Research Note

Shadow IT and Organizational Risks

Nicholas Montgomery

August 2017

Keywords: Shadow IT; cybersecurity; cloud technologies; operational risk

Abstract: This paper discusses the rising prevalence of and risks associate with shadow IT - the use of unauthorized devices, software, and services - on organizations. After examining these risks, the author goes on to identify recommendations to help prevent shadow IT and allow organizations to enable business units to be able to make smarter purchases.

Gartner defines shadow IT as "IT devices, software, and services outside the ownership or control of IT organizations."[1] Essentially, any device or software being used inside of an organization that the IT department has not approved the use of can be categorized as shadow IT. Shadow IT can be happening in different ways, including the use of social media without the approval of IT. Employees may not even know that they are conducting shadow IT because they are either unaware of what it is or unaware of the current policies that an organization has in place with the usage of non-approved applications. However, these employees are potentially putting both an organization and any sensitive information that they are handling at risk if the proper measures are not taken. This paper will explore the risks associated with shadow IT and make recommendations to an organization for ways to combat them.

The rise of cloud technologies has been one of the main driving forces behind enabling shadow IT in an organization, specifically Software as a Service (SaaS). Although cloud technologies are not the reason for why shadow IT first started, it is one of the major reasons for its rapid growth.[2] SaaS is one of the three cloud services that are offered, the others being Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). SaaS gives the least amount of responsibility and ownership to the organization or user, having ownership of the application and the maintenance left to the responsibility of the service provider. SaaS also makes it easy for users to be able to access it from anywhere with an Internet connection and all the user does is use their own data to put inside of the application. This makes the use of these applications extremely convenient for the user to begin using and will often come at a low, or even no, cost.

There are multiple reasons why employees are using these non-approved SaaS applications, from people simply wanting to do their jobs to the employee not knowing that an application needed to be approved by IT. Frost & Sullivan conducted a survey from a range of different sized companies that made many discoveries about the usage of non-approved SaaS applications. Of the respondents, 80 percent of which admitted to using applications that were not approved by the IT organization inside of their company. A very surprising discovery was that more IT professionals admitted to using shadow IT than the line of business users were, with 83 percent of IT professionals and only 81 percent of line of business users admitting to using the non-approved applications. There are many implications for why this is happening, including that the IT professionals believe that because they understand the risk that they are confident with knowing how to mitigate it. Whether the ability for them to mitigate the risks is true or not, it is still leaving an organization at risk.[3]

There are four risks associate with shadow IT for businesses that will be discussed in this paper. The first is vendor or third-party risk, or the risk that arises when an organization relies upon outside sources to preform services on their own behalf.[4] The second is the legal risk of shadow IT, or risk that comes when failing to be compliant with government statutory or regulatory obligations.[5] The third risk is the financial risk that an organization will face, or the risk that a company may not be able to meets its financial obligations.[6] Finally, the last risk that will be discussed is reputational risk, or the threat to the name and standing of an organization.[7]

The first of the risks that will be discussed is the vendor or third-party risk. This deals with the risk behind the vendor not properly keeping either the sensitive information or their own systems secure. This can also be an issue if the proper research on the vendor has not been conducted in advance. Some vendors may be more prone to having security flaws or breaches and can be a liability for the organization. If the employee decides to place sensitive information onto the applications that the vendor is hosting and the vendor was to experience a breach, the sensitive information may be accessed by unauthorized users or potentially stolen. This can have some serious implications on an organization that trusted the vendor with this information, especially because an organization might not even know that the vendor is housing this information unless the employee reports it. If the information is intellectual property or trade secrets, this can lead to another business using the information for their own use and potentially reducing advantages that an organization previously had.

There is also the risk that the user is using the same account name and password on the vendor's application that they are using inside of their own business. It is common for users to recycle the same username and password across multiple different applications, posing large risk if the credentials are taken. A study from Ofcom, a communications watch dog in UK, suggested that 55 percent of users used password for most or all websites, making the risk of credentials being repeated reasonably high.[8] If the user with the stolen credentials had access to sensitive information and proper measures are not taken, such as regular password resets, the hackers may use those credentials to infiltrate an organization. This could then lead to a hack of an organization because of the vendor, but all comes down to the employee who originally used a vendor without the IT department's approval.

