ENTERPRISE

Are You Losing Control of your Information to Shadow IT?

RICOH
imagine. change.

ENTERPRISE

An Introduction to Shadow IT

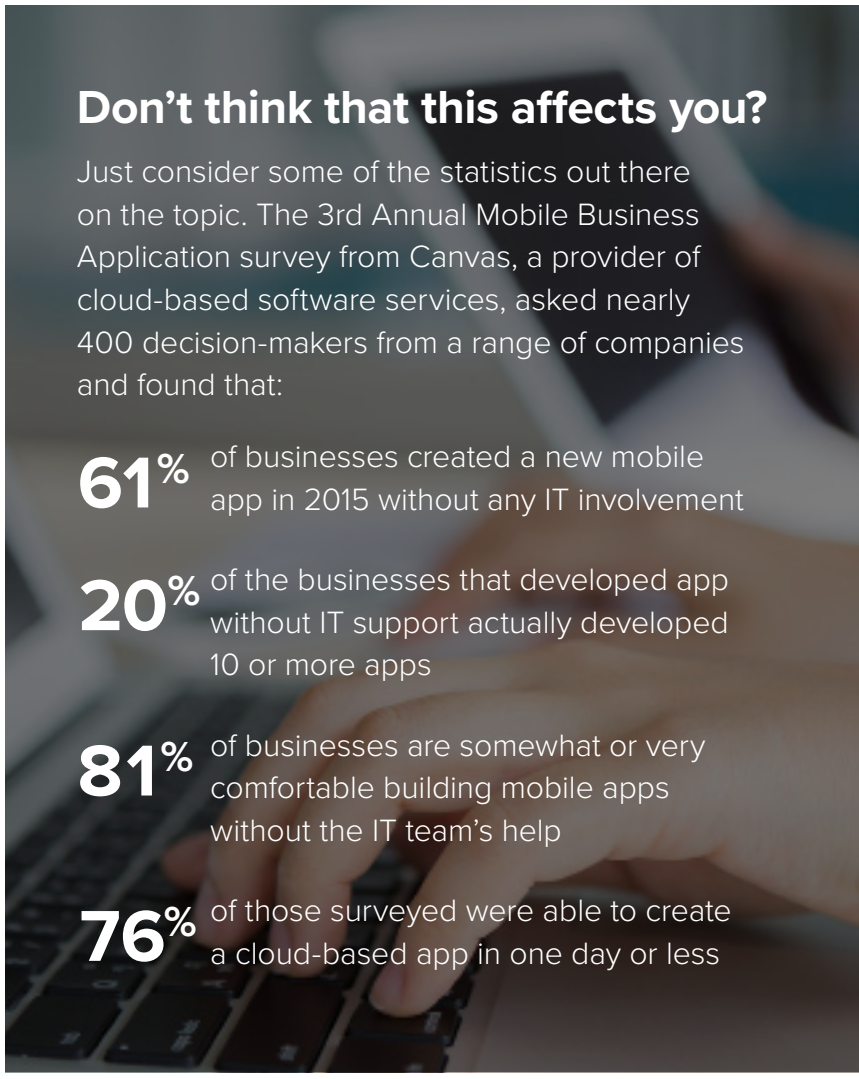
There was once a time when the IT department had a lock on its systems.

The tech team was the sole authority for what applications ran on its computers. Earlier generations of computer systems required specialized skills, so installing a favorite program was not only expensive, it was a clunky and time-consuming process. Sure, there may have been a rogue developer or a tech-savvy worker somewhere in the business ranks, running an unauthorized server with a pet program designed for a specific task. But other than that, the technology department kept a firm command of the enterprise's applications and infrastructure.

The landscape's a lot different these days.

The number of applications deployed and used by individual workers (and sometimes, entire business departments) without IT's authorization—and often, even its awareness—has grown steadily in recent years. Cloud computing has certainly contributed to the proliferation of unauthorized applications throughout the enterprise, as even those workers lacking technology skills or training can turn to the cloud for useful applications. Mobile also plays a significant role in this trend, as employees turn to app stores to find programs that help them do their jobs better.

Either way, workers now often have little (if any) need to bring in IT. Just buy and download. All those unauthorized apps make up an IT operation outside the officially sanctioned technology environment. It's called shadow IT. And it exists at enterprises everywhere.



RICOH imagine. change.

Then, there are the findings from the Brocade Global CIO Survey 2015. The survey found that 83 percent of the 200 CIOs polled saw unauthorized provisioning of cloud services. That figure may be even more surprising, considering that a third of the CIOs surveyed also said their organizations prohibited cloud adoption without IT involvement.

