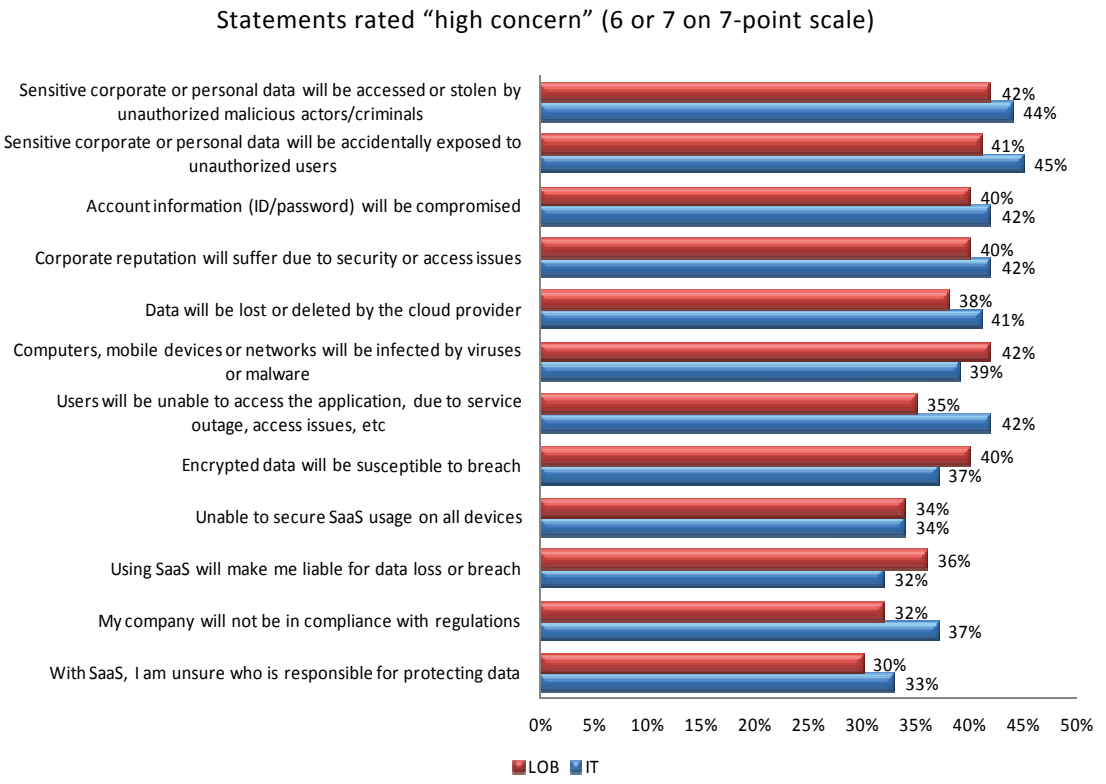
Source: Stratecast

Also noteworthy is that every category is poised to experience increased numbers of users willing to adopt non-approved software. Non-approved usage in categories associated with proprietary data (including HR, ERP, and financial/legal) are expected to grow at an even greater rate. This indicates that whole departments or divisions feel comfortable breaking away from the corporate systems to implement their own choice of software. In fact, they are even now making plans that deliberately circumvent corporate processes for software adoption.

6. Employees recognize risks, but feel they are justified.

A somewhat surprising revelation is the degree to which employees recognize the risks associated with using non-approved SaaS. As shown in Figure 5, LoB and IT respondents showed similar patterns in assessing degree of risk, with one-third or more of respondents claiming they have a "high level" of concern over every risk factor presented.

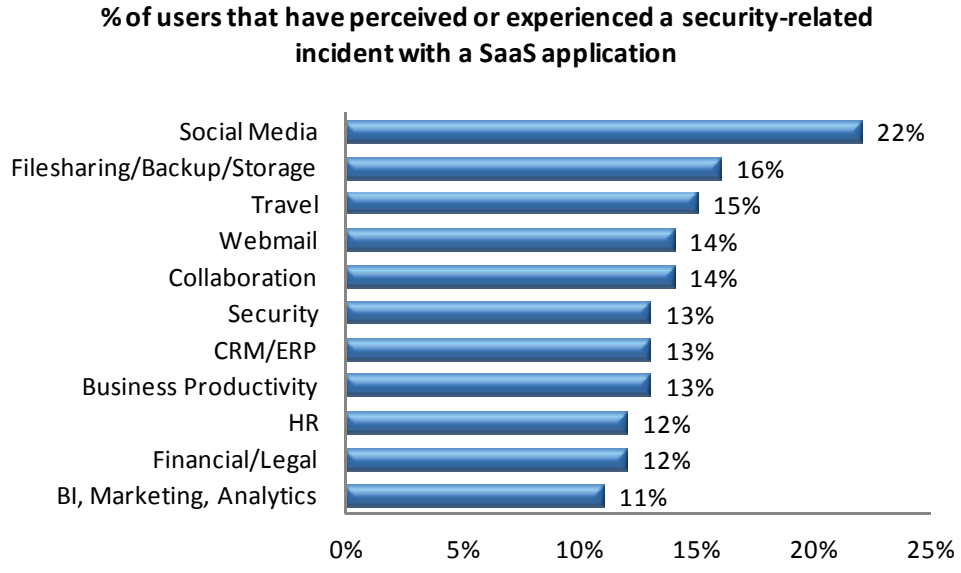
Figure 5: Level of Concern over Security, Access, or Liability Risks



Source: Stratecast

Furthermore, the risk perceptions are largely backed up by experience rather than hearsay. About 15 percent of all employees have experienced or perceived one or more "incidents" (for example, malware infection, data loss, unauthorized or blocked access) associated with using a particular SaaS application. Figure 6 below shows average responses by SaaS category. Not surprisingly, the highest number of users (by percentage) says they have experienced incidents with social media applications (which are, by their nature, designed to reach the broadest number of users). Perhaps more surprising is that the other categories are statistically very close in the percentage of users that have experienced issues. That indicates that no SaaS category is immune from incidents.

