What to Do about Shadow IT

By

Heather A. Smith
James D. McKeen

The IT Forum …

Is a focus group of senior IT managers from a variety of different industries convened regularly by the authors to address key management issues in IT. This report highlights a recent discussion.

– See back page for details of the IT Forum and other reports.

Introduction

Shadow IT is out of the closet and waltzing around the corporation, leaving IT departments rushing to do damage control.
(Dyche, 2012)

Shadow IT is the bane of my existence!
(an IT manager)

Technology spending is growing rapidly in organizations – but just not in IT (Materna 2017, Colony 2017). Today approximately 35% of technology spending is managed outside the IT budget by business leaders and this percentage is rising annually (Wikipedia 2018, Wilczek 2017, Fitzgerald 2016). Put another way, between 5-15% of business unit budgets are now spent directly on IT (Colony 2017, Anonymous 2015A). These funds are being used to buy a variety of technology – hardware, software, devices, and services – outside the control of IT and in many cases, without its knowledge. Known collectively as Shadow IT, it represents a growing gap between company-sanctioned IT and what employees are actually using (Ray 2016).

This gap is also a growing challenge to the roles and responsibilities of the IT function as the traditional stewards and guardians of an organization's data, technology, and IT resources. Although end user computing has existed in organizations for decades with IT's blessing, it was largely limited to sanctioned tools and used for very small scale development (Zimmerman et al. 2017, Myers et al. 2017). Today, as technology skills have become more widespread in business, and with the availability of cheap, easy to implement cloud services, access to a variety of consumer products, and the pressures of digital transformation, Shadow IT usage has grown significantly. Estimates of its actual use in business vary widely but there is general agreement that it is much larger than IT departments believe. Best guesses range from 10-30 times more than estimated (Anonymous 2015B, Overby 2016, White 2017). One study found that the average large enterprise used 11,220 individual public cloud services with IT supporting about 5% of these (Anonymous 2015B). Another found that 86% of cloud applications used by Fortune 1000 companies were unsanctioned by IT (Raymond et al. 2016).

As these numbers grow, IT is rapidly losing control of how technology is used in organizations, how much is spent on it, and its ability to protect it, and the data that resides on it. Clearly, Shadow IT is an indicator of where business wants to go, said the focus group. "It's never been easier to do," said a manager. "And it can serve as a pressure release valve with so much demand on IT these days." The question many organizations are asking as a result is, What is the best way to handle Shadow IT?

This paper explores this question beginning with the nature and scope of Shadow IT, the value it offers, and the challenges it presents. Next, it examines the range of options IT managers have for governing Shadow IT in the immediate term. Finally, it looks at some of the longer-term issues that Shadow IT poses for the relationship between IT and the business and how the role of the IT function in the organization is likely to change in the future.

What is Shadow IT?

Shadow IT is a surprisingly broad concept that encompasses a variety of IT-related expenses in organizations for anything other than the IT provided by the enterprise for work tasks, and outside of formal/informal IT policies, rules, guidelines, standards, and procedures (Haag and Eckhardt, 2017). At its most basic, Shadow IT refers to the business' use of hardware, software, systems, solutions, or services for work without the explicit approval or knowledge of IT (Materna 2017, Wikipedia 2018). Originally, the term was used to describe solutions that grew out of End User Computing tools and applications that were adapted for other purposes and had drifted out of IT's control (Zimmerman et al. 2017). "A classic example of this is users who use spreadsheets for mission critical work, including storing data", said a focus group manager. More recently, it has also come to describe the autonomous development, purchase, implementation, and use of a variety of technology by departments other than IT (Wikipedia 2018). The cost of this type of IT is usually covered by business unit budgets (Wong 2017).

However, within this generic definition there are "fifty shades of Shadow IT" according to the focus group managers, and in order to identify them it is important to know where to look. These include:

- End User Computing. This uses enterprise-approved tools and systems for development of localized solutions but their application may go well-beyond what they were originally-intended for (Zimmerman et al. 2017). For example, "One of our business units built their own data warehouse with approved tools that accounted for one-third of the demand against company database resources," said a manager. Another added, "One business unit hired summer students to work with SharePoint. It was a critical application but broke no rules. IT didn't know until real problems developed."

- Workarounds. These adapt existing work systems to circumvent constraints imposed by the original system design (e.g., utilizing a data field to gather information for something else) (Haag and Eckhardt 2017).

