CIO Insights
Bringing Shadow IT into the Light

Section | Page
---------|-------
Executive Summary | 2
Backstory: IT Challenges Today | 5
IT vs Workforce Mobility | 6
The Workplace’s Attitude to Risk | 10
IT Today: The Police or The Enablers | 13
Conclusion: It’s All About Data | 15
It is clear that three disruptive forces are accelerating a change in workplace technology today, and these influences are driving organizations to rethink their IT strategies.

**Mobile**
Creating an expectation of anytime, anywhere access and transforming how businesses engage with customers and employees. Gartner recently predicted that tablets will become “the new PC” in 2015 when there will be nearly 321 million tablets shipped, versus 317 million PCs.\(^1\)

**Consumerization**
Transforming what users expect from an application and changing how IT is required to meet expectations. We are now in the era of user-centric IT. IDG recently found that 40% of businesses expect consumerized technologies to inflict a negative impact on enterprise security.\(^2\)

**Cloud**
Challenging the old ways of doing things and creating a new breed of competitors that can apply technology faster. Some would argue we are now in an ‘applications arms race.’ IDC recently predicted that the cloud software market will surpass $75 billion by 2017, an annual growth rate of 22%.\(^3\)

Further to this, Workshare surveyed more than 5,000 knowledge workers across EMEA and U.S. companies. The results showed that 81% of workers access work documents outside the office, 62% use their own personal devices for work, and 69% are resorting to free file sharing services to access their documents.\(^4\)

---

\(^1\) Source: Gartner, June 2004
\(^2\) Source: 2014 Consumerization of IT in the Enterprise, IDG Enterprise
\(^3\) Source: IDC MarketScape: Worldwide Datacenter Hardware Support Services 2013 Vendor Assessment
\(^4\) Source: Workforce Mobilization: What Your IT Department Should Know
The shift is forcing IT groups to support new ways of working and a move towards a more mobile and digital workplace. Leading analyst firm Forrester, recently highlighted that most enterprises will need to provide more structured and formalized support for employees using personal devices for work. These changes are set to challenge the modern-day CIO to stay on top of data compliance and governance issues while allowing their workforce to do what they need to do to get their job done.

Over four roundtable discussions twenty-six Chief Information Officers and senior IT professionals, representing a cross section of vertical markets across the globe, discussed how the trends of consumerization, cloud, and mobility are influencing IT strategies today.

This paper analyzes the discussions that took place: what current strategies are used, what issues are arising, and what the modern-day CIO’s IT strategy today must consider.
The last decade has seen huge advances in the world of technology, which has resulted in today’s workforce being connected more than ever. The way we work is evolving. It is important to understand that technology and business are symbiotic, so as one evolves, the other must adapt. This means the role of IT is becoming even more significant in the fast paced and dynamic workplace environment.

Globalization, cloud computing, and mobile working are all accelerating this move to a digitized workplace and impacting how business is done. In parallel with these trends, IT faces a constant tug of war between the demands of the end users and the demands placed upon them by their organisations.

End users want the freedom to work the way they want. They want simple-to-use applications and the flexibility to work from anywhere, on any device. The new ‘bottom up’ trend, influenced by these tech-savvy users, means new applications are brought to the attention of IT every day. IT groups must adapt to accommodate users’ needs while balancing the pressures from their businesses.

Business owners want more for less. They strive for enhanced work productivity (and ultimately increased profits) while reducing commercial risk. With the recent economic downturn still at the forefront of companies’ minds, there is a constant pressure for cost reduction, which has in turn impacted how organizations buy and apply technology.

Businesses are demanding different (preferably cheaper) pricing models and a streamlined, cost-efficient approach to deployment. Furthermore, distributed data – where corporate data resides – is also becoming more prevalent in discussions at business board level. In light of new global regulations, IT must ensure their strategy addresses compliance, risk, and security requirements.
The rise of Bring Your Own Device (BYOD) and Bring Your Own Application (BYOA) has led to a workforce that is more mobile than ever. As workers continue to mobilize, IT groups need to establish how to effectively control the growing number of mobile devices and applications in their organization, as well as protect the corporate data and documents that are being accessed and shared on them.

Forrester recently found that by 2015, most enterprises will have to provide more structured and formalized support for employees who use personal mobile devices for work. Does this change in strategy mean the power of what devices are used in the workplace has shifted to the user?

We asked the roundtable attendees:

Does your organization supply tablets for corporate use?

