Shining a Light on Shadow IT

stevemordue.com/shining-a-light-on-shadow-it

Steve Mordue MVP

The IT organization, inside of most enterprise customers, is primarily focused on Security, Governance and Compliance these days. One of the biggest tools in their arsenal is the word "No". That approach, to requests from various departments for solutions to help them accomplish their goals, planted the seeds for Shadow IT, and that Genie is not going back in the bottle.

Shadow IT

In every organization, that is of a size to have an actual IT Department, Shadow IT exists. If you work or run one of these departments, and think there is no Shadow IT in your organization… you are wrong. There are tens of thousands of pay-by-credit-card online services available, to solve just about the same number of problems that people in your organization are struggling with. When you said "No" to Sally, and her 5-person department, for some kind of a solution they could use to track their projects, Sally signed up for "Billy-Bobs Project Whiz", a SaaS service, that she put on her credit card and adds to her expense reimbursement request.

Studies A Plenty

Clearly the "Democratization of IT" is bringing it's challenges to IT. There have been many studies over the years about the potential impact of Shadow IT, I pulled a few interesting tidbits from this Forbes one from late last year, where they surveyed 350 Enterprise Execs.

"60% of organizations don't include Shadow IT in their threat assessments." I'll call this the "putting your head in the sand" approach.

Yet "46% say Shadow IT makes it impossible to protect their data." So we are aware… we just choose to ignore it.

When asked who should be responsible for a security issue from unsanctioned apps, 87% said the users themselves! So Sally unknowingly connects "Billy Bob's Project Whiz" to sensitive data, that is then exposed and brings the whole company to a stop… but it's Sally who is responsible? 68% said it was the IT Department's responsibly for software that they are not even aware of, not causing a problem! Another 64% said it was Billy Bob's responsibility!

Less than half of the Execs believed they were even aware of the extent of Shadow IT. My guess is, that the ones who claimed they were aware, don't know the depth of it.

There are more scary facts in that study, as well as the many other studies out there.

Battle Tactics

Up until now, the typical tactics used by IT to curtail Shadow IT have been lockdown measures, including elaborate data access policies, Zero-Trust policies, encryption, etc. Basically removing access to the most valuable resources from the people who need access. How are Line-of-business owners supposed to advance their organizational goals, without access to the very data they need to accomplish that? Obviously you can't just open up your data stores to every "Billy Bob" SaaS service... but your users need it.

Embrace It?

If it's going to happen anyway, is it better to just embrace it, and attempt to govern this Shadow activity? This would require a significant change in IT's thinking. "Hey Sally, I know I said 'no' to your request last year, but I assume you have solved your issue another way, can I take a peek at that please?" Certainly you could review "Billy Bob's" app, and maybe realize that Sally, not being a knowledgeable person, could have checked a box to encrypt all data, or similar things. Maybe you could even get satisfied that "Billy Bob's" App does not present a threat. What's next? Find every app like that in use your organization? How could you even do that? And checking them all would become a year-long project. For the ones that don't pass your review, how would you stop them from using it anyway... I mean they already went around you. Asking "Nicely"? That's not a trait of IT.

What are these Apps?

Most of the Shadow IT Apps in your organization will be some kind of point solutions to solve specific business challenges for your users. Many of these "Apps" will be brought in by the department to replace spreadsheet based systems that are just not cutting it for them anymore. Maybe you could track your users' Excel usage... if it suddenly goes down, you may have a new Shadow App in your org. Here's the problem, if you keep saying "No" to requests for help, they are going to solve their problem another way. But if you start saying "Yes", you now have a full-time job of vetting and monitoring all these "Billy Bob" apps.

Microsoft's Power Platform

Ok, I am aware that as a Microsoft Partner, I have my bias, but that does not mean that they haven't created a path for you to solve this problem. The Power Platform, which includes Power Apps, Power Automate, Power BI and Power Virtual Agents, was purposely designed

to be used by your line-of-business users to build applications, using no/low code, to solve many of the problems they are going outside for. But are you just trading one problem for another? Again, saying "No" means Power Platform is just one more place your users can go with a credit card and sign up for on their own. Or you could bring it into your organization yourself and give them access to it. Why? Well now it is running in your environments that you control, and access to all of it is via Active Directory. The ultimate in security is their login page to your Microsoft account. So does the Power Platform solve your Shadow IT problem? Hell no.

Internal Shadows

Microsoft made a recent decision to turn on the ability for your users to create their own apps "by default". I guess they thought you would get in the way. Yes, if you have Office 365, your users can start building apps, and many may have already. Sure, you have a master kill switch, but that would just drive them back outside. Based on Microsoft information, users are building thousands of apps right now on the Power Platform… because they can. Using connectors, these users can be sending your data outside of your organization right now. So the Power Platform alone does not solve your problem, it could even be making it worse! How can you figure out the extent? I guess you could hit the kill switch and see how many screams you hear. Is there a better way?

Center of Excellence (CoE)

Fully cognizant of the potential of the Power Platform to transform an organization, but at the same time drive IT nuts, Microsoft developed an alternative to the kill switch they desparately hope you won't push. Since pushing it will drive your users back into the shadows, maybe a CoE is worth a look. Microsoft developed a CoE "starter kit". From the document:

"The Center of Excellence (CoE) starter kit is a collection of components and tools that are designed to help get started with developing a strategy for adopting and supporting the Power Platform, with a focus on Power Apps and Power Automate."

So this toolkit can help solve some of the biggest challenges, visibility for one. Basically you would create your own Power App, install their components on it, connect to their APIs and voilà, you now have visibility of all of the apps in your organization, as well as who is building them. A light on the shadows.

What's in the box?

Okay, there is no box actually, but some of the things that are part of the CoE toolkit are: Environment and Environment Security management, Data Loss Prevention (DLP) policy management, as well as Data integration and Gateway management. Compare that to the control you have over Shadow IT today. Is the toolkit a magic bullet to cure all ills? No, it is a part of a more comprehensive plan. Again from the document:

"The kit does not represent the entire Center of Excellence, because managing a CoE requires more than the tools alone; the Center of Excellence also requires people, communication, defined requirements and processes. The tools provided here are just a means to get to the end goal, but the Center of Excellence itself must be thoughtfully designed by each organization based on their needs and preferences."

So there is more to do.

Why bother?

Bringing Shadow IT into the light alone is a huge benefit for IT, but actually embracing the Power Platform and fostering and nurturing it's "governed and controlled" use, has had significant proven benefits for Enterprise organizations. Here I will provide a few highlights and links to case studies.

- A small team at G&J Pepsi with no previous app-development experience created auditing apps that saved the company $500,000. Link
- The Miami HEAT used data insights to grow fan engagement and increase season-ticket sales by 30 percent. Link
- Virgin Atlantic creates custom-built mobile apps to continually improve the start-to-finish travel experiences of 5 million passengers a year. Link
- One Autoglass employee created 40 apps that boosted the productivity of 3,000 field technicians and brought $40,000 savings. Link
- France's national railway improved maintenance procedures and incident reporting by enabling employees to create more than 150 apps. Link

There are a ton of other stories about how IT, partnered with their users, has become the hero in their organizations.

What's Next?

Well, the first thing you should know, is that the CoE tools that are "provided" by Microsoft, are not "supported" by Microsoft. They have enough on their plate. So it is pretty much a DIY project. My company Forceworks, is offering a free CoE Briefing to learn more, you can sign up for that at forceworks.com/coe.

Steve Mordue MVP © 2020. All Rights Reserved.