- Personal IT. Here, business people use personal technology developed for consumers for business purposes. This could be devices, such as smart phones or tablets, or applications (e.g., What's App or Dropbox) for communicating or sharing information (Haag and Eckhardt 2017).

- Third Party Access. Here, a business user authorizes access to a third party (such as a vendor, consultant, a contractor, or even an application) to connect to an organization's network to use a sanctioned service (Wikipedia 2018). In this way, non-sanctioned access is provided to networks, data, systems, or devices.

- Unintended Use. This can result from social pressure to use unapproved tools that others are using for communication or to share knowledge (Haag and Eckhardt 2017).

- Bricolage. This is the construction of larger-scale solutions that bypass formal systems using whatever technology is available (Zimmerman et al. 2017). "We had one application that was spun up in the cloud but when the person who created it quit, the system crashed and we had a disaster on our hands," a member said. This can also include repurposing company IT or approved personal IT for use in unexpected ways.

- Software-as-a-Service. Here, users purchase standard software from the cloud that promises them flexibility and productivity and the ability to facilitate user-driven innovation (Zimmerman 2017). "We discovered we had multiple instances of SalesForce operating in our organization," said a manager. "We only found out when we received a change request for two different versions."

Personal IT and cloud services have created new ways for employees and business units to easily circumvent internal IT (Froelich 2015, Materna 2017). In some organizations, business units have created their own IT teams to implement and support solutions in this way (Materna 2017). Some suggest that this democratization of IT is a natural evolution and that Shadow IT should be renamed "citizen development" (Girard and Driver 2016). This view holds that Shadow IT is essential for the rapid implementation of specialized, nimble, engaging, and personalized front end software. Interestingly, however, several studies show that much shadow IT is being spent on back office functions – which are typically centralized and managed by the IT department to achieve synergies and cost savings (Colony 2017, Anonymous A 2015). Some of the worst offenders in this area are: back-ups, file sharing, archiving data, storage, business productivity apps, and social media communications (Anonymous B 2015).

There is no shortage of reasons given for the existence and growth of Shadow IT. Some of the common ones include:

- Necessity. With new technologies and their applications appearing at a rapid pace, business units are under pressure to transform and innovate and IT has not responded quickly enough (Froelich 2015, Mingay 2014, Anderson 2015). "Shadow IT is a symptom of unmet needs," said a manager.

- IT processes and constraints. "Often our processes can hamper what the business units are trying to accomplish," admitted a manager. "We are perceived to have too much bureaucracy and take too long to deliver." "IT has said 'no' so often, it is often perceived as the 'business prevention group'", said another. In short, official IT is perceived as a party killer, not responsive enough, and lacking necessary tools and capabilities. This may be perception and reputation, not reality, but it affects business unit decisions (Suer 2017).

- IT's inability to relate to the business. Shadow IT can be a sign of IT's failure to collaborate with the business (Drucker 2015). Demand for IT services is growing and the centralization and consolidation of IT services tends to result in a greater decision-making gap between users and IT, leaving the business feeling that IT is out of touch with business needs (Mingay 2014). Many users feel that IT doesn't work well with them (Lowe 2015). "Our relationship management activities are not very effective with the business," one manager noted. "If it doesn't work well, users will work around IT." All of this is compounded by the fact that IT staff are overworked, busy, and sometimes too disinterested to listen to what the business is saying to them (Lowe 2015).

- Ease of use. Shadow IT is about business users solving their own problems with technology and the cloud has made it much easier for them to do this (Lowe 2015). The Consumerization of business applications has created an environment where it is easy for business users to download and configure powerful systems without the assistance of IT (Ray 2016). Vendors and consultants also influence the business in this regard, according to the focus group.

- Rising expectations. As younger, more digitally-adept workers have joined the business, workplaces have become more technically capable and more comfortable working with development tools and options from the cloud (Mingay 2014). These workers expect workplace technology to be as fast and agile as what they use at home and when it isn't, they feel their needs are not being met (Bannister 2017). For example, enterprise communication/collaboration tools are seen as particularly unsatisfactory when compared with personal ones (Mailmann et al. 2016). These rising expectations are beginning to erase the differences between business and IT skills (Colony 2017, Mingay 2014).