The semi- and highly regulated sectors, in particular banking and legal, did not provide tablets due to the security risks associated with them; while the less-regulated industries, such as entertainment, were more open to the idea. One banking representative explained that the high degree of sensitivity of the data that their workforce deals with means there is a need to be much stricter in enforcing corporate data policy on mobile working – surprisingly much stricter than the legal sector. They explained that the IT group monitors all emails and has a system in place that identifies if a large amount of credit card information, personal identifiable information, or other sensitive data is being shared externally. “The data we are working with is highly confidential; we put policies, systems, and procedures in place to protect our clients.”

Other CIOs argued that a soft copy of a document was actually far more secure than a hard (paper) copy if you have the right security measures in place. “The good thing about digital formats is that you have an audit trail and, therefore, the ability to track what has happened to a document. What if a pad of paper is left on the train? Digital means you are able to track the history of a document – who accessed it and when, for instance,” said a CIO from the retail sector.
It was also generally acknowledged that the present-day workforce is now circumventing IT and finding their own ways to access corporate data while out of the office. “Workers expect to be connected all the time. Even in the consumer space, apps such as WhatsApp and BBM are streams of continuous communication with participants always connected to each other.” As a result, there has been a significant increase in the use of unauthorized consumer apps in order to be ‘connected’ and to access information on the go. But the security risks associated with these are high, and cases of data leaks are becoming more and more prevalent.

End users will generally use whatever allows them to do their work easily especially if this demand is placed on them by their clients. If that means developing an unsecure way to work, then some will take that route

said an IT Director from the legal sector. This has resulted in a rise in use of shadow IT applications like Dropbox. All representatives around the table were aware of employees using similar Dropbox-type applications in their companies.

Does your organization supply tablets for corporate use?

<table>
<thead>
<tr>
<th>Sector</th>
<th>Percentage</th>
<th>Supply Tablets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal &amp; Professional</td>
<td>92%</td>
<td>No</td>
</tr>
<tr>
<td>Creative</td>
<td>89%</td>
<td>No</td>
</tr>
<tr>
<td>Finance &amp; Accounting</td>
<td>52%</td>
<td>No</td>
</tr>
<tr>
<td>Government NFP</td>
<td>29%</td>
<td>No</td>
</tr>
<tr>
<td>Pharma &amp; Healthcare</td>
<td>72%</td>
<td>No</td>
</tr>
</tbody>
</table>
Participants from financial, professional, legal, healthcare, and entertainment all said their IT departments had banned, and in some cases blocked, Dropbox. So, what is the alternative?

“Identity, trust, and reputation are what’s most important,” a legal CIO said in the case for replacing Dropbox. “When you can trust a company based on the relationship you’ve built with them, its more likely that you will trust them hosting and looking after your data. With some of the new start-ups, who knows if they’ll be around in five years’ time? Trust is key.”

One IT professional from a large legal firm described how they had created their own secure environment where internal and external parties could share documents. Based on the private cloud, documents must be shared in this area by all collaborators, and the result was a large decrease in the use of banned IT applications.
Most of the attendees agreed that Dropbox must be replaced with a solution of similar functionality. “If you say you can’t use this, then there must be a ‘but you can use this,’” a participant from the entertainment industry said. “There must be an alternative because there is obviously a need for it!”

A participant from the retail sector detailed how they had replaced Dropbox with a secure, enterprise-grade file sharing and sync (EFSS) alternative. This EFSS application provided the simple and intuitive, user-friendly design but had the security and control that the IT group required. “It is important that the app be easy to use, with features and designs like drag and drop and folders. This will make it easily adoptable.” He went on to suggest that the trends of BYOD or BYOA may have been superseded by BYOC – Bring Your Own Cloud. As mobile devices continue to add functionality and features, IT groups must try to mitigate the risk and security issues that come with their workforce using them.

In order to do your job, do you require access to your work documents from outside the office?

- United States: 84%
- EMEA: 89%
Hand in hand with mobility comes risk. Of course, IT departments are fully aware of the security implications that arise with enabling a mobile workforce and the use of unsanctioned consumer-grade applications in their workplace. But do end users understand, or even care about, the risks associated with them?

Do end users care about risk?

Based on the roundtable discussions, it was evident that some users simply don’t care about risk, despite many of their documents that they handle being confidential. “One thing that’s abundantly clear is that often our users do not understand the risks of divulging, losing, or leaking data – even if they have signed an AUP (Acceptable Use Policy)” a legal CIO said. He went on, “Lawyers have a different perspective in what’s secure and what isn’t. They often believe that they are practicing safe sharing behavior because they are more “tech-savvy” or “in the know” with the regular use of their smartphones and other devices.” Of course, they then go on to use Dropbox or other consumer-type applications and do not understand the security implications of these.

