FUJITSU

White paper
Spotting Shadow IT

Cloud and mobile computing make it easier than ever for organizations to turn IT services on and off as needed. But these services are easy for individuals to use, too. And, increasingly, people are using such applications at work – with or without their employers' knowledge.

Introduction

Cloud and mobile computing make it easier than ever for organisations to turn IT services on and off as needed. But these services are easy for individuals to use, too. And, increasingly, people are using such applications at work – with or without their employers' knowledge.

Shadow IT – the ad hoc and unauthorised use of IT services for work – creates significant potential risks for enterprises. However, it can also boost collaboration, creativity and innovation among users, which benefits their companies in many ways.

For better or for worse, the use of shadow IT in the workplace is growing steadily. Analyst firm Gartner, for example, predicts shadow IT could account for up to 30 per cent of IT operations activity in 2016. That represents a sizeable use of resources that might be going mostly or even completely undetected in the average enterprise.

So how can a company spot shadow IT in action, and reap the benefits while minimizing exposure to the risks? Every business is different. But, in most cases, it's not wise – or even possible – to put an across-the-board stop to such uses. Instead, Fujitsu recommends that enterprises take steps first to detect and measure the use of unapproved IT services at work. After that, companies should work to standardize and manage the deployment of such services, ensuring that employees have the tools they find most useful without opening up their organizations to security and privacy problems.

This approach requires the right mix of technologies, capabilities and experience but – done right – it can help enterprises tap the good of shadow IT and avoid the bad. Fujitsu has helped many organizations achieve these goals and can help yours do the same.

Pros and cons

Shadow IT can pose tremendous risks to an organization for a number of reasons. One, as we can see from the above figure by Gartner, is that applications and services deployed without the control and oversight of the IT function can drain budgetary resources that would otherwise be available to the IT department. For instance, if another part of the business acts independently to equip employees with iPads, that could mean less total budget under IT's control. It can also hurt the department's ability to deliver necessary software updates, data back-ups, archiving and other services across the organization.

Keeping systems and data secure is a particular challenge. Uncontrolled use of unauthorized devices, apps and services can lead to unevenly managed – or even non-existent – security controls. That can do more than increase the potential for costly and/or damaging data breaches and losses. In highly regulated industries such as finance or pharmaceuticals, security lapses or inadequate data controls can lead to heavy fines and even criminal penalties.

This is a special concern in Europe, where new requirements are expected to come into force over the next couple of years following the adoption of the EU General Data Protection Regulation. The EU GDPR will introduce much stiffer sanctions for improper data handling of up to 4 per cent of an organisation's worldwide turnover. For some companies, this could mean fines of many millions of dollars.

With this risk looming, it is little wonder that – to some CIOs – shadow IT constitutes a continual source of risk and expense that must be stamped out at all costs.

However, other business leaders take the exact opposite view. To them, improvised, unofficial and on-the-fly applications and services are the means by which employees can communicate with one another more effectively and work together more creatively and successfully. Some, in fact, even offer prizes and awards for the best uses of shadow IT.

Key issues to consider

How can organizations find a balance between these two widely diverging viewpoints? Much will depend upon the individual company's unique needs and culture, including its desire for innovation and overall appetite for risk. However, whatever level of shadow IT an enterprise is willing to accept, two things are certain: eliminating it completely is all but impossible; and allowing a free-for-all environment where anything goes is also out of the question.

The key is finding a way to standardize use of shadow IT as much as possible to tap into its benefits while eliminating risks. To achieve that goal, the first thing an organization must do is get a picture of what kinds of shadow IT are being used.

These can include anything from personal consumer devices such as smartphones and tablets to individual or departmental use of cloud-based resources, whether those are Facebook®, LinkedIn® and Slack®, or Box, various Google® apps and Salesforce.com®, or indeed any of thousands of less-well-known cloud services. Shadow IT can also include the use of advanced tech offerings from providers like Amazon® Web Services. In fact, one AWS executive remarked in 2014 that the company's growth stemmed in part from teams who "could start using AWS with just a credit card and they would actually get projects done when they wanted to get done... and then show the results to their leaders, their CTO and CIO and say, 'Look we should do more of this.'"