- Lower perceived cost and turnaround. In many cases, business units choose Shadow IT because it is perceived to cost less and take less time to implement (Wikipedia 2018, Wong 2017). Often, because IT is seen as inefficient and ineffective, business leaders may trust an external provider over IT (Drucker 2015, Settle 2016). While this belief may be untrue given the risks that IT must manage, the focus group noted that Shadow IT is often a way for business to get something done quickly. "Shadow IT grows gradually," said a manager. "It's not even seen as an application until they need IT."

Overall, Shadow IT is becoming a force to be reckoned with in organizations. While in some cases, it may be a reaction to IT problems, said the focus group, in others, it is occurring because a business is in a hurry and needs action. "Shadow IT is only going to increase as the technology gets easier," said a manager. "It will play a greater role in our organizations and this can be a good thing. However, we need to have clearer oversight of what is being done and make conscious choices about where to use it. Otherwise, it can significantly undermine what IT is trying to accomplish."

Shadow IT: Bane or Blessing?

Shadow IT pulls IT in two ways. On one hand it introduces risks and vulnerabilities into the organization which IT processes and standards are specifically designed to mitigate. On the other, it adds value and encourages innovation in the business units (Zimmerman et al. 2017). Thus, Shadow IT is both rogue IT that creates problems for the real IT organization and a way to leverage technology and create benefits. Research and the focus group were fairly equally split with regard to the risks and benefits of Shadow IT (see Table 1).

Shadow IT Risks	Shadow IT Benefits
• introduces security vulnerabilities	• adds value, especially in the short term
• inefficiencies in technology procurement	• catalyst for next generation applications and innovation
• privacy concerns, data leakage, information silos	• brings customer requirements front and center – can feed the IT pipeline
• hidden costs	• can reduce IT workloads
• disruption of organizational goals and IT's strategic roadmap	• unlocks opportunities for longer-term strategy
• single points of knowledge	• solves the little stuff, the long-tail projects
• performance, integration, and scalability issues	• faster, more effective way to improve productivity

Table 1. Shadow IT Risks and Benefits

The focus group noted that in many organizations, Shadow IT has a negative, chaotic connotation and that IT's instinct is to clamp down on it. "We have many problems with Shadow IT," said a manager. "When users do stuff on their own, we end up paying for it for a long time." Another added, "We have siloed data from many different CRM systems everywhere. We're still figuring out how to migrate them into one system. Implementing a single instance of an application takes more time than just doing different implementations in different business units." The focus group also noted the extra cost involved in having duplicate systems, adding that procurement should be an enterprise function to gain the synergies involved.

However, they also recognized the potential of Shadow IT. "It's a 'glass half-full' situation," said a member. "Innovation is happening as a result, but it needs to be better managed." Another added, "It's great for the projects that don't make the cut. These are the long-tail processes and little things that could add up to additional value for the business." Shadow IT is recognized as an important source of innovation that can create prototypes for future, approved IT solutions (Wikipedia 2018). It's also seen as a way to open up opportunities for long term strategy development and catalyze entrepreneurial talent hidden in the company, bringing customer requirements front and center (Materna 2017). When used wisely, Shadow IT can feed the corporate IT pipeline and reduce IT workloads by identifying business requirements for IT (Driver et al. 2017). A focus group manager summed up this view of Shadow IT by stating, "We shouldn't be too sensitive about Shadow IT because innovation is happening with it but at the same time, business needs to work with us to help prevent potential problems."

These problems are very real because Shadow IT introduces significant security, privacy and compliance risks to the organization. For example, Gartner estimates that by 2020 one-third of successful attacks on enterprises will be on data located in Shadow IT resources and that business units are using many more cloud services to store critical company data than CIOs were aware of or had authorized (Young 2017). And many business leaders are unaware of where their data is being stored, often violating privacy and compliance regulations (Anonymous 2016).

Data leaks and loss of data integrity are particularly significant risks. "It's taken a long time but I've finally got our executive team to see that we're a data company," said a manager. "Above all else, we need to protect our data." This can't happen when there are myriad unofficial or uncontrolled data flows happening in Excel macros, websites, cloud solutions, business intelligence apps, and personal devices (Wikipedia 2018). Duplicate data, errors in data, and information silos are major reasons why IT is concerned about Shadow IT. "We can't get value from our data if it's inaccurate or we can't integrate it," explained a manager.