WHAT'S THE PROBLEM?

Workers want access to data at any time using any device they choose. Moreover, they want access to whatever data they need, so they can get their jobs done whenever and wherever they are at the time.

And business leaders want to support that access—as well they should. Studies have found that employees with such access are more productive. Figures from the 2016 Mobile Productivity Report from Wrike Inc. make the point. Wrike, a provider of online project management software, surveyed more than 850 professionals from various enterprise departments, including marketing, IT, finance and HR and found that:

- 43 percent of respondents view mobile device use as very critical for their work
- 44 percent of respondents check or use their mobile device for work more than 20 times per day
- 37 percent of respondents say their mobile devices improve their work-life balance

This anytime-anywhere access to data, a key element of information mobility, comes with challenges. The proliferation of unauthorized apps that enable this information mobility is just one of them.

But why, if it enables information mobility, is shadow IT such a problem?

PROBLEMS WITH SHADOW IT

Many organizations do not have strategies in place to deal with shadow IT. But doing nothing isn't an option here. If unauthorized apps are allowed to proliferate within your company, your risk of data loss or getting hacked increases. Plus, you'll likely find the task of taking back control much more difficult, the longer you allow the situation to go on.

Think about the potential issues. A salesman who uses his own favorite app to store client data can walk out the door with all that information (without you even knowing), but also may put that client data at heightened risk of being stolen, leaving your company to deal with the aftermath. Or the HR department might opt to install its own cloud-based program to handle some employee records, but because department leaders failed to loop in IT, the records never make it to core personnel systems.

HERE'S A BREAKDOWN OF THE PROBLEMS THAT SHADOW IT PRESENTS:

First, shadow IT often puts data at risk by putting information outside enterprise controls. Sensitive data could be more easily hacked. A 2014 study from cloud security company Netskope estimated that the use of cloud services by the business increased the likelihood of a data breach threefold.

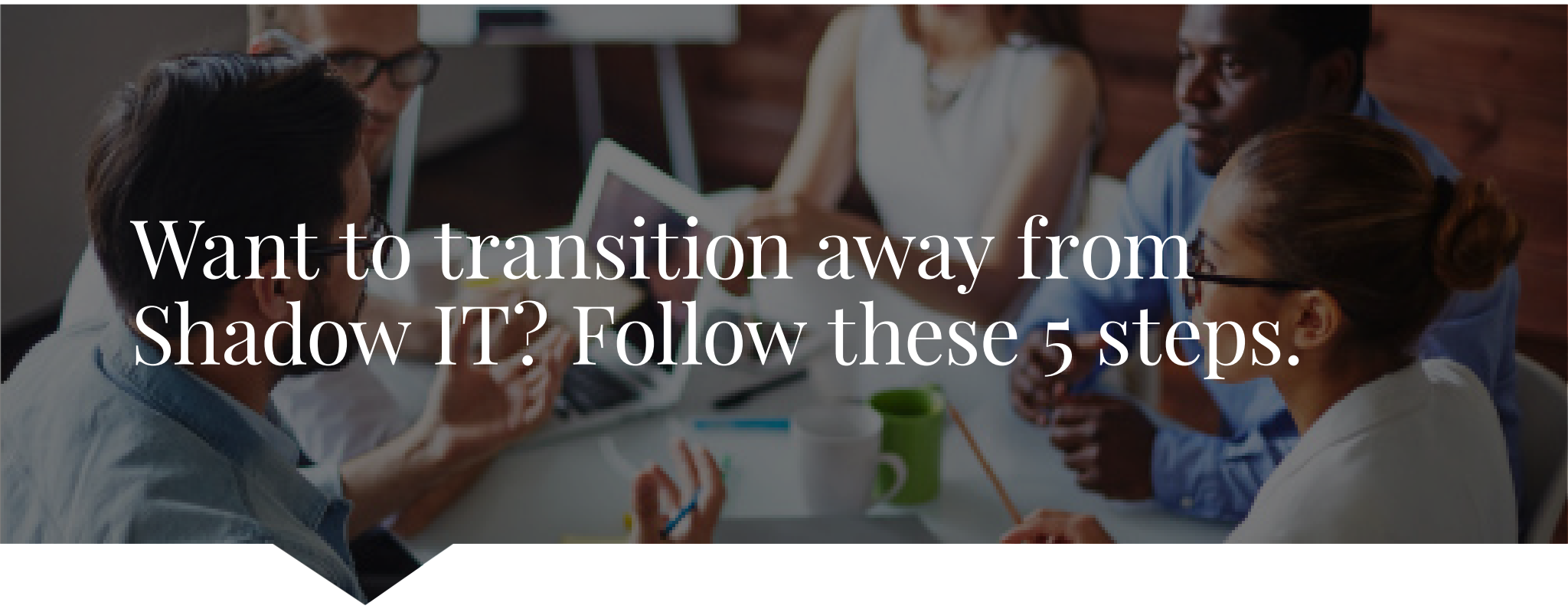
Also, **data collected by these unauthorized apps could fail to make its way back to core enterprise systems**, jeopardizing the company's efforts to gather all its data into a so-called Single Version of the Truth (SVOT), or a centralized data repository essential for an accurate view of corporate information.