The second risk is the legal risk that comes with shadow IT. With the use of non-approved applications by the user, the user may be using applications that will make the organization no longer compliant with certain compliances. An example of this in the past is the use of Dropbox with sensitive information. There have been cases of nurses using Dropbox to share patient information back and forth with each other because the file sizes were too large for emails and the internal IT had not supplied a file sharing application that the nurses were using. The problem with this is that the use of Dropbox would make the hospital no longer compliant with HIPAA, and the survey conducted by Frost & Sullivan showed that of the 36 percent of respondents who were using Dropbox unapproved, 16 percent of those have experienced a security event.[9] If the sensitive information is stolen from an organization, this has the potential for heavy fines to be placed.

Shadow IT also brings a financial risk to an organization. Without approval from IT for applications or cloud services, the purchases being made may already be owned by the organization or people may be purchasing more than what they will need for their usage. Without the approval or consultation of the IT organization, business units may not be aware of all the options that are available to them and may not have educated staff making the purchasing decision to know how much of that service they will need. This can also lead to multiple business units purchasing the same service without the IT department even knowing. Cisco had found that 28 percent of the total amount of IT spend a company does is completely outside of the IT department.[10] Of that 28 percent, there is the potential that funds are being spent inefficiently and may have a significant impact on the amount of revenue that an organization will make.

Finally, the last risk is the possible damages to the organization reputation from Shadow IT. The use of non-approved applications has been shown to lead to a higher risk of having a security event with sensitive data. If sensitive information is stolen from an organization, consumer trust of an organization can decrease and it can have an impact on customer loyalty if not properly handled. This can also double as a financial risk because the decrease in loyalty may influence the amount of money that an organization will make. If consumers do not trust an organization with their sensitive information or are worried that the information may be stolen, there is a possibility that the consumer will make the decision to support a competitor's business instead of their own.

Shadow IT may have many potential risks that can have a serious impact on an organization, however there are multiple different ways to combat shadow IT. The following will discuss five recommendations to an organization that will help prevent shadow IT and allow an organization to enable an organization units to be able to make smart purchases. These five recommendations are that an organization should have a well-educated IT/Cloud Broker; proper software should be implemented in an organization; the IT approval process for applications should be streamlined; the policies for applications should be inclusive instead of exclusive; and finally that an organization needs to communicate with and educate its employees on its policies and shadow IT.

The first recommendation is for an organization to enable the purchasing ability of business units by having a well-educated IT/Cloud Broker on hand to consult for IT purchases. This is someone who will be knowledgeable on the current business and what it can offer its employees, as well as knowing the market and knowing which tools are available with the right vendors. This will enable business owners to be able to make swift purchasing decisions with the help of the broker. It will also provide the IT department with information on what is being purchased and used inside of an organization. This will give business units the ability quickly determine what the current available options to use are within an organization, and then make a swift purchasing decisions if none of the available options are a right fit for them. Business owners might not be aware of the available options to them are, but the broker will allow a quick way to learn them.

This will also help to build a stronger relationship between the IT department and the rest of an organization. Without a strong relationship, business units may not listen to the advice or policies that are implemented by the IT department; having shadow IT continued to be conducted inside of an organization.

The second recommendation is for an organization to implement software to help the IT department detect when shadow IT is going on, as well as secure the use of applications. This is a way to help automate the discovery process by monitoring the network and being able to see when non-approved applications are being used in the work place.[11] When non-approved applications are being used, this gives the IT department a chance to act upon the situation and for them to be able to seek out the answer to why this application is being used. If an application is being used because IT does not currently have an application approved that can fill that specific need, this gives an opportunity for the IT department to act upon the situation by understanding the behavior of employees, as well as allowing them to work towards approving an application for that need. This will enable the IT department to consistently tackle shadow IT as it is detected in an organization.[12]

Implementing software that will secure the use of these applications will also help an organization stay secure when these applications are being used. If an application sends its packets unencrypted, this leaves open the opportunity for someone to dive into the packets and see the information inside. An attack like a man-in-the-middle attack would benefit from unencrypted traffic. The man-in-the-middle attack is when a person has traffic diverted to a device that allows them to monitor and see all the packets, which would allow them to look inside certain packets and steal any important information. By having software that will encrypt the traffic, this will allow users to use applications that originally did not encrypt the traffic that it sends.[12]