One of IT's biggest concerns about Shadow IT is loss of the synergies and efficiencies that can be achieved when many aspects of IT are controlled centrally. "Many of our younger, more technically adept employees simply don't understand our business model," said a manager. Another added that there are many hidden costs involved when people do IT work without experience or consultation with IT. "It's like giving a toddler a handgun," said a manager. "It's easy to develop inconsistencies from small differences and errors from not following rigorous processes." Business units often don't understand the costs involved to IT in helping them fix the problems that develop because apps and systems can't speak to each other when the company runs multiple services with similar functionality or when there are performance issues (Loten 2016, Bannister 2017). These costs can add up, not only in terms of dollars, but also as a result of the loss of a strategic IT roadmap for the enterprise as a whole (Froelich 2015).

Shadow IT Governance

Current IT governance tends to stress adherence to standards and reducing enterprise risk over delivery speed and innovation and this "one size fits all approach" has often driven Shadow IT deeper into the shadows and hampered IT organizations in effectively supporting business-delivered technology (Klock 2017). But the focus group was clear that organizations can effectively govern Shadow IT if it is brought out into the open. "The most important aspect of governing Shadow IT is visibility," said a manager. "Then what was really rogue IT becomes business technology (BT)."

IT governance must therefore be enhanced to address and embrace Shadow IT. Organizations have different choices for doing this, depending on their industry and business model. Some, particularly global enterprises, may stress more centralized control while others may enable more coordination, collaboration, and creativity (Young 2016, Buchel and Wade 2013). In any case, having a balance of governance styles with clear but lightweight guidelines and unambiguous decision rights and responsibilities with regard to BT, will help bring Shadow IT out into the open (Zimmerman et al, 2017).

There are two overarching principles when governing Shadow IT:

1. All Shadow IT must be identified. "Everyone gets governance," said a manager. "Business units can only do Shadow IT if it's approved." To do this, many organizations take a 'carrot-and-stick' approach with the carrot being some support for business technology, a greater partnership with business, and simplified review processes (Drucker 2015, Girard and Driver 2016, Mingay 2014), and the stick being formal detection of what is being done through tools to identify undeclared technology, encrypt data, prohibit expensing of BT, internal audits, and locking down systems (Bannister 2017, Raymond et al. 2016, Mingay 2014). "We use perimeter surveillance to determine what people are connecting to," said a manager. Another added, "we have robust perimeter data defenses and people can't move data across them." As senior management has become more aware of the vulnerabilities of Shadow IT, working around traditional IT has become a more serious offence. "If you use an unapproved service, you will get fired," said a manager. "We provide ethics training to ensure that people know that they must declare the technology they want to use and get it approved."

2. All Shadow IT is subject to oversight. Providing Shadow IT with oversight does not mean banning it altogether as this would drive it further into the shadows, but it does mean embracing it the right way to protect the organization and facilitate innovation (Lowe 2015). "We need to protect the business units from themselves but not obstruct them," said a manager. As security has become more important to organizations, the protection component of Shadow IT governance has become stronger. "We've progressively locked things down. We've identified our core systems and no one's allowed to touch them," said a manager. "Business can't connect with data unless it's masked," said another. "And we've banned USB sticks." Governance is not only essential to enable an organization to determine

the right mix of standard and non-standard processes and systems but also to provide for movement between these two categories as strategies evolve (Bucher and Wade 2013). Here, many focus group organizations offer light reviews for using BT. "An architecture review is not optional because it forces a dialogue," one manager stated. "However, we keep the process very simple and provide frameworks for business to self-manage to ensure consistency." By getting IT involved through partnerships and touch points, organizations can ensure they have compatible technology that is consistent with their architecture.

The focus group stressed that Shadow IT is not going to go away, with or without governance but that without governance it is dangerous. "Governance should be a partnership," said one manager. "We have less Shadow IT now because we have established joint accountability for business technology." "The key is balance," said another. Most large organizations will likely have pockets of local autonomy within a larger context of centralized systems. However, it is important to strategically define where the organization should be and to design governance for this goal. The trick for leaders is figuring out where individual processes and systems should be (Bucher and Wade 2013).

"We should assume some Shadow IT is necessary and do it right," said a manager. What would this look like? Suggestions range from more to less restrictive:

- Tightly control data access and what can be done with it (Anonymous 2016). "We've created 'sandboxes' of masked data for users to use for experiments but these are not connected to anything else," said a manager. "We've created a castle keep around our data," said another. "Our data is locked and monitored," said a third.