Moreover, **shadow IT drains enterprise resources**. Workers who buy unauthorized apps could be generating extra, unnecessary costs by purchasing duplicate or redundant services. They could strain IT support when they seek help for integration and other needs. And they could wreak havoc on IT asset management efforts and software licensing agreements.

In short, shadow IT goes against critical governance, risk and compliance best practices.

RICOH imagine. change.

Executives need to understand that the days of the CIO and IT department exerting strict control over all the technology in the organization are over. That doesn't mean, however, that IT should ignore shadow IT and all the potential problems it creates. Instead, IT needs to find a way to better align its services with the business needs.



Want to transition away from Shadow IT? Follow these 5 steps.

Step 1: DETERMINE WHAT YOU HAVE

If you want to move workers out of the shadows, start by shining a light on the situation. To do that, you must create an inventory of what's out there. In other words, you must assess just how deep shadow IT runs in your organization. Unfortunately, most IT leaders just don't know what's really running in their enterprises.

The nonprofit Cloud Security Alliance surveyed 212 business leaders for its 2015 Cloud Adoption Practices & Priorities Survey Report and found that:

- 72 percent of companies did not know the scope of the shadow IT that existed at their organizations
- For companies with 5,000 or more employees, the number of those in the dark (pun unintended) was 80 percent
- Only 8 percent of companies indicated that they knew the scope of shadow IT within their organizations

Such figures may make the task of creating such an inventory seem impossible, but technology tools can move the dial.

To be clear, there's no silver bullet here that will track and inventory all applications and eliminate shadow IT. But there are technologies that can help find, monitor and manage authorized and unauthorized applications, both in the cloud and on premise. Network traffic analyzers and cloud management tools, for example, can scan traffic to see where data is going and whether it's headed to the cloud.

Step 2:
ALIGN IT WITH BUSINESS NEEDS & EXPECTATIONS

CIOs and business line executives who want to tame shadow IT must keep in mind that this is not a technology problem—at least, not entirely. So you can't rely solely on software to identify and build an inventory of shadow IT. You have to work relationships with managers and workers, explaining what you mean by shadow IT and why it can be so problematic.

More importantly, though, you need to explore why workers and, if applicable, entire departments have bypassed IT when selecting and deploying applications. For example, did IT know about a business need and fail to respond, or fail to respond fast enough? If IT knew about the need and deployed a solution, why did that solution fail to meet the business need? Did it lack the functionality the workers needed? Was it too cumbersome to use?

It's critical to know what's driving shadow IT if you're committed to switching more workers over to enterprise-sanctioned apps.

Once you have insight into the why behind shadow IT, then it's time to align the IT department. IT needs to make sure it's delivering the systems needed by the business partners within the timeframe they expect with the user-friendly functionality they want.

This is where change management skills are crucial. You may be asking your IT staffers to think differently about how they work with their business colleagues to develop or select technologies. IT can no longer take weeks or months to deploy solutions, as such delays are what often prompt workers to turn to unauthorized apps that they can often get almost instantaneously.

IT needs to update its policies and processes to ensure timely innovation and fast-tracked implementation schedules if it wants the business to turn to IT first, rather than outside vendors or app stores.

Step 3:
EMBRACE THE CLOUD

If you're only dabbling with cloud computing, or using it only for select applications, you're missing out on an opportunity to meet your business needs while also combating shadow IT. Why? Because **cloud allows IT to deliver at the speed that business needs in the new world of work**.

Cloud also enables your developers to work in an agile fashion, giving them a secure space where they can quickly develop and test. This not only helps meet the business' we-want-it-soon requirements, but also keeps your development team from seeking out their own unauthorized environments.

