HOW TO REDUCE RISKS OF SHADOW IT BY APPLYING GOVERNANCE TO PUBLIC CLOUDS

According to Gartner, almost a third of successful cyber attacks will be directed at companies' shadow IT resources by the year 2020. This prediction, among others, demonstrates how significantly most organizations underestimate the number of shadow IT applications their employees are already using, as well as the major consequences that would result from a data breach as a direct repercussion.

MVISION Cloud's (formerly Skyhigh Networks) annual Cloud Adoption and Risk Report recently stated that the average enterprise uses 1,935 different cloud services, which is an increase of 15% over the last year alone. When employees choose a cloud service, they often ignore its security limitations and inadvertently expose corporate data to risks, a problem that clearly is only going to amplify as companies continue to migrate to the cloud. With each organization generating an excess of 3 billion events each month (such as logins, edits, deletes, shares, uploads, etc.), leaders must take strategic measures to both reduce the risks associated with Shadow IT solutions as well as establish structured policies to control the need.

What is Shadow IT and Why Does It Happen?

Shadow IT refers to when an employee uses IT technologies, solutions, services, projects, or infrastructure without formal approval and support of the internal IT department. This can include free and bought systems and encompasses SaaS, PaaS, IaaS, off-the-shelf software, and hardware

like computers, tablets, smartphones, and other devices.

For a variety of reasons, individuals typically steer around IT to increase productivity and agility in their own operations, with the most popular being SaaS offerings that address certain issues the user is looking to address. While this in itself isn't malicious, it quickly results in management losing its overview of employees' use of cloud applications and their cost, and can open up the network to serious data compromises.

Some common reasons for Shadow IT include:

- The wait for formal approval is too long or troublesome
- The internal environment is less developed than the public services already available
- The internal environment offers little to no self-service, a major challenge especially for the DevOps team when focusing on continuous life cycles and rapid software developments

For most users, adopting Shadow IT is meant only to fulfill their job duties in the most efficient and effective way possible. One of the best ways for companies to respond to this need is to revise their governance process that supports employees while facilitating innovation.

Applying Governance to Public Clouds

Cloud Governance plays a vital role in compliance, security, cost control, and performance, as well as in the reduction of Shadow IT. While not that different from the general IT governance policies, it is crucial that cloud services are taken specifically into account and have their own defined structure.

Governance in the cloud can be difficult because of its distributed nature. One of the first things for organizations to explicitly address is who is responsible for the security and privacy of certain cloud services, whether it be the IT department, individual user, or the service provider, for example.

Compliance also becomes a necessary piece of cloud governance, especially in fields like healthcare. Data must be tracked and all access to information must remain under control of the IT department in order to remain compliant.

When developing a cloud governance structure, it should leave plenty of room for growth through the use of new technologies, which are able to be vetted, available, and provisioned for the necessary user at a quick pace. The policies should enforce security and mitigate risks, but should also be flexible enough to evolve with the changing needs of IT employees and users.

What Should a Cloud Governance Policy Cover?

Regardless of the chosen factors included, the cloud governance policy should be created and regularly reviewed by a team of both IT experts as well as managers or executives. This combination and frequency ensures that policies stay up-to-date with the latest technologies while at the same time including ways in which cloud infrastructure meets and impacts business activities.

One of the most common items that should be included in the cloud governance policy are the uptime expectations as defined by specific business requirements. Different tiers of applications might be established based on how critical they are to the daily success of the business.

Tiers can also be useful when categorizing cloud services based on risk. By dividing cloud services

into high-, medium-, and low-risk buckets, it is easier to enforce data loss or prevention policies on the lower risk apps while blocking high-risk services if deemed necessary.

Since the deployment and usage of web applications is the most common form of Shadow IT utilized in enterprises, having a specific policy just covering when and how SaaS environments are acceptable is another must-have in the governance structure. This policy can be as lax or explicit as desired, but it allows IT and businesses to maintain visibility and security of departments' services.

Other important factors to consider including in the policy might include standards for the design of infrastructure, disaster recovery plans, programming standards, and how to monitor apps and infrastructures. Security and mitigating risks are huge components to cover, with clearly outlined measures to access cloud services, such as a central login point, along with which employees should receive certain authorizations and permissions.

Benefits of Strong Cloud Governance

- Automation – working established processes and workflows can be automated, significantly raising efficiency
- Innovation – the evolution of cloud offering is driven by the provider which in-turn creates effective opportunities to evolve one's IT infrastructure at a low cost
- Optimization – having a huge integration capacity that can leverage the existing potential of alternative, more capable infrastructure that can be installed/integrated within a matter of minutes, hours or a few days
- Change – proper processes in place over a highly dynamic and responsive IT landscape facilitates change management, quality assurance, and compliance
- Profitability – Organizations with above-average IT governance have been shown to have more than 20 percent higher profits than those with poor governance following the same strategy

Embracing Shadow IT

Shadow IT is inevitable, and as an organization, you can choose to understand your users and find ways for them to use the cloud services they need to fulfill their job duties, or, you can attempt to crush Shadow IT like a bug and eliminate it completely. No matter what route you choose to go with, one thing is for sure: Shadow IT exists at extremely high levels and there must be some type of plan put into place before a massive security breach of sensitive data occurs.