- Provide choice within guidelines. "Whitelist" applications and tools that can be used; "blacklist" those that cannot (Girard and Driver 2016). Create an approved list of vendors and suppliers (Mingay 2014) and set up a virtual corporate marketplace of approved technology, that triggers deployment on request, and keeps track of what's happening. Continuously enhance this so a business unit is not tempted to be "unfaithful" (Wilczek 2017).

- Define clear accountabilities for both business and IT to create value and reduce risk (Mingay 2014). "We now have joint accountabilities and our users understand that it's not okay to just throw stuff into our network," a manager noted.

- Update policies and guidelines for Shadow IT, where it can be used and where IT needs to be involved (Anonymous 2016). Establish guiderails and touch points to manage and direct Shadow IT (Overby 2016A). "We need better up-front expectations," said a manager. Include Shadow IT in event, incident, problem, request management, and performance metrics (Overby 2016A).

- Educate all employees about what is expected of them with regard to Shadow IT and ensure they understand its implications for the enterprise (Ray 2016, White 2016). "Our people are educated on privacy and security every year so they now care more about them," said a manager.

- Maintain ongoing communication with business units to ensure their needs are listened to and addressed (Zimmerman et al. 2017). Seek "win-wins" that also embody good corporate citizenship (Wilczek 2017).

- Transform Shadow IT into citizen development programs that are fostered and managed by IT (Wong 2017). "We've created a registry of business-managed applications," said a manager. "We allow them to take innovation to a point and then put it into the queue for more professional development," said another. "We've created simple checklists which the business can use to determine where and how they can use technology," a third added.

- Assign IT resources to help Shadow IT projects work within IT guidelines, standards and policies and for advice and consulting for solution acquisition and development initiatives (Lowe 2015, Mingay 2014). Create a community of practice within IT specializing in this work (Fitzgerald 2015). One IT organization offered to look at business users' spreadsheets and identify broken links and errors. "When we did this and they saw all the problems, they were shocked!," said a manager.

- Decompose IT service offerings so that business users can draw on those services they find most valuable e.g., requirements specification; project management; solution development; vendor relationship management; and application hosting (Mingay 2014).

Leveraging Shadow IT

Although it must be governed, Shadow IT represents more than a few frustrated business users and an irritation to IT. In fact, it is a symptom of a much larger social and organizational change where technology is osmosing outwards from IT and changing the dividing line between business and IT (Fitzgerald 2016). This means that IT's operating model must change as well (Mingay and Cox 2017, Howard and Struckman 2018). "Shadow IT is a reality check on how we're doing in IT," said a manager. "It is the canary in the coal mine. The world isn't standing still and we cannot expect business as usual." There is broad consensus that in the longer-term Shadow IT will force IT to change to better address business needs and think differently about what value IT brings to the organization (Froelich 2015, Anderson 2015). Whether they like it or not (and many IT professionals do not), IT is not going to be able to completely control the use of technology in the organization (Loten 2016). "We have to accept Shadow IT as a necessary evil or IT will be out of business," said a manager.

IT therefore needs a new vision for itself that will embrace Shadow IT as an important element of digital transformation and an extension of IT capabilities (Bannister 2017, Wong et al. 2018). Embracing Shadow IT should mean shifting power partially away from centralized IT and towards more appropriate autonomy for business (Driver et al. 2017). However, it is also a disintermediation of IT's traditional roles and responsibilities (Settle 2016). The focus group identified four ways that IT must change to integrate and leverage Shadow IT appropriately:

1. IT must partner more effectively with business on business technology initiatives. "This is a real opportunity for IT and the business to speed up delivery," said a manager. It is also an way for IT to take advantage of the business' skills and specialized knowledge to create more innovative and relevant technology (Wong et al. 2018). "In this way we can support a culture of innovation and experimentation, getting involved up front, and helping to percolate value up into the rest of the organization," said a manager. "If we're at the table we can let them go ahead and when the time is right make the business case for consolidation to the 'mother ship'." Taking a more consultative approach to Shadow IT will help organizations avoid its pitfalls and increase the quality of its results (Wong et al. 2018, Driver et al. 2017).

2. IT needs a new mandate. This new role as a consultant, advisor, and partner to the business should come within the context of an environment which IT must develop to support, facilitate, measure, govern, and guide Shadow IT work. In this environment, IT will more closely link IT and BT together treating them as one comprehensive set of capabilities that provides a full range of value and also better facilitates easier transitions of applications between business and traditional IT (Colony 2017). "The business has always asked IT for help when its technology grows too complex for it to handle," said a manager. "In the future, we must create an ecosystem of tools and services that will enable us to scale an application if it becomes more broadly useful in the organization or if it becomes mission critical."

