VIEW POINT

SHADOW IT - THE BIGGER CHALLENGE FOR ENTERPRISES

Abstract

Shadow IT is becoming a growing problem for enterprises and possess huge security risks. This POV talks about Shadow IT, its causes risks and possible mitigation steps to remediate it.

Infosys®
Navigate your next

Shadow IT – A growing problem

Since the advent of digital era, Shadow IT or to say unapproved / unauthorized use of software, hardware such as tools, applications, devices, or services are growing. In almost all the cases, these assets are not formally supported by the IT department or provisioned without IT department's knowledge. Problems grew many folds during Covid-19 era where change of workplace happened and nearly 100% of IT workforce started working remotely. Due to limitations at the IT department's end, Shadow IT could not be well controlled by enterprises.

Employee's convenience, improved balance between personal & official work, speed & agility, led the IT workforce to use software and hardware as per their choices.

- Uses of external cloud storage, drives, personal accounts for official data storages are easily accessible from multiple devices
- Use of social media platforms for collaboration and messaging
- Personal mail ids for official communications & data sharing due to better features compared to official channel of communication
- Usage of own preferred software / hardware than company provided
- Tedious processes, documentation & self-declarations, prior costing & budgeting etc. related to software / hardware provisioning
- Stringent sprints, delivery timelines which promote shortcuts
- Misinterpretation of BYOD (Bring Your Own Devices) which gives impression of ownership of official data, source codes belongingness to the employees
- Organization limitations to support pervasive computing & distributed teams' working culture
- Better features, easy to use, or social branding of unofficial platforms, open sources
- In Agile DevOps environments, developers find themselves disconnected from IT departments which is perceived as inflexible

External Document © 2023 Infosys Limited

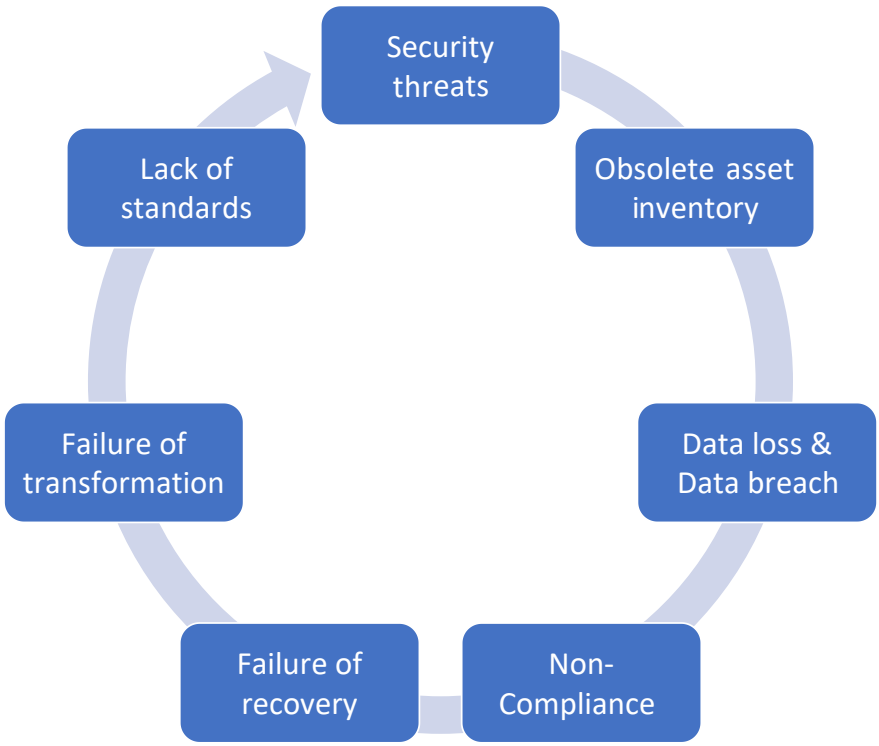
Shadow IT – Security threat to the organization

Shadow IT places the enterprises at risk due to non-compliance, security policy violations, data breaches or potential liabilities. BYOD policy not only usage of personal devices, smartphones, laptops but also open many loopholes. Every enterprise is not able to properly ring fence its environment from Shadow IT, thereby, resulting in data transmitting through external storage devices (hard disks, USB drives) or cloud storage using personal id.

