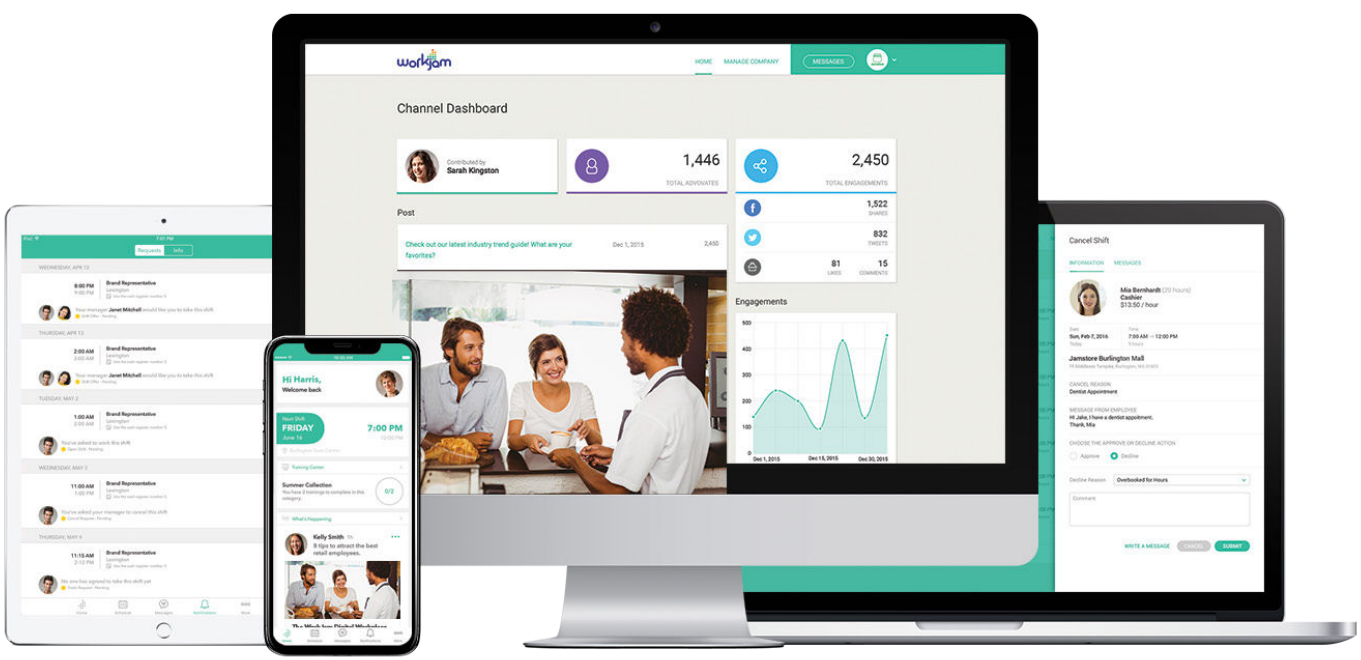
Is Shadow IT Putting Your Company at Risk?

workjam | AXSIUM



Our connected world makes it easier than ever for people to communicate. Mobile and cloud-based applications such as texting, online chat, personal email, and file sharing programs have also blurred the lines between work and home, making it easier for employees to talk to each other, share information, and get work done outside of the four walls of the business.

At first glance, this seems harmless, maybe even desirable.
As it turns out, it's created a serious problem for retailers and other organizations that employ hourly staff.
And that problem has a name: **Shadow IT.**

workjam | AXSIUM

What Is Shadow IT?

Shadow IT is a term used to describe any technology that is utilized to share business data or perform business processes that is used without the consent or oversight of the organization's IT or IS department.

Here are some examples of Shadow IT at play:

- Matt is at work, and the new schedule has just been put up. He snaps a photo of the schedule and posts it to his ***Facebook*** feed, tagging his coworkers and saying, "Hey guys, new schedule's up."
- Heather is taking some new training and is confused about a section. She sends a ***WhatsApp*** message to Jamie, her best work friend who is currently at home watching ***Netflix***. Heather tells Jamie about the training and asks her some questions about it. Jamie takes 20 minutes out of her evening to reply to Heather, helping her out as best as she can.
- Tyson wants to have Friday off because his mom will be in town visiting. He pops into a text message chain he and his coworkers have set up, without consent of their company, and asks if anybody can take his Friday shift. Sandra readily volunteers, and the two agree to swap shifts.

Some common forms of Shadow IT include:

- Social media applications like ***Facebook***, ***Twitter***, and ***Instagram***
- Online chat applications or programs like SMS, ***WhatsApp***, and Slack
- Smart applications that allow employees to download the freemium model, which is unsanctioned by corporate, for point solution tasks such as shift swapping
- Cloud-based document management like ***Dropbox*** or ***Google Docs***
- Cloud-based email programs like ***Gmail***
- Hardware items like USB drives.

workjam | AXSIUM

The Dangers of Shadow IT

All of the above scenarios seem fairly innocuous. After all, the employees are simply sharing information, chatting with each other, and managing their schedules. Surely that can't be a problem?

It can. And it is. Here are five reasons why:

SHADOW IT CAUSES COMPLIANCE & LEGAL RISK

A major component when it comes to compliance is control, explains Bob Clements, President of ***Axsium Group***, a global workforce management consultancy. *"If a company does not have 100% control over its processes and its information, it runs the risk of non-compliance with regulatory legislation such as the Sarbanes-Oxley Act[1]," says Clements.*

Here's an example: The Sarbanes-Oxley Act prohibits the willful destruction of evidence. Now, only if every bit of a company's information and records are held under their firm and clearly defined control, will they remain compliant.

But work-related conversations taking place on a non-sanctioned platform like ***WhatsApp*** can lead to non-compliance and result in possible penalties of up to 20 years in prison.

Other compliance issues pose a risk as well, says Robin Merritt, Senior Vice President of ***Axsium Group***. The Fair Labor Standards Act currently requires that non-exempt employees must receive overtime pay for hours worked over 40 hours per workweek (any fixed and regularly recurring period of 168 hours—seven consecutive 24-hour periods) at a rate not less than one and one-half times the regular rate of pay[2].

"If employees (or managers) are adjusting schedules outside of the checks and balances your WFM system puts in place, companies run a real risk of employees working overtime without the company being aware—which puts them into a position of noncompliance with the FLSA," says Robin.
The potential penalties? Due to a precedent set in ***Walton vs. United Consumers Club[3]***, Inc. , employees may be able to recover not only back pay but "liquidated damages" (an amount equal to the pay employees should have received). In large organizations with a massive workforce, losing control over shift scheduling can easily put the company at

One of the biggest risks of Shadow IT is the blurring of work and home life, potentially leading to "off the clock" work. In our example of Heather and Jamie (who answered some work questions for Heather while sitting at home), a lawyer could easily make the case that Jamie was working and should have been paid for that work. Enough Jamie situations and you have a class-action lawsuit—worth potentially millions of dollars—waiting to happen.

risk for tens or even hundreds of thousands of dollars in penalties.

SHADOW IT PUTS YOUR DATA IN PLACES IT DOESN'T BELONG

Any company with an educated Information Security team knows that when it comes to attempted data breaches, it's not a matter of if, but when one will happen to them. To reduce their risk, these teams put stringent data controls and cybersecurity measures in place.

All of this hard work is undercut when employees share data (or worse, things like login credentials) via externally managed communications channels. IT and IS departments can't protect technologies that they don't even know are being used. If cyber attackers can gain an "in" from an employee's carelessly managed ***WhatsApp*** or ***Gmail*** account, they can quickly leverage that access into a headline-making[4] data breach.

Furthermore, there is the issue of data wiping to consider. Data that lives solely in the company's own servers is accessible and if needed, can be erased off of an employee's device when they leave the organization. On the other hand, if data winds up being shared through third-party apps, it lives in that application's servers forever, permanently out of reach of the organization.

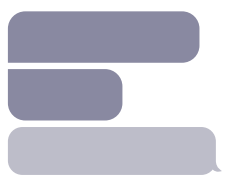
In the age of GDPR and other data privacy laws, an inability to remove this data after an employee's departure can set a company up for a considerable amount of liability.

SHADOW IT MAKES IT HARD TO GENERATE MEANINGFUL LABOR ANALYTICS

With the cost of labor increasing each year, every organization can benefit from improving its processes and increasing its efficiency. To do this effectively, organizations need to have a 360-degree view of all scheduling practices.

However, if communications, scheduling, shift trades, and other work-related tasks are taking place outside of the organization's view and control, it can be impossible to understand what's really happening at the store-level.

This makes after-the-fact analysis difficult. Why was staff turnover so high at a given location? Was it because the weekly schedules were always changing? Was the store manager making it too difficult for associates to shift swap? Did employee schedules vary



significantly week to week? If employees are managing all these things via text message or ***WhatsApp***, it can be difficult to say. And that puts organizations in a position where it's impossible to make informed decisions about labor–like a doctor trying to diagnose a patient without knowledge of their symptoms: an accurate diagnosis is impossible and making assumptions is possibly harmful.

Corporate communications teams work diligently on their messaging. Conveying the corporate vision, goals, and plans effectively and persuasively can mean the difference between an aligned and engaged team of front-line workers and an unmotivated, unfocused group - each of whom heard something different from their manager or their coworkers about the company's goals. Instead of having a focused and coherent message, Shadow IT makes it all too easy for misinformation to spread unchecked.

SHADOW IT CAN EVEN PUT YOUR EMPLOYEES IN DANGER

Remember Matt (who posted the new schedule on ***Facebook*** and tagged his coworkers)? He thought he was being helpful. Unfortunately, he didn't realize that Sarah, his coworker, is being stalked by her abusive ex-boyfriend. And although she blocked her ex from her own social media, she hadn't thought (and would have been embarrassed) to ask her coworkers to block him as well. Now, this ex knows exactly when Sarah works, which puts Sarah in extreme danger and makes Sarah feel unsafe at work.

This may seem like an extreme example, but stalking and domestic abuse are alarmingly common[5]. And if company information is shared on social media or other publicly accessible communications channels, it can put some employees in very real danger.

workjam | AXSIUM

Why Is Shadow IT So Pervasive?

Shadow IT carries substantial risks, but is it something that the average organization really has to worry about?

In a word, yes. And even those companies who do worry about it tend to grossly underestimate the scope of the problem. In 2015, Cisco performed a survey of CIOs[6], revealing that the average CIO estimated their organizations had company data stored on 51 cloud services.

The real number? 730. Even more alarmingly, ***Cisco*** estimated that number to climb to 1000 by the end of that same calendar year.

In the four years that have passed, it is safe to say that this number has not decreased. But why has this become such a problem?

CHANGING TECHNOLOGY

Twenty years ago, the lion's share of technology a person could access at work was technology that had been procured, tested, secured, and installed by the company's IT department. Smartphones were still a nascent technology, and the average hourly worker did not have access to a computer unless it was to perform specific business functions. It was easy for the IT team to block these computers from accessing external websites such as ***Hotmail*** or ***Yahoo Mail***. Social media sites weren't yet a part of our lives.

Since then, cloud infrastructure has resulted in an explosion of applications and software, while mobile technology has put a powerful computer in everybody's back pocket – one that is entirely outside the control of the IT department. Today, a frontline associate at a cash register can download and install a program on their phone in less than a minute with absolutely no oversight from anybody in the company, and in another minute, can start using that program to share company information. This wild west environment makes it impossible for IS/IT teams to keep the company's technology self-contained and impenetrable, vastly increasing its attack surface.

CONVENIENCE

The ease with which Shadow IT can rear its head makes it a formidable competitor for any company's internal, pre-approved systems.

Because corporate IT infrastructure does go through stringent processes, it moves at a slower pace. If this pace is outstripped by the needs of the business and the needs of the employees, it will be

left by the wayside as workers seek out their own solutions to their business problems. After all, if your workplace's communication platform is clunky, slow, and works poorly on mobile devices, it's understandable why employees would want to sidestep it and use Slack or ***WhatsApp*** instead.

Add in the fact that most employees have no idea what Shadow IT is or why it's a risk to the organization. Even if they do, they haven't been given a compelling reason enough to care. So, it's no surprise that employees don't think twice about using it.

CHANGING DEMOGRAPHICS

In 2009, ***Apple*** trademarked a new slogan: "There's an App for that." This trademark proved not only to be eerily prophetic, but it perfectly captured the technological gestalt of the Millennial generation.

While previous generations had grown up learning to make do with the options and information they had, Millennials grew up with a solid understanding that if they didn't know something, they could look it up online, and if they needed a tool to make their lives easier—well—there was an app for that.

Generation Z is no different, having played with their parents' smartphones since childhood. Now in their late teens, they're entering the workforce in droves, almost exclusively in hourly positions in retail or hospitality.As a result, the majority of today's frontline workers are simply unaccustomed to putting up with unsatisfactory technology and incredibly adept at seeking out other technological tools to meet their needs.

workjam | AXSIUM

How to Prevent and Address Shadow IT

The reality for today's employers is that there is simply no way to forcibly prevent Shadow IT in your organization. You can't confiscate every employee's cell phone at the door. And while you can write policies that are clear and strongly worded, there will always be some non-compliance.

The only viable path to stamping out Shadow IT is to remove any incentive for employees to want to use WhatsApp, Facebook Messenger, or whatever else they're currently using. The question is: how do you do this?