   Increasingly, as well, IT will need to provide specialized technology services to the rest of the organization through libraries of approved APIs, security testing and development tools, assistance with vendor evaluation and selection, contract negotiations and renewals, and establishing internal and external SLAs. IT will continue to act as data stewards, set policy, and provide the deep architectural and technical knowledge that will integrate applications and prevent security gaps and maintain and develop large, centralized back office applications. However these will be reoriented to better serve as a background and staging platform for business technology and facilitating connecting back office systems and data with customer-facing programs (Wong et al. 2017, Colony 2017).

3. IT needs new skills. Clearly, if IT is going to succeed in transforming itself to better leverage Shadow IT, it will need new skills to support it. And many of these new skills will need to be mirrored in the business as well. To achieve this, IT must support formal training programs for both its own and business staff to develop advanced digital skills and create hybrid career paths that combine business and IT skills (Wong et al. 2018). Identifying the right people in both business and IT and developing them will help the organization truly leverage their skill sets (Driver et al. 2017). At the same time, IT needs to improve its consulting skills, said the focus group, in order to enable it to undertake its new partnering roles. It will also need to develop specialized skills in any services that IT offers to the business to facilitate BT, particularly those for managing vendors, data stewardship and protection, agile development and devops, and supporting prototype development and experimentation. In turn, it will likely cede expertise in user experience, data analytics, analytics tools, and use of highly specialized hardware and software to the business community (Wong et al. 2018).

4. IT needs to devote resources to BT. Clearly, none of these changes can happen unless IT devotes resources to making them happen (Driver et al. 2017). This is not an area in which the focus group had any advice or recommendations and resources will only be assigned if IT and business leaders can create a compelling case for them. Embracing and leveraging Shadow IT requires the thoughtful and intentional transformation of both IT and BT functions but it will not get far without resources and senior management support. As is often the case, it will likely be up to the CIO to take the first steps in this area and gain the support of the company leadership team.

Conclusion

Shadow IT here to stay and it is directly challenging IT on many levels. Not only do today's business users have the skills to undertake larger and more complex technology projects than ever before, they are expressing their lack of confidence in IT's responsiveness by voting with their credit cards. Although IT organizations have legitimate concerns about security, privacy, and general technology chaos, too many of them react to the discovery of Shadow IT by trying to stamp it out or inhibit it in any way they can without regard to the value it brings to the organization or how IT can leverage it. This paper has shown that the growth of Shadow IT is really a symptom of how organizations and technology are changing. As technology gets easier and cheaper to implement, it has suggested that IT leaders should take a more thoughtful and strategic approach to all forms of IT work – one that envisions much broader and less doctrinaire mechanisms for delivering technology to the organization in true partnership with the business.

References

Aller, R. and H. Weiner. "Finding, fixing, and foiling shadow IT problems", CAP Today, April 2016.

Anderson, M. "Embracing shadow IT", Database Trends and Applications, V.29, N. 3, Jun/Jul 2015.

Anonymous. "IT lurks in the shadows: 20% spend increase in 2015", Progressive Digital Media Technology Review, 27 March 2015A.

Anonymous. "Five of the worst shadow IT offenders", Progressive Digital Media Technology News, December 2015B.

Anonymous . "Cisco takes on shadow IT for about $1 a head", Health Management Technology, V. 37, N. 2, March 2016.

Bannister, J. "How to harness the power of shadow IT", CIO, August 15, 2017.

Buchel B. and M. Wade. "Anchored agility: the holy grail of competitiveness", IMD Perspective for Managers, N. 186, June 2013, www.imd.org/pfm.

Colony, G. "CIOs and the future of IT", MIT Sloan Management Review, 2017, Reprint #59215.

Drucker, P. "IT in the shadows: why shadow IT is a concern (and how to address it)", June 9, 2015, https:/www.thinkhdi.com/library/supportworld/2015/shadow-it-itsm.aspx, downloaded March 23, 2018.

Dyche, J. "Shadow IT is out of the closet", Harvard Business Review, September 13, 2012.

Driver, M., V. Baker, J. Wong. "Citizen development success depends on an equal partnership between business and IT leaders", Gartner Research G00332405, 13 October 2017.