Risks of Shadow IT

Shadow IT possess many risks for enterprises related to security threats, data breaches and non-compliance.

- **Empowerment at the cost of security:** Self-procurement, self-provisioning brings decentralization, enables agility and faster provisioning in any enterprises. It embraces empowerment culture which every employee expects, but it comes at the cost of compromising security.
- **Unapproved / unauthorized IT increases the threat landscape:** Due to lack of security and awareness in the IT department, this possesses serious vulnerabilities and increases the threat landscape. This leads to, Shadow IT assets becoming soft targets for hackers. The typical security solutions such as scanning, SAST, DAST, SIEM don't cover the Shadow IT assets.
  In a Shadow IT environment where official data resides, it is possible that any malicious application may also be installed which may easily access the data shared by employee. Since these assets, tools are undetected, uncontrolled or unprotected by IT team, it is noticed when damage or loss is done, making it irreversible. As it is "no one's land", IT team also cannot impose identity governance and access management. Shadow IT not only put enterprises at risk but also third parties such as vendors, partners, suppliers. Its vice versa is also true.
- **Obsolete configuration management database (CMDB):** The number of assets in the enterprises, license software usages controls etc. go for a toss. Due to uncontrolled, unauthorized software / hardware provisioning, It becomes impossible for creating such inventory (CMDB) or updating it. Since these assets are not listed under inventory, hence they miss security patches, upgrades and zero day vulnerability advisories. This will cost an enterprise heavily during a data breach/ cyber-attack, as detection and isolation of owner becomes extremely difficult.
- **Data sharing leading to data loss & data breach:** Unauthorized data transfer and confidential sharing of confidential document, source code leads to data breaches. Data remains unclassified, unprotected at outside network and does not expel when an employee leaves the organization.



Shadow IT Risks

External Document © 2023 Infosys Limited

- **Non-compliance:** Unauthorized use of applications, software, hardware possesses risks of non-compliance related to licenses and IP violations. It is also risky in terms of meeting the compliance imposed by various countries, regions, regulations, or even respective enterprises. For example, compliance such as General Data Protection Regulation (GDPR) requires a pre-defined way of handling personal data which Shadow IT does not provide. There are other compliances such as Payment Card Industry Data Security Standard (PCI DSS) or Health Insurance Portability & Accountability Act (HIPAA) etc. which become impossible to adhere or brings under audit purview when enterprises do not have control on data flow storages. While non-compliances are due to the employees who violated it, for any legal actions, penalties or overall obligations, respective enterprises will be held accountable.
- **Disaster recover, backup continuity and planning:** As Shadow IT does not guarantee a single source or destination of data stores, it becomes difficult to recover or restore the data in case of loss. Even after restorations, it does not guarantee that data is up to date.
- **Future transformation becomes difficult:** As multiple & redundant tools exist in the IT organizations with lack of ownership, it becomes difficult to plan & implement any transformation program. In such cases End of Life (EOL), End of Support (EOS) may be found deployed in productions & in use, where upgrades, patches are not available. As ownership of these apps, tools and implications of its downtime could not be established, such environment is kept out of transformation projects. Hence these apps remain in the environment with known risks and create roadblocks for fully committing the transformation programs.
- **Roadblock for standardization:** Any enterprise-wide standardization exercise such as tools consolidation, standard policy enforcement becomes difficult due to existence of diverse & redundant tools. It costs time & money to enterprises for such tool's replacement, upgradation, renew or making purchase "official".

