Growing Pains in the Cloud II: The People vs. The Ministry of No

Following on from the NTT Communications Growing Pains in the Cloud report comes exclusive research revealing the growth of shadow IT and why many enterprises are now dependent on it.
In one corner we have the IT department, let us call them the ‘Ministry of No’. In the other corner we have ‘the People’; IT users who are bypassing the Ministry’s rules to procure cloud services directly to get their jobs done. By doing this they are breaking security policies and hiding expenses. The last thing an enterprise wants is a clash on its hands that might jeopardize business. So how can the situation be defused?

Certainly from our experience, the IT department’s self-image is that of an enabler, helping the company protect itself and maintain compliance and that rogue users are the scoundrels in the camp. There is a danger here of breeding an ‘Us vs Them’ mentality – a tug of war where each side is pulling the other in the name of value creation. Such internal battles, if they exist, are enormously counter-productive, wasting time and energy and potentially damaging customer relationships.

It is clear the IT landscape has changed to the point that customers are no-longer locked in and can change to another supplier more easily than ever before. There are still costs in doing so, of course, but the added mobility means that front line operational and sales staff are turning to shadow IT for its flexibility - being able to work from anywhere on any device, speeding up their responses to customers.

This snapshot shows IT users being in control of their computing needs. So much so that 77 per cent of those surveyed said stopping using these services would limit department functionality.

But look at the bigger picture. This agility comes with associated risks. Employees procuring ad hoc cloud services often have no knowledge of where data is stored so could inadvertently be contravening one of many data protection and financial regulations. This will become a bigger issue in 2018 with the launch of the EU General Data Protection Regulation, which means organizations will need to take far greater responsibility for their data or risk hefty fines.

Unsanctioned cloud usage could also be putting enterprises at risk of data leakages, breaches and hacks – with the IT department powerless to support what they do not know about. Furthermore, decentralized procurement can also be expensive; buying-in applications and services individually means that enterprises may not be getting best value or the most appropriately designed services.

Media coverage would suggest that shadow IT has moved from the margins to the mainstream; witness the ongoing uproar over US presidential candidate Hillary Clinton’s private email server. But just how much truth is behind the headlines - is it really that commonplace? Has the IT department lost control? Do business units really want to run their own IT services?

To find out, we commissioned an extensive study of European enterprises to understand the motivations behind shadow IT and how prevalent it is within large organizations. We talked to CIOs and managers from business units.

We found that IT departments are fully aware of the existence of shadow IT, but feel powerless to stop it. Business units believe red tape is blocking them from getting the business critical tools they need from the IT department. Both parties recognize the security and financial implications, yet believe shadow IT is the new reality and will only grow.

The results of this survey might surprise you and make you take a fresh view of the role of shadow IT in your own organization. Perhaps you will recognize that shadow IT is the symptom of something deeper, but the prognosis is good if both sides can find a way of working together with IT as the enabler serving responsible users.

NTT Communications, June 2016
EXECUTIVE SUMMARY

The aim of this research was to understand the scale of shadow IT and the different perspectives of IT decision makers (ITDMs), representing the Ministry, and business decision makers (BDMs), representing ‘the People’. In all, we surveyed 250 ITDMs and 250 BDMs, from European enterprises with at least 1000 employees. We found that:

1. **Majority of organizations experiencing shadow IT:** 78 per cent of business decision makers (BDMs) admit that employees in their department were using cloud services without the IT department’s knowledge. 77 per cent of ITDMs were aware of this happening in their own and other departments.

2. **Widespread throughout organizations:** 57 per cent of respondents believe that shadow IT is happening in at least half the departments in the enterprise. 27 per cent believe shadow IT is occurring in the majority of departments.

3. **No plans to stop:** Shadow IT has been used on average for 18 months, and 83 per cent of respondents believe it will increase in frequency over the next two years.

4. **Why they do it:** Main reasons for using shadow IT are speed of set-up (62 per cent), ease of use (52 per cent), choice (30 per cent), price (29 per cent) and that the IT department does not understand their needs (28 per cent).

5. **Shadow IT has become essential:** 80 per cent of respondents believe that data stored in shadow IT is critical to their organization, and 77 per cent think that stopping using these services would limit department functionality.

6. **Free cloud storage is a double edged sword:** 83 per cent of those surveyed use popular free, unregulated cloud storage applications such as Google Drive, Dropbox and Apple iCloud for sharing company information. Storage can be a cloud driver, but needs to be managed correctly.