Third, the IT department should redesign and streamline the approval process of applications inside of an organization. This will allow people to stay true their want of doing their jobs, while also allowing for people to complete their tasks in a secure way. The ability for the IT department to continuously deliver solutions swiftly will help decrease the likelihood that an employee will totally skip the process and use an application that is not currently approved. This will also help increase the amount of applications that are approved for usage by employees. A speedy approval process allows for the ability for employees to look at the IT department as a tool for helping them use applications, instead of a deterrence.[12]

Fourth, an organization needs to create a policy that is inclusive to new applications instead of being exclusive. You do not want to try to force your employees into using only one application, because this can lead employees back into their habits of using applications that are not approved by the IT department. As previously stated, people just want to do their jobs and get their tasks done in a timely manner. By having a policy that is inclusive to these new applications, the IT department will be able to better recognize the risks of using all the additional applications and create plans on how to handle security events that are to arise. This will also allow employees to be more comfortable reporting security events that are to occur. Employees should not be punished for committing shadow IT because this will lead to them not wanting to report anything to the IT department to save themselves. Having an inclusive policy will include protecting the employee if an event is to occur. This will help an organization because the sooner that a security event is reported, the sooner an organization can work towards mitigating any further damages that are to occur.[12]

Finally, the last recommendation is that there needs to be communication on the policies and solutions that a company offers, as well as employees needing to be educated on these policies and processes. When new policies and processes are implemented into an organization, employees need to understand them and be aware, especially inside the IT department itself. Employees should also understand the proper actions to take if a security event is to arise, as well as understand the need for quick reporting. Employees who do not know what to do if they are to perceive that an event is happening may report it for fear of the repercussions. However, an employee who has been trained on what to do will know the process of reporting an event and can potentially save the company a lot of trouble and money in the future.[12]

Overall, shadow IT is currently affecting businesses in a significant way, and there is not a whole lot of options to stop employees from wanting access to other applications in addition to what an organization currently offers. With the vendor, legal, financial, and reputational risks that come along with shadow IT an organization needs to be able to adapt and change its policies to work with its employees, not against them. To accomplish this, an organization should implement multiple different strategies, including: Having a IT/cloud broker, implementing the right software to detect shadow IT and help improve applications, redesigning and streamlining their application approval process, having policies that are inclusive instead of exclusive to new applications, and finally to communicate and educate their employees. All the recommendations mentioned in this paper will allow for an organization to enable employees and business units to be able to use or buy applications, however it enable them in a way that will also keep an organization aware of these purchases and protect sensitive information from being accessed.

[1] "Shadow IT." Gartner. N.D. Accessed <www.gartner.com>.

[2] "FAQ: How Does Shadow IT Complicate Enterprise Regulatory Compliance?" *SearchCompliance*. Oct. 2012. Accessed <www.searchcloudcomputing.techtarget.com>.

[3] *The Hidden Truth Behind Shadow IT: Six Trends Impacting Your Security Posture*. Frost & Sullivan. Nov. 2013. Accessed <www.mcafee.com>.

[4] "Third Party Risk." Federal Deposit Insurance Corporation. Jun. 2013. Accessed <www.fdic.gov>.

[5] McCubbrey, Don. "What is Legal Risk?" *Boundless*. 2014. Accessed <www.boundless.com>.

[6] "Financial Risk." *Investopedia*. N.D. Accessed <www.investopedia.com>.

[7] "Reputational Risk." *Investopedia*. N.D. Accessed <www.investopedia.com>.

[8] Culey, Graham. "55 Percent of Net Users Use The Same Password For Most, If Not All, Websites. When Will They Learn?" *Naked Security*. 23 Apr. 2013. Accessed <www.nakedsecurity.sophos.com>.

[9] "The Hidden Truth Behind Shadow IT." McAfee. N.D. Accessed <www.mcafee.com>.

[10] Diana, Alison. "Bring Shadow IT Out of the Dark, Gartner Tells Tech." *EnterpriseTech*. 17 Jun. 2015. Accessed <www.enterprisetech.com>.

[11] Moyle, Ed. "5 Strategies to Combat Shadow IT." *SecurityCurrent*. 11 Sep. 2014. Accessed <www.securitycurrent.com>.

[12] *The Hidden Truth Behind Shadow IT*.