External D © 2023 Infosys Limited

The flip side of Shadow IT

Shadow IT is also viewed as a"globally accepted" norm in some cases. In most of the cases, employees unknowingly engage in Shadow IT practice

- Shadow IT is also seen as a cost-effective measures by some enterprises as it does not increase the cost for software purchase or IT support staff, administrative work
- In some cases managers approve such practices to meet the deadlines
- In some enterprises publicly available social media platform is well accepted as the alternate communication medium is not well defined
- This culture is widely promoted across startups where companies are concerned about the result than how it is achieved
- Employees are also invited to use social media groups for employee engagements which slowly turns into the official platform for sharing all information including project challenges, achievements, or business sensitive data
- With the of new tools, technologies and open-source, IT departments are struggling to keep the inventory latest and updated which is leading to employees searching for better tools in open market
- Partner, client, or colleagues preferred tools are adopted without any ill intentions for easy commutations & collaboration

There may be many reasons and short-term advantages but in long-term, damages & liabilities of such practices are much costlier than the benefits it offers.

External Document © 2023 Infosys Limited

Measures to tap Shadow IT

Shadow IT needs a holistic approach which covers all dimensions of people, process, and technologies.

People:

- Security awareness training to employees, through gamification / quizzes
- Educating employees about the IT usage policies and associated risks of bypassing it
- Adopting employee friendly approach while defining the IT usage policies, making them partners in IT decision making or engaging with them to find amicable solutions.
- Making employees vigilant for Shadow IT detections or unauthorized provisioning
- Enterprises should also demonstrate tolerance for failure so that employees are not adopting shortcuts due under work pressure
- Two-way (IT & employees) communications to understand the employee needs and keep revising the whitelisted / blacklisted software / hardware

Process:

- Strategies & planning to handle Shadow IT, making collective goals and employee's centric policies.
- Policies & process to be aligned with each department's needs
- Self-declarations & regularization is required periodically for Shadow IT. Analyzing tools benefits, cost benefit analysis, feature comparisons, assessing wider usage needs and, associated risks should be key factors to regularize any blacklisted tools.
- Making IT governance, provisioning & procurement process more agile & flexible.
- Better synergy between employee & IT to identify the exceptions. IT provision processes to be revisited to regularize the approved exceptions. Policies to be evolved and improvised as per growing business needs and changing IT environment.
- Faster discovery and management of Shadow IT assets
- Policies related to social media usages or external data transfers
- Regular audits & compliance assurance
- Managing and mitigating Shadow IT risks. Instead of adopting common strategies for all the risks, specific strategy is required for each risk. Employees need to be aware about the risk exposures, mitigation stargates and subsequent remediation process.

Technology:

- Providing alternate official platforms for most common Shadow IT areas such as cloud storages, communications
- Tools for Shadow IT detection, visibility, and centralized controls
- Tools for threat detection and response
- Logging and audit trails to monitor unapproved provisioning. Unplanned, non-budged cost bookings, invoicing, billing also highlights Shadow IT
- Since cloud storage is more prevalent as part of Shadow IT, solutions like cloud asset security broker (CASB) must be implemented which will enable organizations to establish secure connections, access control policies, (authentication, authorization single sign-on), device profiling data encryption etc.

External Document © 2023 Infosys Limited

External Document © 2023 Infosys Limited

Conclusion

Shadow IT is outside the IT security boundaries, hence it is most prone to enterprises. Due to lack of visibility of many unknown in the environment, risk exposure is very high and threat landscape is very wide. Shadow IT cannot be fully eliminated but certainly can be controlled by taking holistic approach. Enterprise needs to look into effective measures such as tailoring policies, promoting whitelisted open sources / tools adoptions, or providing better enviornment such as collaboration platforms, cloud storage etc. Enterprises also need to make employees their partner to overcome Shadow IT challenges.

About the Author

Manish Pandey

Delivery Manager

Manish has over 24 years of experience in consulting, solution & product management, IT services & large programs management. He has been working with Infosys for more than 16 years. Manish holds degree of Master of Computer Applications. He is a Purdue University USA CyberSecurity specialist, certified Scrum Master, and certified in several areas by EnerDynamics Corp. (USA). He heads Infosys CyberSecurity delivery for Europe, ANZ & APAC regions. He is passionate about writing and has published / presented 50+ papers / articles / blogs in various forums. He actively promotes diversity, corporate social responsibilities and employee engagements.

References:

https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs

For more information, contact askus@infosys.com

Infosys®
Navigate your next

© 2023 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.