7. **Data location unknown:** 56 per cent of respondents do not know where all or some of their data is stored when employees use shadow IT. Of those that do think they know where the data is, 44 per cent recognize that it may be stored outside of their region.

8. **Rules are for breaking:** 73 per cent of respondents believe that their employees are knowingly breaking the rules and compliance when they provision their own cloud services.

9. **The appeal of a Cloud Amnesty:** 70 per cent of BDMs believe their department would voluntarily give up control of their cloud accounts, even if access to most services were disabled.

Research Methodology

*NTT Communications commissioned independent market researchers Vanson Bourne to carry out a survey of 500 respondents in France, Germany, Spain and the United Kingdom in March 2016. Respondents were from companies with at least 1,000 employees and represented a wide variety of industry sectors. The respondents included 250 IT decision makers and 250 business decision makers.*
Cloud computing has been widely embraced within enterprises. Most organizations (98 per cent) use cloud services, with 73 per cent saying they will increase the use of cloud services over the next two years. Currently, 94 per cent of enterprises have at least two cloud services.

The most common cloud service is business productivity with over half of enterprises using Microsoft Office 365. More than a quarter are using sales, Customer Relationship Management (CRM) and marketing software from Salesforce. Many enterprises are continuing to manage applications themselves but in a shared environment. Microsoft Azure (48 per cent) is the most dominant of these platforms followed by Google App Engine (28 per cent), NTT Enterprise Cloud (16 per cent) and Amazon AWS (15 per cent).

The picture that is emerging is that no single cloud service can deliver all of the IT needs of an enterprise: 42 per cent of enterprises have at least four clouds.

Q: How many cloud services does your organization officially use?

(Based on ITDM respondents whose organization uses at least one cloud service)

Q: What cloud services are your organization currently using?

(Based on ITDM respondents)
The appeal of cloud services is that they offer on-demand computing without a huge management effort. Cloud services are typically easy to order, provision and consume, without having to go through the IT department, which is seen as the ‘Ministry of No’ by many employees, because it does not or will not supply the applications they want. By skipping internal processes and procuring cloud services without the involvement of the IT department, business units are potentially putting their organization at risk.

Our research reveals that shadow IT is viewed as legitimate by many people. In fact, 77 per cent of BDMs in our survey admitted that their departments were using cloud services without the knowledge of IT. An almost identical number of IT decision makers also believe their own IT staff and other departments were commissioning cloud services without permission. From these findings one can assume that IT departments are either turning a blind eye to shadow IT because they feel powerless to stop it, are too busy keeping legacy systems going or don’t believe it is an issue.

Our research found there is a wide range of cloud services being procured without the knowledge of IT departments. Software-as-a-Service (56 per cent), Infrastructure-as-a-Service (48 per cent) and public clouds from Amazon AWS, Microsoft Azure and Google Cloud Platform, among others (39 per cent) are the most common.

The findings suggest both the business and IT have a similar picture regarding the use of unsanctioned cloud services: 78 per cent of ITDMs were aware of shadow IT, compared to 77 per cent of BDMs. From this it would appear there are no pain points. But its dramatic growth appears to underline an issue. The low cost and easy availability of cloud service subscriptions has allowed anyone with a credit card to buy enterprise information applications. This has allowed employees to buy the applications they want to use, rather than the ones they are told they can use by the IT department, according to research by PricewaterhouseCoopers (PwC)1.

Do users adopt shadow IT in a carefully considered way or on the fly and in a hurry? If you look at the wider vista, it seems that employees and departments adopt applications pragmatically. They have tasks that require completion and will find the best applications available to do this as quickly and efficiently as possible, even if it means bypassing the IT department.

There is a host of cloud services that employees can choose from to help make work easier; services that enable users to backup, store and share information in the cloud and access it from other devices such as smartphones or tablet PCs. Employees can upload work they need into the cloud and access it later while traveling, from home and from multiple devices.

Free cloud storage is on the increase and 70 per cent of respondents expect its use to become more widespread. The problem is that shadow IT can create major problems for data storage protection because files can be created, edited and shared within the enterprise without them ever touching the IT department. IT, for example, cannot back up files it does not know exist.

When employees open cloud accounts, they often establish a personal contractual relationship with the cloud service provider, which means that if they leave the organization, the data may be difficult for their former employer to recover. In addition, there is the risk of employees uploading company data to free storage and file-sync websites that are outside the scope of the corporate security policy – leaving the enterprise exposed to data leaks and breaches.

1 PricewaterhouseCoopers - Managing Risk in the Cloud
Q: Do you expect the usage of free cloud storage to increase?

Expect the amount to increase

- 70% for Total
- 63% for ITDMs
- 78% for BDMs

(Based on respondents who say that free cloud storage services are used within their organization without the approval of the IT department)

Q: Which free cloud storage services do you use?

- Google Drive
- Dropbox
- Apple iCloud
- Amazon Cloud Drive
- OneDrive
- BT Cloud
- Box
- WeTransfer

(Based on respondents who say that free cloud storage services are used within their organization without the approval of the IT department)
Most businesses are under pressure to drive down costs or expand rapidly into new markets, and IT is a critical enabler in this. So, if the IT department cannot respond quickly enough or with the right solutions, or just simply says “no” to demands, business departments will continue to bypass them and provision their own IT solutions. Our research found that most organizations (83 per cent) expect shadow IT to increase.

Q: Do you expect the usage of shadow IT to increase?

83%  80%  87%
Total  ITDMs  BDMs

Expect the amount to increase

(Based on respondents who say that cloud services within their organization have been commissioned without the involvement of the IT department or say that free cloud storage services are used within their organization without the approval of the IT department)

The problem is that uncontrolled IT procurement can create silos and duplicate services causing costs to spiral upwards. CIOs need to find a way to embrace a borderless world, where they can provide the tools that business departments require, while working together on IT decision-making to ensure the most appropriate IT solution is employed for the job. This means engaging employees in the process. Today every employee should be viewed as a digital employee, according to Gartner².

Technologies available today make it easier than ever for business departments to adopt their own technology solutions. To avoid this, CIOs need to work more closely with business departments to ensure that they are providing the services necessary to maintain a competitive edge.

² Gartner - Workplace of the Future
Public cloud and SaaS typically offer rapid installation, ease of use and familiarity with consumer apps, which entices users to reach out and get what they want immediately rather than have to go through IT’s approval and ordering processes - where on occasion they are told they can’t have the solution they want.

Of the respondents that said cloud services have been commissioned in their organization without the knowledge of the IT department, 62 per cent said the prime motivator was that they were easy to set up. 52 per cent of respondents said ease of use was a defining factor. In addition, 29 per cent said they felt shadow IT provided a cheaper option (compared to the cost charged by the IT department).

These motivations reflect that businesses need to become more agile as part of digital transformation. They need to be able to keep the lights on, while having resources available for innovation.

Our research suggests that employees believe cloud providers can deliver the services they want at a fraction of the time and cost than the IT department can. If IT doesn’t find a way of bringing shadow IT into the fold, employees will see the IT department as a block and continue to look outside for the solutions they need.

Shadow IT carries both risks and opportunities – but where shadow IT does occur there is a chance for IT to really understand the functionality that business departments require. By collaborating with business departments, IT can provide secure scalable solutions that satisfy business needs.

Q: What are the key motivators for using shadow IT?

![Bar chart showing the key motivators for using shadow IT.]

<table>
<thead>
<tr>
<th>Motivator</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is quicker to set up</td>
<td>70%</td>
</tr>
<tr>
<td>It is easier to use</td>
<td>60%</td>
</tr>
<tr>
<td>To get the service needed</td>
<td>50%</td>
</tr>
<tr>
<td>It is cheaper</td>
<td>40%</td>
</tr>
<tr>
<td>Departments understand their IT needs better than the IT department</td>
<td>30%</td>
</tr>
<tr>
<td>There are technology experts in the departments</td>
<td>20%</td>
</tr>
<tr>
<td>IT security policies wouldn’t allow it</td>
<td>10%</td>
</tr>
<tr>
<td>Other</td>
<td>10%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>0%</td>
</tr>
</tbody>
</table>

*(Based on respondents who say that cloud services within their organization have been commissioned without the involvement of the IT department or say that free cloud storage services are used within their organization without the approval of the IT department)*
Nearly everyone using unauthorized cloud services recognizes that they are breaking IT corporate policy, although they may not understand compliance issues. But this does not appear to be a barrier to their use if they need to get a task done and believe it is the most efficient solution to get it completed quickly and efficiently. 84 per cent accept that their shadow IT actions could put the enterprise at risk.