Figure 6:
Users Experiencing or Perceiving a SaaS Security Incident, by Category



Source: Stratecast

Correlating the behavior with the perceptions is not so simple. Generally, for both business and personal transactions, risk experience drives behavior. Drop your iPhone once, and it's a good bet you'll add a protection plan to your next purchase. Just knowing someone who suffered the damages of a flood or hurricane is likely to prompt a review of your own insurance coverage.

But SaaS risks appear not to drive that same thought process. Despite their experiences and expressions of deep concern, more than 80 percent of respondents presumably feel justified in continuing to use the non-approved services without ensuring that protective IT policies are applied. Is it "threat fatigue," resulting from constant exposure to shrill reminders of dangers we face in every area of our lives (from genetically modified food to terrorist attacks to NSA privacy invasions)? Is it optimism—the belief that, while bad things happen, they certainly won't happen to us? In the case of IT employees, is it overconfidence—the unsupported belief that they know how to detect and deflect any risks in their own SaaS use? Most likely, it's simply a conviction that "the end justifies the means."

Yet, as every risk and security officer knows, bad things can happen even when the employee has the best of intentions. And the company—not the individual employee—suffers the damages from a security incident. That's why it is essential for businesses to stop treating non-approved SaaS as a minor nuisance; and to accept that its broad penetration and unmanaged scope catapult Shadow IT into a serious threat that calls for immediate attention.

STEPS YOU NEED TO TAKE NOW TO ADDRESS SHADOW IT

So, how can a company protect itself from the risks of Shadow IT? Whether the responsibility falls to the Chief Information Security Officer, CIO, or other business leaders, it is important to establish and implement an approach that protects your business, without implementing a police state. Here are tips for getting started:

1. **Establish a SaaS policy that aligns with your business objectives.** Do you see yourself as an innovative company? Are you looking to out-maneuver competitors by being agile and responsive? If so, you need to ensure that your employees have the freedom to find creative solutions to business problems, and easy access to the tools they need to make your business successful. That calls for a broad SaaS policy, rather than a restrictive one. It can also be noted that a heavy-handed policy—one that seeks to shut down any SaaS usage beyond a limited number of approved apps—will likely backfire. You will not only be at a competitive disadvantage in hiring and retaining younger workers, who expect freedom in selecting applications, but you will squelch the kind of innovative thinking that characterizes successful companies.
2. **Protect your enterprise in a way that is transparent and comprehensive.** Choose a security solution that protects your employees from themselves. Test a tool, like McAfee® Web Gateway (available as a free trial), which can track all web traffic; automatically provide proactive protection against malware, even if it's hidden in encrypted packets; as well as block undesirable URLs, prevent outbound leakage of sensitive data, and enforce acceptable usage policies.
3. **Be inclusive, rather than exclusive.** There are thousands of commonly used business SaaS products on the market. Don't force your employees to use just the ones you have approved. Instead, build your policy around a security solution that can provide your employees with secure access to a broad range of recognized SaaS options.
4. **Mitigate risks in commonly-used applications.** Rather than shut down usage of popular but risk-prone applications, implement a security solution that allows you to control their use. Look for a solution that offers policy-based control over sub-functionality of commercial software—for example, allowing users to access Facebook but restricting the "chat" function; or automatically encrypting files before they are uploaded to a file-sharing site, like Dropbox.
5. **Make sure your business safeguards data, and complies with privacy regulations.** Data loss prevention, available as an integrated feature in some secure web gateway solutions, can monitor SaaS traffic for sensitive information, such as credit card numbers; and then (based on your preference) encrypt or even block the data, and issue an alert.

6. **Implement identity and access protection.** When employees sign up on their own with multiple SaaS vendors, the inevitable result is password chaos—with passwords attached to sticky notes and filed in (unprotected) lists in the employee's mobile device. The balance between protection and ease of use can be reached with a robust Identity and Access management solution that offers single sign-on for all SaaS applications.
7. **Communicate – communicate – communicate!** Once you have developed a reasonable policy that balances employee freedom with corporate protection, and implemented security solutions that are strong yet non-intrusive, you still need to gain support from your employees and business leaders. Start with the IT department, the guardians of the corporate IT policy, and work your way through all business units and departments. Keep an ongoing dialogue with LoB leaders, inviting them to evaluate new SaaS options for inclusion. Share reports showing the threats you have staved off with your new security policy, and distribute media accounts of security breaches suffered by your competitors or other organizations within your industry. If employees feel that your SaaS policy is reasonable and effective, they will be more likely to take pride in its success.

THE LAST WORD

Trying to limit SaaS usage in your business is like shutting the barn door after the horse has escaped: it won't help, and you will just look foolish for trying. With over 80 percent of employees admitting to using non-approved SaaS in their jobs, there clearly is a need to expand the software tools available to employees. Rather than attempt to restrict usage, your goal should be to enable the freedom your employees need to do their jobs better, without compromising company security and liability. The right security solution can help you find that balance.

In the near future, "shadow IT" will come out of the shadows, as successful companies loosen restrictions that are getting in the way of business agility and innovation. Don't be left behind.

Lynda Stadtmueller

Program Director – Cloud Computing
Stratecast | Frost & Sullivan
lstadtmueller@stratecast.com

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
http://www.frost.com

ABOUT STRATECAST

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion