SHADOW IT EXPLAINED: RISKS & OPPORTUNITIES

Cloud computing has made it easier for IT users to bypass IT procurement protocols in order to access the solutions they need to fulfil their job requirements. From a user perspective, IT oversight and stringent governance policies are often designed to protect the organization—not necessarily to address the challenges of IT users at the workplace.

The result is **shadow IT**: the practice of bypassing these limitations and accessing the required IT solutions without knowledge of the appropriate IT department.

This article introduces shadow IT and how it affects IT management and procurement. We will look at:

What is shadow IT?

Shadow IT is the use and management of any IT technologies, solutions, services, projects, and infrastructure without formal approval and support of internal IT departments.

Users might adopt shadow IT technologies that do not align with your organizational requirements and policies pertaining to:

- Compliance
- Security
- Cost
- Documentation
- Service Level Agreements (SLAs)
- Reliability
- Other key factors

As such, users of shadow IT bypass the approval and provisioning process and utilize the unauthorized technology without knowledge of their IT department.

Shadow IT systems can include:

- SaaS, PaaS, IaaS, and other cloud services
- Prepackaged off-the-shelf software
- Hardware such as computers, smartphones, tablets and other devices

The most prevalent form of shadow IT systems are SaaS offerings, since these include unique products and solutions to address specific requirements of IT users that may not be identified, considered, or addressed by the vast array of common IT solutions already supported by the organization. The convenient purchase process allows IT users to subscribe, use, and decommission the shadow IT SaaS solution before the organization identifies the purchase or detects anomalous network activity.

The second most common source of shadow IT products is commercial desktop products, along with phone and tablet apps. Remote PCs and laptops are frequently configured as desktop administrators or they may be using their own devices not controlled by IT. Cellphones and tablets are usually locked down for email, but they are frequently left open for app installation. It is common to find unauthorized free and commercial products loaded on user devices. Many prohibited and dangerous apps sneak on to user devices this way.

Why do users turn to shadow IT?

Shadow IT is inevitable. IT users adopts shadow IT practices only to fulfill their job requirements in ways that make their life easier. Gartner research finds that an average of 30-40% of the purchases in the enterprise involve shadow IT spending. A research study by Everest Group found puts these figures closer to 50%.

Part of the problem lies with the organizations:

- Not offering adequate support for technologies that IT users require.
- Making the governance, approval, and provisioning process too slow and ineffective.

Especially for Agile or DevOps-driven organizations focused on continuous innovation and rapid software development and release cycles, the need for new tooling can arise with little warning for IT departments to identify, vet, and approve the products at the Agile/DevOps pace.

Inadequate communication and collaboration between developers and IT teams further bottleneck

the speed and flexibility of IT support required to approve the necessary technologies. At the same time, inadequate security capabilities tend to prevent organizations from approving new technologies even when they want to support devs with the latest and greatest solutions available in the industry.

Shadow IT risks

Shadow IT introduces **shadow risk** (unknown unknowns). While employees are able to conveniently complete the job tasks using shadow IT systems, the technology introduces unprecedented risks, inefficiencies, and cost to the organization, such as:

- **Lost control and visibility.** Migrating data to shadow IT means you've lost control and visibility. The risks include security and regulatory noncompliance, data leaks, and inability to perform disaster recovery measures involving data in shadow IT systems when required.
- **Lost data.** Organizations can lose access to shadow cloud-based data, particularly when the user who owns the information leaves the company. A simple example is a personal Dropbox account where the user keeps customer contracts, drawings, and other project documentation. If that user is terminated, the company may have problems getting critical customer information back from the user's personal account. Shadow IT cloud services can also be quickly disconnected when a terminated user stops paying the bill.
- **System inefficiencies.** Storing and using data in multiple infrastructure locations is inefficient. If

the organization is not informed of the data flows, IT departments cannot plan for capacity, system architecture, security, and performance across data in disparate and siloed shadow IT apps. Analysis and reporting become skewed and more complicated when multiple data versions exist in different unmapped locations.

- **Cost.** Once a shadow IT system becomes a critical part of the project and IT users need to scale the resources, the cost incurred by the organization to continue using the service may be unjustified. This is a common concern with SaaS applications such as cloud storage.
- **Non-compliance.** For organizations subject to stringent compliance regulations, the risk of shadow IT can have far-reaching consequences. Shadow IT creates additional audit points, where proof of compliance must be expanded. For instance, if IT users at a healthcare institution store sensitive patient data in Shadow IT cloud storage solutions, they may be required to audit, identify, and disclose the scope and impact of each incident. In addition to exposing privacy-sensitive information to cyber-attacks, the organization may also face costly lawsuits or fines for noncompliance that may damage its brand reputation and business.
- **Unknown expansion of attack surfaces.** Organizational attack surfaces increase with shadow IT. Unmanaged data repositories lie outside established security boundaries. Weak or default credentials risk exposing unmanaged assets to the Internet. None of the organization's penetration testing, intrusion detection, security information and event management (SIEM) systems, or threat log management will cover shadow IT.

How to respond to shadow IT

To respond to shadow IT, you must implement two strategies:

1. Take strategic measures to reduce the need and the risk associated with shadow IT solutions.
2. Establish policies and implement strategies that anticipate—and manage—shadow IT.

Let's look at each.

Reducing shadow IT need and risk

Here are a few things you can do to reduce the need (and the risks) involved with shadow IT.