So why do they continue to do something they know is wrong and risky? The simple answer could be convenience.

Q: Are you aware you are breaking enterprise governance and regulation?

97% Yes
3% No

(Based on BDM respondents)

Q: Does a cloud service used in the organization for which the IT department was not involved in commissioning or approving pose a risk to the organization’s IT security?

84% Yes
16% No

(Based on all respondents)

Q: Do you access public cloud services for personal use on work devices?

85% Yes
15% No

(Based on BDM respondents)
CRITICAL DATA: LOCATION UNKNOWN IN THE CLOUD

Widespread use of cloud services can result in critical data such as customer records being dispersed across different locations and regions. This is exacerbated when there is no record of what cloud services are being used. Respondents estimate that 80 per cent of employees store critical company data in unauthorized cloud services.

With accounts set up on a personal or departmental level, there could be literally hundreds of places where sensitive data is stored online, making management of those files almost impossible to secure. Over half of respondents admit they do not know where their data resides. This will need to change with the General Data Protection Regulation (GDPR), which will lead to a greater degree of data protection harmonization across the EU.

With the arrival of GDPR legislation in Europe in 2018, organizations will need to know where cloud apps are processing or storing data. They will also need to understand the security controls for the applications they use, and either block or institute compensating controls for ones that have insufficient security.

While the benefits of using a SaaS delivery model are well documented, enterprises need to recognize that employees are possibly using the same delivery mechanism without the help, visibility or consent of the IT department to share proprietary corporate information. Storing critical data outside the jurisdiction of IT opens up significant security risks. Storing or sharing business-critical data in non-authorized cloud services leaves enterprises exposed to internal breaches, where employees, partners or contractors can end up leaking this data intentionally or unintentionally.

Q: Are you storing critical company data on cloud services in shadow IT?

- Yes: 79%
- No: 18%
- Don’t know: 3%

(Based on respondents who say that cloud services within their organization have been commissioned without the involvement of the IT department or say that free cloud storage services are used within their organization without the approval of the IT department)

Q: Do you know where your data is?

- Yes, I know where it is stored for all of the cloud suppliers we use: 44%
- Yes, but only for some of the cloud suppliers we use: 39%
- No, I do not know: 17%

(Based on respondents who say that cloud services within their organization have been commissioned without the involvement of the IT department or say that free cloud storage services are used within their organization without the approval of the IT department)
Our research shows that three-quarters of enterprises depend on shadow IT to run business processes - if they were blocked from doing so, it could have serious consequences on business departments and how they operate and could have a detrimental effect on business itself.

To retain a productive workforce, enterprises must adopt innovative technologies. By figuring out how to manage innovation, new solutions that can benefit the wider business can be found to add to the IT department offering.

Identity-as-a-Service (IDaaS), multi-factor authentication and user provisioning all help to eliminate risks. Allowing employees to use applications they feel comfortable with increases both productivity and employee engagement. In a study, PwC found that in 100 organizations it ranked as top performers, IT controlled less than 50 per cent of the IT expenditure. Users in these organizations evaluate and use software and IT solutions without being tied to IT’s decision making. PwC notes that moving to a world where IT is seen as an orchestrator requires a strong relationship between the CIO and the rest of C-suite executives by way of ongoing ‘digital conversations’.

Our research highlights the fact that IT needs to take a new approach to shadow IT. A traditional stance could result in stifling innovation, but may be seen as necessary to a compliance regime, while a free-for-all approach is a security breach waiting to happen. To truly capitalize on what shadow IT has to offer, a balance must be struck between the risks and values by setting guidelines outlining when shadow IT is acceptable and where such activities need to be reined in.

Q: What would the implications be if shadow IT was blocked?

<table>
<thead>
<tr>
<th>It would limit department functionality</th>
<th>Total</th>
<th>ITDMs</th>
<th>BDMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>77%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>81%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>72%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Based on respondents who say that cloud services within their organization have been commissioned without the involvement of the IT department or say that free cloud storage services are used within their organization without the approval of the IT department)
EMBRACING THE UNKNOWN

Managing a complex landscape of cloud platforms is a major challenge, but respondents believe it can be achieved by having a view on an enterprise’s entire IT estate.

Most enterprises believe it would be useful to have a single tool that could manage cloud providers, providing visibility in one view. NTT Communications has created such a tool: the Cloud Management Platform.