Another legal participant explained that the attorney’s mindset is to simply get the job done. When attaching a contract to an email and sending it, “They say, ‘Why should I check where it goes? It’s not my problem, as long as I can get my work done.’” One legal firm even stated that they offer their lawyers a short course on IT security, however the participant level is low and the dropout rate is high because “people just don’t care – they rely on IT to have it covered.”

The banking and financial industries seemed more confident that their employees understand the notion of risk, likely due to the reputational damage and significant fines that would be imposed on their organizations (and personally) if a data breach were to happen. “In banking, regulation based on directives from the FCA (Financial Conduct Authority) is principal – it’s all about content risk!” According to one IT professional for financial and banking, “In order for the end users to do the right thing, they need to be fully aware that if they share confidential information and data, knowingly or inadvertently, they will face disciplinary action.” As a result of this, he believes that responsible content sharing occurs as a matter of course.
Participants from the financial sector explained that it is now clients that are becoming increasingly more demanding about the information security policies adopted by suppliers, and in order to win business, a client’s basic security requirements and policies must be met. Another leading financial and professional service organization divulged, “Clients send all credit transactions securely, and if data is found to have been put in the cloud, then disciplinary action results. If there is a security breach, the organisation will be put out of business!”

Satisfying the client is now becoming an important factor for the legal sector also. “It’s the client that is leading the way as far as risk mitigation is concerned.” One IT Director said, “They ask what technologies we use and how our own technology vendors are assessed. They perform full audits and penetration tests, and it’s becoming even more important for firms with an international presence.”

The Head of IT from a leading educational institution brought up the influx of Generation Y in the Workplace now and addressed how they may change the attitude towards risk. “Look at social media; people share personal information, ideas, and details about themselves without a second thought. Over time, as users so easily share their own confidential information, will their attitudes to risk and how they share confidential work or client information change?” This is something IT must consider as Generation Y (“Millennials”) and Generation Z begin to flood the workforce.

In your opinion who is responsible for ensuring that sensitive company content isn’t inadvertently leaked?

- The person who sent it: 65%
- The organization: 15%
- IT Group: 13%
- The CEO: 3%
- Other: 3%

The organization
IT Group
3%
The CEO
3%
Other

Participants from the financial sector explained that it is now clients that are becoming increasingly more demanding about the information security policies adopted by suppliers, and in order to win business, a client’s basic security requirements and policies must be met. Another leading financial and professional service organization divulged, “Clients send all credit transactions securely, and if data is found to have been put in the cloud, then disciplinary action results. If there is a security breach, the organisation will be put out of business!”

Satisfying the client is now becoming an important factor for the legal sector also. “It’s the client that is leading the way as far as risk mitigation is concerned.” One IT Director said, “They ask what technologies we use and how our own technology vendors are assessed. They perform full audits and penetration tests, and it’s becoming even more important for firms with an international presence.”

The Head of IT from a leading educational institution brought up the influx of Generation Y in the Workplace now and addressed how they may change the attitude towards risk. “Look at social media; people share personal information, ideas, and details about themselves without a second thought. Over time, as users so easily share their own confidential information, will their attitudes to risk and how they share confidential work or client information change?” This is something IT must consider as Generation Y (“Millennials”) and Generation Z begin to flood the workforce.

In your opinion who is responsible for ensuring that sensitive company content isn’t inadvertently leaked?

- The person who sent it: 65%
- The organization: 15%
- IT Group: 13%
- The CEO: 3%
- Other: 3%
It is clear that the highly regulated industry workforce seem to understand the notion of risk and security, while other industries, such as education and legal have struggled to get the message to resonate with their employees.

We asked the CIOs, what does IT need to do to make their workforce care?

Two recurring themes in the answers were education and training; educating the users about the risk involved with sharing files and training users to use the secure applications installed to help them. Another suggestion was the use of notifications or pop-up messages. These alerts could appear to users to indicate that they are working off grid and are no longer working in a secure sharing environment. A final suggestion that seemed to garner support was by automating policy enforcement across all channels of communication. The automation of systems means IT can set the rules so that users do not even have to think about the risk.

So what exactly is the IT groups role today? Does the IT group hold a proactive role, where strategy and measures are put together early to prevent security breaches, or is it a reactive role, where IT reacts to situations as they happen?
Is ensuring corporate data security the responsibility of IT?