Once an organization has succeeded in taking an enterprise-wide inventory of who's using what, it should then launch a conversation with employees about why they're choosing these tools and what the perceived benefits (as well as drawbacks) are. From here, a business can make decisions about which types of shadow IT are acceptable and under what circumstances. For example, if most employees prefer to use OneDrive for data storage, a company can designate that as an acceptable option over other storage providers such as Box or Dropbox.

"Very few [organizations] have a strategic vision where the business benefits of consumerization are thoroughly analyzed and implemented in a methodical and synergistic way across business units," Gartner observed in a 2015 look at the digital workplace. "Making computing resources more accessible in ways that match employees' preferences will foster engagement by providing feelings of empowerment and ownership."

Armed with such guidelines, managers can follow up with internal communications to share these new shadow IT dos and don'ts with employees. Education is a vital part of effective shadow IT management. Successful management will also require continued monitoring and communication to make sure those guidelines stay relevant and effective.

Fortunately for enterprise customers, an ever-growing number of tools and technologies are making this easier to do. Mobile device management systems, for example, allow employees to use personal smartphones for work while also ensuring a company can retain control over business-related data and functions on those devices. These systems can, say, allow the IT department to remotely lock access and/or wipe sensitive information if a device is lost or stolen.

Other technologies such as Microsoft® SharePoint® or IQProtector® from Secure Islands (acquired by Microsoft last year) can track and manage business data – and even embed security into documents – no matter where it's stored or how it's shared, making it easier for enterprises to keep information secure and stay in compliance with regulatory data requirements.

Whatever approach a company chooses to take, it's important to ensure that the IT department acts as an enabler, rather than a barrier, for effective technology use. One of the main reasons employees turn to shadow IT solutions in the first place is because they view the IT team as more of a hindrance than a help when it comes to getting things done. Business leaders need to make sure this isn't the case.

Fujitsu's approach

Here at Fujitsu, we not only understand the importance of managing shadow IT effectively but have the expertise and ability to help our customers spot and identify it in all its many possible manifestations. Our aim is to enable enterprises to understand the big picture of shadow IT in their particular organisations, help them assess their preferred levels of risk and innovation, and then guide them in the process of standardising and managing shadow IT use for optimal business results. The ultimate goal is to help companies prevent (as much as possible) 'bad' uses of shadow IT while allowing them to reap the benefits of 'good' shadow IT. We view this as the difference between 'rogue IT' and 'digital enablement'.

For customers seeking to get a handle on all the different devices and services employees might be using, we can start with real-time monitoring of an organisation's web traffic. The data generated helps to spot shadow IT in action, pointing to where it's being used the most and how. This information also allows us to identify where the greatest problem areas are – including areas of potential data loss, security risks and compliance failures.

From there, Fujitsu can help enterprises by making recommendations about the best ways to monitor, manage and standardize uses of shadow IT across the organization. We can also help them implement encryption, tokenisation and other strategies to ensure that sensitive data is protected and secure across all devices and platforms.

Our new Cloud Services Management offering, for example, provides users with a way to integrate and unify control over a wide variety of IT environments across different departments and work units. It's a Hybrid IT-driven approach that enables customers to choose the solutions that work best for them – whether those are based in a legacy environment, a private cloud or the public cloud – while maintaining control of all services and expenditures from a single, easy-to-use platform.

Such a Hybrid IT approach, Gartner says, "separates the risk-averse and 'slow' methods of traditional IT from the fast-paced demands of digital business, which is underpinned by the digital workplace. This dual mode of operation is essential to satisfy the ever-increasing demands of digitally savvy business units and employees, while ensuring that critical IT infrastructure and services remain stable and uncompromised."