Fitzgerald, D. "How the PMO can make the best of shadow IT", Gartner Research G00318343, 30 November 2016.

Froehlich, A. "Shadow IT: 8 ways to cope", Information Week, March 3, 2018.

Girard, J. and M. Driver. "Good citizen IT app development security depends on good IT citizenship", Gartner Research G00301708, March 29, 2016.

Haag, S. and A. Eckhardt. "Shadow IT", Business and Information Systems Engineering, V. 59, N. 6, 2017.

Howard, C. and C. Struckan. "2018 CIO agenda: a U.S. perspective", Gartner Research G00346758, 09 March 2018.

Klock, C. "Build an agility-based commerce release practice to deliver business outcomes", Gartner Research G00337889, 04 October 2017.

Loten, A, "Business news: Egnyte tackles shadow IT", Wall Street Journal, October 5, 2016.

Lowe, S. "Don't fear Shadow IT – exploit it and prosper", Inforworld, September 28, 2015.

Mailmann, G., G, Macada, A. Carlos, and M. Oliveira. "Can shadow IT facilitate knowledge sharing in organization? An exploratory study", European Conference on Knowledge Management, September 2016.

Materna, J. "What's next for enterprise security?", CSO Online, December 5, 2017.

Mingay, S. "Embracing and creating value from shadow IT", Gartner Research G00264121, 09 May 2014.

Mingay, S. and I. Cox. "Why traditional I&T operating models are under stress and how to plan a response", Gartner Research G00331732, 24 August 2017.

Myers, N., M. Starliper, S. Summers, and D. Wood. "The impact of shadow IT systems on perceived information credibility and managerial decision making", Accounting Horizons, V. 31, N. 3., September 2017.

Overby, S."Fo ur ways to apply SLAs to shadow IT", CIO, April 20, 2016.

Ray, D."Managing risk in light of shadow IT", Inside Counsel, November 14, 2016.

Settle, M. "The world turned upside down: conventional IT is rapidly becoming shadow IT", CIO, July 19, 2016.

Suer, M. "Is shadow IT something CIOs should worry about?", CIO, June 6, 2017.

White, J. "Your IT spend is 50 percent more than you think", Government Procurement, V. 25, N. 4, Aug/Sept 2017.

White, S. "Empower your employees by embracing shadow IT", CIO, September 13, 2016.

Wilczek, M. "Headache for the CIO: shadow IT is soaring as LoBs seek greater autonomy", CIO, July 24, 2017.

Wikipedia. "Shadow IT", https://en.wikipedia.org/wiki/Shadow IT, downloaded March 23, 2018.

Wong, J. "Survey analysis: citizen development is happening and IT needs to be more engaged", Gartner Research G00324372, 28 September 2017.

Wong, J, M. Cain, C. Idoine, B. Zakheim. "Cultivate citizen X practices to maximize digital dexterity", Gartner Research G00348654, 15 March 2018.

Young, C. "The built-to-purpose IT organization", Gartner Research G00307927, 26 April 2016.

Young, G. "How to respond to the 2018 threat landscape", Gartner Research G00335145, 28 November 2017.

Zimmermann, S. and C. Rentrop. "A multiple case study on the nature and management of shadow information technology", Journal of Information Systems, V. 31, N. 1, Spring 2017.

Concept

The purpose is to bring senior IT managers together to examine topics that are of critical concern to them and their organizations. Via the Forum, members share experiences, learn from their peers, establish valuable networks, and develop practical strategies for creating, implementing, and managing IT solutions.

Recent Papers

- Innovation with Technology
- Emerging Technology Management
- Developing a Data Strategy
- Developing a Cloud Strategy
- IT in 2020
- Transforming to Dev-Ops
- Developing Thought Leaders in IT
- IT's Role in a Culture of Experimentation
- Managing Disruption in IT
- Balancing Information Security and Enablement
- Artificial Intelligence
- Moving Towards an API Economy
- Developing New IT Talent Management Capabilities

Participating Organizations

- Bell Canada
- BMO Financial Group
- Canadian Tire
- CIBC
- Empire Financial Group
- LCBO
- OLG
- Ontario Teachers Pension Plan
- Ontario Universities' Application Centre
- Reliance Home Comfort
- Sun Life

Membership

Membership in the IT Forum is by invitation only. The annual fee is $3,000. Please direct inquiries to Dr. James McKeen at jmckeen@business.queensu.ca.