In addition, you should think about loosening IT controls in exchange for greater transparency on what the business units are doing. How do you do that? Allow business to experiment with new apps as long as they work within set parameters, such as security standards or time limits, after which they need to loop in IT. Support these innovation efforts by providing help from IT.

Such policies can foster innovation by giving more workers the opportunity to develop ways to do their jobs faster, better or more efficiently.

Yes, this is a departure from standard procedures at many (if not most) IT shops, but this goes to the heart of process transformation and optimization—a critical undertaking if your organization is to remain competitive in this era of digital transformation.

Step 4:
ENABLE YOUR WORKERS

Another way to bring shadow IT out into the light is to convert those enterprising business folks who embrace unauthorized apps into allies. To do that, you have to give them the right tools and support. Sure, they might not be full-time programmers and developers, but that doesn't mean you can't harness their energy, enthusiasm and imagination to bring authorized solutions into the enterprise.

Empower these "citizen developers," as they're called today. These end users can create business applications with IT's knowledge, approval and support when needed with low-code platforms. And you may be amazed at their potential.

The 2015 State of Citizen Development report from Intuit QuickBase found that 62 percent of citizen developers can turn out an app in less than two weeks, with another 27 percent taking two to four weeks. Just 13 percent of citizen developers report needing more than a month.

This is a fast-growing trend that executives should embrace—or risk being left behind. Want proof? Take note of Gartner Inc.'s 2015 Citizen Development is Fundamental to the Digital Workplace report, which predicts that at least 70 percent of large enterprises will have established successful citizen development policies by 2020—a jump from just 20 percent in 2010.

Step 5:
PUT IN GUARDRAILS

The days when IT could keep a tight control on all its software and systems are over. If you're still holding onto that notion, then consider this finding from Gigaom Research and CipherCloud: 81 percent of line-of-business employees admitted to using unauthorized Software-as-a-Service (SaaS) applications, while 38 percent are deliberately using unsanctioned apps because of cumbersome IT approval processes.

More telling, perhaps, is research conducted by the Ponemon Institute in 2014, which found that on average, 44 percent of the corporate data stored in cloud environments is not managed or controlled by IT.

Regardless of the factors driving shadow IT, it's essential that business leaders remember that it puts data at risk. Too often, shadow IT allows data to move in unsecured environments and outside of integrated systems. Data is already at risk. If you do nothing, the chances of significant problems will only continue to grow.

So as you work to bring shadow IT back into the enterprise fold, it's critical to make sure you set policies about what will and won't be tolerated—and then hold workers and managers accountable to those limits.

IT, for instance, can establish what systems and information must stay strictly within the authorized environment, and what may be developed and deployed by the lines of business with IT's blessing.

Lines-of-business managers who are making their own investments in IT should understand compliance and data governance rules, and be held to those standards.

Organizations also should set parameters around the data itself, especially as information mobility becomes a greater priority within the enterprise. Implementing technologies that protect information as it travels and allow only authorized access can help limit exposure to risk.

Ultimately, it's paramount to realize that shadow IT will not go away on its own. And even if you take steps to mitigate its pervasiveness, you'll likely never stamp it out completely. Enterprises must formulate a plan about how to deal with this issue, and take steps to continue to address the problem in the future.

RICOH
imagine. change.

Cheat Sheet

WHAT IS SHADOW IT?

The number of applications deployed and used by individual workers and sometimes entire business departments without IT's authorization—and often, even its awareness—has grown steadily in recent years. These unauthorized apps make up an IT operation outside the officially sanctioned technology environment called "shadow IT."

WHAT'S THE PROBLEM?

Although shadow IT results from workers searching for ways to be more efficient or more productive, shadow IT puts data at risk by putting information outside the control of your organization.

HERE'S HOW TO BRING SHADOW IT INTO THE LIGHT

1. **Determine what you have.** Use technology tools to create an inventory of what's really running in your enterprise.
2. **Align IT and business needs & expectations.** Understand why workers and managers are bypassing IT, and then create an IT organization more responsive to their needs.
3. **Embrace the cloud.** Cloud can bring speed and agility to the IT organization, so the business is less tempted to go outside for quick solutions.
4. **Enable your workers.** Empower end-users as citizen developers by giving them technologies and support to create their own solutions that meet enterprise controls.
5. **Put in guardrails.** Set policies about what will and won't be tolerated—and then hold workers and managers accountable to those limits.

RICOH
imagine. change.