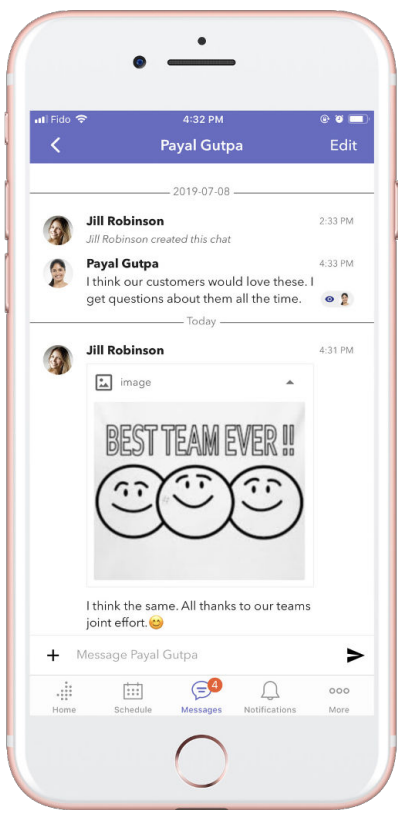
UNDERSTANDING YOUR END-USERS

According to the experts at ***Axsium***, the first key to addressing Shadow IT is *listening*.

"You need to talk to employees and find out which technologies and applications they're using. What do they like about those apps? What problems do those apps solve that your own technology wasn't solving? You can't simply go in and implement a solution to replace Shadow IT when you don't even know why employees are using the Shadow IT in the first place," says Bob Clements.

"End-user experience is key," adds Robin Merritt. *"It's one of the largest success factors when it comes to getting adoption and pulling off an IT project successfully. We tell our clients not to do a project without having significant input and representation from the end-users. Once you understand what that end user experience looks like and what users want, it makes objectives crystal-clear."*

At that point, employers can then use this information to implement a solution that offers an attractive and viable alternative to these external applications and programs.



Learn more about how to make these recommendations actionable at ***WorkJam.com****.* ***WorkJam*** *is a collaboration platform that can scale with your employees' needs. Organizations can get set up with the built-in functionality they need in less than 30 days, while being able to add more modules as they're needed, providing continuous coverage of employees' tech demands and reducing the odds of them looking outside of your organization for their IT solutions.*

IMPLEMENTING A SOLUTION THAT MAKES SHADOW IT OBSOLETE

"When implementing a solution to replace Shadow IT," says Bob Clements, *"organizations need to be forward-thinking to prevent the issue from cropping back up anytime a convenient or exciting new app launches."*

"Your employees may say that they're using applications for swapping shifts. And if you implement a solution that addresses that need, you're solving their problem. But you're only solving the problem they have today. You have to look at what their needs may be in the future. Otherwise, you'll always be putting out fires instead of being proactive and setting the right culture when it comes to technology use.

A platform like WorkJam is ideal for this: Because it's modular and can easily scale, you can use it for shift-swapping today, and then for shift-swapping, communications, and training six months from now, reducing the need for employees to ever look elsewhere. Essentially, you want to look at a platform, not just a point solution."

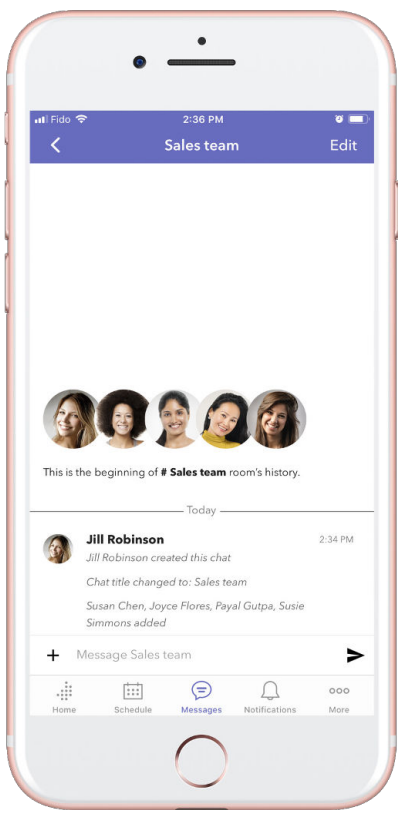
"There are many standalone tools that you can buy that will temporarily dam up your Shadow IT problem," adds Robin Merritt. *"But if you can find a solution that meets multiple employee needs, your employees will stay satisfied longer, and most importantly, the mindset and culture will change—employees will know they can rely on their employer to meet their tech needs and will be more likely to communicate openly with the organization to ensure those needs continue to be met."*

MAXIMIZING ADOPTION AND SUCCESS

After listening to what employees need and implementing a solution to meet those needs, the work is done, right?