Shadow IT in action

It's not hard to find examples of shadow IT in action these days, from Democratic presidential candidate Hillary Clinton's controversial use of a private email service while she was US Secretary of State to the widespread use of services such as Google Drive and Skype or shared USB sticks and other technologies in the workplace. And, across the board, these examples illustrate how organizations need to remain flexible and adaptable in the face of changing technologies and practices in the workplace.

Just a few years ago, for instance, pharmaceutical giant GlaxoSmithKline tried to control the growing use of personal mobile devices in the workplace by enacting a ban on phones with cameras. Before long, however, camera-equipped smartphones had become the market standard, forcing the company to rethink its approach.

Other enterprises have learned similar lessons. GE's CTO has compared attempts at preventing shadow IT to playing a game of Whack-a-Mole. And the CTO at loyalty program provider Aimia has concluded that banning unauthorized devices and services only helps to "drive it underground".

Fujitsu recognizes this reality: our IT experience and expertise has demonstrated to us that a ban on shadow IT is essentially a ban on innovation. Instead, we believe the best approach for any organization concerned about shadow IT is to place it in the correct framework so employees can use the devices and technologies they find most useful in a safe, secure and managed way.

Conclusion

Employees typically don't adopt unofficial devices and services to make life difficult for their employers. Instead, they turn to shadow IT when they don't readily find the support they need via authorised solutions from the IT department – or simply because they discover a quicker and easier way to handle certain tasks and projects. Rather than trying to prevent such creativity, enterprises need to understand the hows and whys of shadow IT and then work to manage those uses as effectively as possible.

Fujitsu understands both the risks and benefits of shadow IT, and can help your organization find a solution that works for you.

Next steps

We can help you better understand the state of shadow IT use in your organization and find ways to standardize and optimize those uses for your company's benefit. Contact Fujitsu to learn more about our cloud-based, Hybrid IT and consulting services solutions for managing devices and applications across your business.

For more information about Fujitsu and its recommendations for shadow IT management, please contact us at: AskFujitsu@us.fujitsu.com.

Contact
FUJITSU AMERICA, INC.
Address: 1250 East Arques Avenue Sunnyvale, CA 94085-3470, U.S.A.
Telephone: 800 831 3183 or 408 746 6000
Website: www.fujitsu.com/us
Contact Form: http://us.fujitsu.com/contact
Have a question? Email us at: AskFujitsu@us.fujitsu.com

Fujitsu, the Fujitsu logo, K5 and "shaping tomorrow with you" are trademarks or registered trademarks of Fujitsu Limited in the United States and other countries. Facebook is a trademark or registered trademark of Facebook, Inc. in the United States and other countries. LinkedIn is a trademark or registered trademark of LinkedIn Corporation in the United States and other countries. Google is a trademark or registered trademark of Google Inc. in the United States and other countries. Salesforce.com is a trademark or registered trademark of salesforce.com, inc. in the United States and other countries. Amazon is a trademark or registered trademark of Amazon.com, Inc. in the United States and other countries. Microsoft, Slack, SharePoint and IQProtector are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries. NetApp and the NetApp logo are trademarks or registered trademarks of NetApp, Inc. in the United States and other countries. BROCADE and the Brocade logo are trademarks or a registered trademarks of Brocade Communications Systems, Inc. in the United States and/or in other countries. VMware and the VMware logo are trademarks or registered trademarks of Vmware, Inc. in the United States and other countries. Intel and Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. All other trademarks referenced herein are the property of their respective owners.

The statements provided herein are for informational purposes only and may be amended or altered by Fujitsu America, Inc. without notice or liability. Product description data represents Fujitsu design objectives and is provided for comparative purposes; actual results may vary based on a variety of factors. Specifications are subject to change without notice.

Copyright© 2016 Fujitsu America, Inc.
All rights reserved.