All participants agreed that while it was not their one and only focus, and that although security was an important function of their job, it was not their sole duty. A participant from the retail sector explained, “Risks are present across the board. Anyone who interacts with corporate data has a varying propensity to expose it.”

At this point the debate moved to whether IT should hold a proactive role in actively putting systems in place to prevent data breaches, rather than a reactive role and responding to issues as they arise.

Do you see your IT group as an enabler or the protector of data?

When the participants were asked: “Do you see your IT group as an enabler or the protector of data?” the CIOs across the industries ultimately agreed IT should be an enabler.

Surprisingly, a participant from the education sector explained they took more of proactive approach to risk. “When working on research projects, particularly those with high-profile clients with extremely commercially sensitive data, the university would not allow access to Gmail or any other web-based mail services. The university monitors for any unusual activity and take steps to find possible sources of breaches before they happen.”

It all eventually comes down to loss of money and reputation. Until there is a threat or major security breach or loss of reputation, we will continue as we are.

It is impossible to police everything that users ever do. Users will find ways around restrictive behaviors, so IT departments need to enable them.
In order for IT groups to enable and facilitate their workforce, they need to understand the way people work, their everyday workflow, and take into the account devices and software they use. Preventing them, or even trying to, is a recipe for disaster. IT groups must supply viable, secure alternatives that are easy to use and can be easily adopted with little or no training.

Another participant from the legal sector agreed that simplicity is what is key, “IT has to build a better infrastructure than what users expect so they can do their job easily. We must make it simple; if it’s not simple, they will turn to alternative services, and this poses reputational risk. We block things like Citrix, exactly because of this risk.”

What is clear is that the role of proactive and reactive varied among the sectors represented and was also dependent upon industry sector and budget. Organizations with larger budgets and higher exposure or understanding of reputational risk had the means to implement the protective IT measures and policies, whereas the IT groups with smaller budgets, or those organizations that cared less about risk, took a more reactive approach. Despite whether IT holds the proactive or reactive role, it is obvious from the roundtable discussions that CIOs and IT groups see their role as the enabler, innovating internally to try to provide their workforce with the applications they need to excel in their job.
Most software used by business was developed in the 1980s and updated in the 1990s based on the same legacy infrastructure and architecture. Today, the cloud has changed things for the better providing a more agile and flexible working environment. Cloud technology and mobile working is the future. But BYOC/M/A has brought problems for IT groups and businesses, particularly with the influx of cloud-based consumer applications and devices being used in the corporate world.

As discussions evolved around the table, it became evident that the problem is not really the devices and applications used; it’s all about the data. Whether IT holds the role of the police or the enabler, they are a ‘custodian of corporate data’ or ‘data guardian’ and will be looked to by a business to prevent/resolve a data leakage or security breach should one occur. This is where the battle for control truly lies – over the corporate data.

The ability for the CIO to be given control by their technology suppliers over their data and to be able to make decisions about their data also resonated throughout the roundtable discussions. The debate between public and private cloud deployment arose, and it was obvious that despite their preferences, the CIOs wanted the ability to be able to choose where the data was held, and even more so, the specific geographical locations for the data residency. This means that the jurisdiction under which data falls can be configured to match the requirements of their organization and IT can appease their organization’s board concerns.

It was also clear from the CIOs present that clients are becoming increasingly involved with the technology infrastructure of organizations, thus ensuring that corporate data is protected. If an organization wants business, it must adhere to the appropriate security standards and meet the expected security requirements of the client.

When looking at the workforce itself, the question of risk and how much employees really care gave a mixed bag of results. Banking and financial institutions appeared to have little appetite for risk, and this is firmly ingrained within their workflow – and culture of significant penalties for security breaches.
Other industries, for example education, also had systems in place to ensure confidential data was not leaving their network. It was clear, however, that other industries such as legal and retail, still have work to do with the notion of “just getting my work done” superseding the risk factor.

Therefore, a successful IT strategy for a CIO today must consider these key factors: Consumerization, cloud, mobility and BYOC, risk, and the control of corporate data.

The CIO must consider the following questions: Are consumer-devices and applications being used by my workforce to share corporate data, and is there a secure, sanctioned alternative for them to use? Does my workforce understand the notion of risk, and if they do not, are there systems in place to handle the risk for them? Am I fulfilling my role as ‘Data Guardian’ and winning the battle of data control?

Technology will continue to evolve, and as it evolves, IT groups will need to adapt.