Not quite. Combating Shadow IT is not a one-and-done. It's a process that needs to be consistently applied if it's to be effective.

To begin, it's vital to make sure team members clearly understand that using third-party applications and programs for work-related



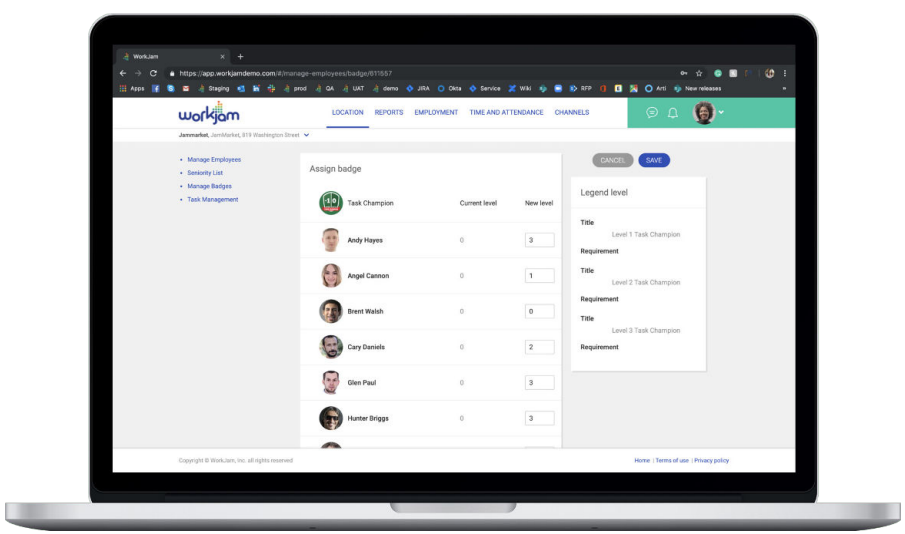
functions is not acceptable. Cover your legal bases by developing a clear policy, communicating it well, and ensuring all employees have signed off on it. Make sure employees know the rationale behind the Shadow IT policy—if they're being asked to change their habits for the sake of the organization, they're more likely to comply if provided with a clear and sensible reason.

From there, put in place a program that not only measures the adoption of the new tool but also identifies holes in that adoption. For example, if the entire company is averaging an 85% adoption rate of the new platform, but one particular district is averaging 20%, that indicates something is going on at a district management level that is undermining your organization's efforts to eradicate Shadow IT, and it needs to be examined. The awareness, education, and monitoring need to be constant, particularly given high turnover rates for industries such as retail. As new frontline associates and managers start, they may bring with them a dependence on a certain application or program and a lower level of awareness regarding the dangers of Shadow IT. Stay on top of the issue by regularly educating associates, and by keeping the lines of communication open to ensure your solutions can continue to meet your associates' evolving needs.

When it comes to Shadow IT, ignorance may be bliss, but it can also lead to a wide range of disastrous consequences crashing down when least expected. However, by being proactive and vigilant, companies can gain clear insight into the scope of their Shadow IT issue, understand why it's happening, and steer their employees happily toward more appropriate technological options.

To learn more about digital workplaces, read WorkJam's white paper:

"What is a Digital Workplace... And Why Do You Need One?"



workjam | AXSIUM

WorkJam is the workforce management solution of choice for industry-leading organizations who are interested in fighting Shadow IT, making their business more efficient, improving employee engagement, and maximizing their profits. To learn more, ***contact us*** today.

Axsium Group is the world's leading workforce management consultancy, helping employers around the world improve their operational performance, increase the productivity of their people, and maximize the ROI of their labor budgets. To learn more, ***contact us*** today.

*For more information on **WorkJam** and how we can help you unleash the potential of your workforce, contact us today.*

Request a Demo

*For more information on **Axsium Group** and how we can help you build a holistic Workforce Management Strategy, contact us today.*

Contact Us

workjam | AXSIUM

SOURCES

1. https://en.wikipedia.org/wiki/Sarbanes-Oxley_Act
2. https://www.dol.gov/whd/overtime_pay.htm
3. https://www.leagle.com/decision/19861089786f2d30311041.xml
4. https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1#adidas-15
5. https://mainweb-v.musc.edu/vawprevention/research/stalking.shtml
6. https://blogs.cisco.com/cloud/shadow-it-and-the-cio-dilemma