If enterprises are going to get the most from IT, they need to balance corporate governance and IT policy against convenience and operational agility. This is not an easy task, as the research shows. But if IT can be seen as the trusted advisor that can quickly provide the solutions required, while having its finger on the pulse of what applications are being used, employees will not need to look elsewhere and order will be restored. IT will no longer be seen as the ‘Ministry of No’, but instead as the ‘Ministry of Yes’.

Q: Would it be useful to have a single tool to manage cloud providers?

Based on ITDM respondents whose organization uses at least one cloud service

- Yes: 98%
- No: 2%

The first step towards regaining balance would be an amnesty where business units and users give up their cloud accounts to IT to manage. By managing all of the cloud services centrally, IT would be able to negotiate better contracts, recommend alternative services and optimize resources.

Our research found that 83 per cent of business managers would participate in a cloud amnesty where users could turn in their shadow IT cloud contracts with no repercussions, even if there was no guarantee that access to the cloud services would remain the same.
Q: Would cloud amnesty work in your organization?

(Based on respondents who say that cloud services within their organization have been commissioned without the involvement of the IT department or say that free cloud storage services are used within their organization without the approval of the IT department)
CONCLUSION

IT and business departments have fast realized the benefits of using cloud systems and applications, yet they still have not worked out a strategy for managing shadow IT as part of the overall enterprise landscape. The challenge is not how to prevent business units from choosing their own tools, but how to give them the tools they want within a controlled environment.

Employees are now comfortable with the process of acquiring and using cloud services, which has put the traditional role of the IT department as both selector and purchaser under threat. It isn’t possible to simply shut the door on shadow IT, because the research shows it is happening anyway, and IT departments know it is happening. Instead, a new approach to IT in the enterprise is required by which the risks and values of shadow IT are carefully balanced. It is only by taking this approach that IT can regain control and visibility of the IT estate, security and governance policies and budget.

The IT department needs to take on the role of enabler, not controller. It may not always say yes, but it needs to shed the ‘Ministry of No’ image. CIOs need to stop acting as gatekeepers and position their departments as functional enablers, embracing cloud deployment and agile project methodologies enabling the quick implementation of new ideas. This does not just focus on technology, it is about cultural change as well. IT needs to find a new way of working with business that is beneficial to both in the long-term.
It is important for IT leaders to keep in mind that the resources available to their users are better and more abundant than ever before. Here are a few recommendations for IT departments looking to harness the power of shadow IT:

**Use the systems your users use**

You may think you have figured out why users are specifically searching out new or different tools – but you will probably only truly understand when you start using them yourself. The lessons you learn here are invaluable when it comes time to discuss their use, or prevention of usage, with your user community. Get the C-suite to use cloud services and the rest will follow.

**Don’t be the ‘Ministry of No’**

Hold regular user groups with your staff. The employees who feel most passionate about the tools they use are exactly the ones you want to include in the decision-making. Make them part of the decision making process. Listen to what they need and the tools they’ve found. If necessary, explain to them why some systems are difficult to integrate into the company’s information management framework. Users that understand the limitations and are included in finding solutions will be your greatest allies and evangelists.

**Compliance is not security**

It is important to be compliant, but security doesn’t end there. You can demonstrate controls and procedures to your auditors, but if users make an end-run around them then you have not achieved anything. Only implement controls and procedures that you are sure your users understand and will follow.

**Get GDPR ready**

The implementation phase has started so it is time to get a real understanding of your IT estate. You have two years to ensure your data processing activities are in line with the newly adopted rules, so it is now time to start acting. It is sensible to undertake an audit of your IT estate and the impact that GDPR will have on your business, so that you can identify and start to implement any necessary changes.

**Implement a Cloud Amnesty**

If you demand that users tell you about their shadow IT practices, with the implication that these systems will be terminated, you may get a poor response. Instead explain that you understand why they are using external systems and promise them that you will help to find a way to either approve their use or find acceptable alternatives. Your users are only trying to get their jobs done - threatening to take their tools away does not help the situation.

**Research Methodology**

*NTT Communications commissioned independent market researchers Vanson Bourne to carry out a survey of 500 respondents in France, Germany, Spain and the United Kingdom in March 2016. Respondents were from companies with at least 1,000 employees and represented a wide variety of industry sectors. The respondents included 250 IT decision makers and 250 business decision makers.*