- **Communicate and collaborate.** Discover the needs of IT users. Break the silos. Enable easy, convenient, and effective communication between IT departments and IT users, in order to understand the true needs, experience, and feedback of end-users on existing and new required technologies.
- **Educate and train.** Inform users regarding the risks associated with shadow IT and how the organization can assist in fulfilling the technology requirements without having to bypass the standard governance protocols. Security-aware employees that share the organization's vision toward IT security are more likely to understand the risks associated with shadow IT and will be encouraged to find appropriate solutions to address their technology needs.
- **Streamline governance.** Develop an IT governance structure that facilitates innovation through the use of new technologies identified, vetted, available, and provisioned for IT users at a rapid pace. Develop user-centric policies and anticipate their requirements. Balance policy enforcement with the flexibility to evolve and respond to changing IT needs of end-users.
- **Use technology to discover shadow IT.** Deploy technology solutions to monitor anomalous network activities, unexpected purchases, data and workload migrations, IT usage patterns,

and other indicators of shadow IT practices. Proactive discovery can allow organizations to mitigate the risks of shadow IT faster:
    - Reviewing on-premises web filtering logs and configuration management databases can help you discover some shadow IT instances.
    - Partnering with Accounting to flag suspicious IT-related purchases may also help you find shadow IT.
- **Assess and mitigate the risks.** Not all shadow IT technologies pose the same threat. Continuous assessment of technologies in use at the workplace can allow organizations to strategize risk mitigation activities based on the risk-sensitivity of every shadow IT offense.

Establishing policies around shadow IT

Shadow IT is a corporate matter that does not merely concern a technical perspective. The CIO needs to discover, list, and classify the organizational shadow IT resources into three categories:

1. Sanctioned
2. Authorized (not sanctioned yet irrelevant)
3. Prohibited (not sanctioned and dangerous)

Compiling this list should be part of your organization's monthly security review. Once compiled, you can make decisions for dealing with each piece of unsanctioned and prohibited shadow IT. A suggested framework for tackling shadow IT is for the CIO to meet with (not confront) the people who acquired shadow IT capabilities and go through a discovery process to determine what to do about these products, covering the following questions.

1. What is the history of this piece of shadow IT?
2. What business need or value does it satisfy?
3. What does this software/service provide that our internal offerings do not provide?
4. Is there any current service IT can provide that would satisfy these needs?
5. What shadow risk does the software/service incur?
6. What costs, budget, or resources does it require?

As much as possible, the discovery should be non-confrontational. The goal is to understand why the shadow IT is there and how it will relate to or be supported by organizational IT going forward.

After discovery, the CIO and the shadow IT user should make recommendations and come to an agreement about how the organization supports the unauthorized or prohibited software/service. Some possibilities could be:

- **Move the shadow IT component to the Authorized list.** It does no harm to the organization. The user can continue using it without change.
- **Replace the shadow IT with an existing IT function.** There may be in-house capabilities that can perform the same function. If none exist, the organization may be able to iteratively create software to gain similar benefits.
- **Discontinue using the shadow IT service.** It is too risky and too costly. You will phase out the software/service and lose its benefits.
- **IT will support this shadow IT function.** The component will continue being used but its support and costs will shift to IT. IT will integrate it with other support capabilities and attempt to mitigate identified risks.

- **Other actions**, as decided upon by IT and the shadow IT user(s).

The goal of discovery is to decide how to move forward with each piece of unauthorized or prohibitive shadow IT. Shadow IT impacts people, their motivations, as well as some potentially business-critical processes or information.

This discovery policy should typically be defined, approved and sponsored at the C-Suite level, to avoid turf wars before putting it into place. If the discovery process does not resolve between the CIO and the shadow IT users, it should be escalated to the C-Suite for resolution.

Advantages of embracing shadow IT

Surprisingly, shadow IT isn't all bad. Something that might initially be shadow IT could present an opportunity for the organization. That is, the benefits of these solutions could outweigh the associated risks. That's especially true with common cloud-based applications. After all, if that many employees are using a shadow software solution, it might be beneficial across a team or organization.

As long as certain "shadow IT" supports the security, redundancy, availability, and compliance policies of your organization, you could embrace the solution as part of Corporate IT, moving it from prohibited to sanctioned. Doing so could result in benefits in these areas:

- **Storage and backups.** Providers assure storage and backups, so the inherent services and operational costs are a fraction of on premises storage infrastructure. In an Office365 environment, for example, an organization may decide to store user files in OneDrive rather than on corporate owned file servers.
- **Data ownership and auditing.** In a cloud environment, every file has an owner as well as complete metadata about the user who shared it and from where. Accountability auditing is assured.
- **Data retention.** Typically, providers offer a complete track record, including file creation and access.
- **Data classification.** Most cloud-based services allow a wide range of classification tags.
- **Access control.** Cloud environments, by default, allow you to define user categories and enable authentication methods.
- **Mobile device/application control.** Mobile control is native in cloud environments—a big plus over in-house work.
- **Encryption.** By default, data is encrypted on the service provider's side.
- **Federation.** It is possible to make the corporate SSO access option the only way to access the environment.

Shadow IT is opportunity

By understanding shadow IT, the needs and expectations of IT users, and the risks associated with the practice, organizations can transform shadow IT into a safe and useful arsenal of tooling that drives disruptive innovation.

Before that happens, you need to devise strategies that work toward the collective goals of employees, IT departments, and the business. Done correctly, support for new technologies can create new opportunities for organizations to deliver better products into the market, faster, and

through convenient efforts on the part of IT users at the workplace.

Additional resources

For more on topics like this, explore these resources:

- BMC Business of IT Blog
- BMC Service Management Blog
- BMC Security & Compliance Blog