REDUCING THE DANGER OF SHADOW IT WITH DEVOPS

Businesses are built on processes, and the good ones help you win. Others, like shadow IT, can hurt you if they aren't tamed. Implementing DevOps best practices to improve your "true" IT organization, and other business units, can help you do that.

If you're unfamiliar with the term, "shadow IT" describes circumstances where businesspeople contract an outside company to implement needed business applications or services normally handled by your IT department. Businesspeople usually do this because they have an immediate need, but IT has told them their project can't be started for several months.

One of the key concerns is that the outside company may ignore company security and coding standards. Usually, these outside companies turn something over to your internal IT department that may not meet the normal or expected standards for code, documentation, or robustness for production environments.

The Dangers of Shadow IT

Many have claimed shadow IT projects can be catalysts for innovation, and maybe that's true in specific cases. There's an exciting aspect to the mutinous process of going rogue, successfully getting around bottlenecks with a secret cloud solution and getting things done you otherwise wouldn't have. But there's more danger tied to shadow IT than good.

Shadow IT ignores transparency and damages trust. The secrecy of the process means no one or only a few are aware of what you're doing. If it's something good, you're hurting your organization by keeping your ideas or innovation in a vacuum. On the other hand, it could be something you don't realize conflicts with another initiative or simply doesn't align with your organization's goals. When a

lack of transparency is realized, it creates distrust between IT and the individual(s) trying to work around it.

Shadow IT creates risk for your business and customers. It's a quick and easy route to sensitive corporate or customer data living outside your organization's secure environments in a public cloud. It might be as simple as collaborating on new product requirements in a Google Doc versus your organization's official collaboration space. It could be a customer data in a public Dropbox folder. Data available outside normal IT controls creates potential risk to the business.

What's interesting is most employees don't realize they're exposing sensitive data when they choose to use an unapproved tool for sharing. Oftentimes, organizations may not be communicating policies and the importance of following certain procedures well enough.

Shadow IT projects are difficult to audit. If someone does something negligent with a shadow IT project that hurts your business or customers, you may not have any recourse to discover what happened without logs in place. It takes time and money to identify an audit trail to uncover what happened or who was involved. And, of course, avoiding security measures that prevent these issues but sometimes slow down projects is often exactly why people resort to shadow IT.

Shadow IT is a workaround that creates more drag. People will use shadow IT to work around bottlenecks. But while shadow IT may make things go faster, because that speed is occurring outside normal IT processes, it can actually slow things down. For example, if IT can't integrate the workaround into their existing infrastructure, it will take extra time to make a solution work when IT absorbs it.

How DevOps Can Help

The reality is, you can either declare your organization will never do shadow IT and lose the battle, or you can recognize its proliferation and start putting some governance around it. Here's how DevOps can help.

Communication and Collaboration

DevOps is all about fostering better communication and collaboration between teams and across platforms; it's all about including people from different areas of the business, even outside IT, from the beginning development stages of new software to the end. If you're going to "okay" certain projects under shadow IT, there should be communication and transparency about what's occurring.

To do this, keep sanctioned shadow IT projects within the bounds of IT processes already in place. If you use Agile methodologies, such as two-week sprints, make sure shadow IT projects follow them and, for instance, include a security person and someone knowledgeable with coding standards in sprint reviews. This addition will help keep projects safe and in line.

Quality, Velocity and Efficiency

DevOps is also all about developing and delivering high-quality innovation as efficiently and quickly as possible. If your organization is already doing this, it will reduce the number of shadow IT projects because people won't have to feel pressured to work around bottlenecks as often—you'll be reducing them with DevOps instead!

And by prioritizing the most important requirements to be delivered iteratively along a road map,

people will develop trust that what they need will come at the right time. If your internal IT department can implement key requirements for the business from their prioritized list, even if the complete list can't be achieved, it may relieve enough pressure on business units to forego starting shadow IT projects.

Good Tools

Another important aspect of DevOps is enabling people with the tools they need. If people are sharing data on Google Docs, why isn't your organization providing them with an excellent collaboration tool like Atlassian Confluence?

With DevOps, you prevent shadow IT groups from scouting and using unapproved open-source tools that may not integrate well with your environment or that aren't properly secured or licensed. Instead, you provide good tools that help people be productive and successful.

Fighting shadow IT is a battle no organization will ever completely win, but letting it run amok is financially dangerous and unsecure. The best tactic for organizations is to control their shadow IT activity by improving their own development, operations and security organizations through DevOps best practices and being willing to address small but high-priority business initiatives quickly.