Courtesy of
MST Insurance Solutions, Inc.

CYBERRISKS&LIABILITIES

Shadow IT: Exploring Benefits, Risks and Management Approaches

In today’s fast-paced digital world, employees are increasingly turning to tools and technologies outside the purview of their organization’s IT department. They may use personal devices to access corporate records, personal cloud storage to share files or unapproved software to streamline workflows. While these actions are not usually malicious, using unsanctioned IT tools—commonly referred to as Shadow IT—can introduce significant risks to organizations, especially as it pertains to data security, regulatory compliance and operational integrity.

The shift toward remote and hybrid work models and the rapid adoption of cloud-based software have further accelerated the growth of Shadow IT. Specifically, unsupervised remote work environments can make it easier for employees to adopt tools that bypass security protocols. Meanwhile, cloud-based applications, often affordable and easy to deploy, appeal to employees looking for faster alternatives to standard corporate systems. This combination of autonomy and accessibility has created the ideal conditions for Shadow IT to proliferate, often without the IT team’s awareness or oversight.

This article explores the benefits of Shadow IT, examines its risks and downsides, and outlines strategies organizations can use to manage Shadow IT risks.

What Is Shadow IT?

Shadow IT describes the unsanctioned use of information technology (IT) systems, services or devices within an organization without the explicit approval, oversight or support of the official IT department. Examples include the use of personal email or cloud storage for work files, unapproved software-as-a-service (SaaS) applications, personal devices used for corporate access, and unauthorized messaging and collaboration tools. One evolving component of Shadow IT is the unauthorized use of artificial intelligence (AI) tools, known as Shadow AI.

Both Shadow IT and Shadow AI occur for numerous reasons, particularly employees’ desire for tools that help them work faster, collaborate more effectively or automate routine tasks. Moreover, many unsanctioned apps are modern and intuitive, and may be more appealing than existing enterprise software, particularly when legacy systems lack the features or flexibility employees desire. Compounding the issue, cumbersome internal processes may prevent employees from quickly and efficiently requesting new applications or services through official channels, prompting them to take matters into their own hands.

Benefits of Shadow IT

Despite its inherent risks, Shadow IT presents several compelling advantages. By circumventing traditional IT channels, employees can rapidly adopt cutting-edge technologies that better match operational needs and workflows, fostering innovation. This agility empowers departments to deploy and experiment with digital transformation tools without being slowed down by lengthy approval or procurement processes, enhancing operational efficiency.

Additionally, greater control over technology decisions can enhance employee satisfaction, potentially leading to stronger employee engagement and improved retention, key factors in overall business performance and profitability. Moreover, leveraging free or low-cost software outside conventional IT oversight, coupled with bring your own device (BYOD) practices, can deliver meaningful cost savings for individual teams and the organization they serve.

Risks and Downsides of Shadow IT

While shadow IT can streamline workflows and foster innovation, it can also introduce numerous risks, including the following:

- **Security gaps**—Instances of shadow IT erode an organization's control over its digital environment. Because IT can't vet unsanctioned tools, these assets fall outside the scope of corporate cyber hygiene practices, such as antivirus software and threat intelligence services, increasing the likelihood of data breaches and cyberattacks. Compounding the risk, employees often configure these tools with weak credentials, leaving them vulnerable to exploitation.

- **Data loss and leakage**—Shadow IT poses serious risks to data integrity and accessibility. Sensitive data can be stored, transmitted or shared through unprotected channels, increasing the risk of data leaks. Additionally, data stored in personal or unsanctioned accounts may become inaccessible if an employee leaves the organization, disrupting operations.

- **Compliance failures**—Several regulations (e.g., the Health Insurance Portability and Accountability Act, the Payment Card Industry Data Security Standard and the European Union's General Data Protection Regulation) mandate strong data protection measures. As shadow IT operates outside IT's visibility, these assets may lack the necessary access controls, encryption and logging required for passing compliance audits, leaving organizations exposed to regulatory fines or legal action.

- **Loss of visibility and control**—IT teams depend on complete visibility to enforce policies, manage access and apply timely patches that safeguard systems with the latest security updates. Shadow IT undermines this oversight and could leave critical vulnerabilities unpatched, increasing the risk of cyberattacks or regulatory breaches. Unmanaged and outdated shadow IT assets can also malfunction, creating operational inefficiencies.

- **Increased costs and redundancy**—Shadow IT introduces overlapping or duplicate services that drain company resources and complicate IT support. When digital tools are unaccounted for, multiple departments may unknowingly pay for similar SaaS tools, creating additional costs. Inconsistent software use between teams can also hinder collaboration and cause friction between departments, impacting productivity and employee morale.

- **Reputational damage**—Shadow IT can lead to software breaches, performance issues and compliance failures that undermine an organization's reputation. These problems may trigger customer complaints or negative publicity that damage brand credibility and erode stakeholder trust.

Managing Shadow IT Risks

To mitigate the risks of shadow IT, organizations should consider the following proactive strategies:

- **Discovery and inventory**—Organizations should routinely audit network traffic and cloud activity to identify unauthorized tools and hidden assets. Asset discovery platforms and network sniffing tools that detect unfamiliar IP addresses can provide critical visibility into shadow IT across the digital environment. In addition, companies should conduct periodic IT assessments that incorporate employee input, help desk activity and expense report reviews to uncover unsanctioned applications and services.

- **Risk assessment**—Organizations should evaluate the risk posed by each instance of shadow IT. Risk assessments should consider the severity and context of each case to prioritize mitigation efforts on high-risk applications and devices, ensuring resources are allocated effectively.

- **Policy and governance**—Organizations should establish clear, company-wide usage and procurement policies to curb shadow IT. Policies should define acceptable use of third-party applications and devices, set restrictions on unsanctioned software and create transparent approval mechanisms.

- **Employee education and training**—Organizations should educate employees on the dangers of using unapproved applications, devices and software. Training should include practical tips for secure technology use and reinforce the process for requesting new digital tools.
- **Access management and control**—Organizations should implement robust identity and access management protocols to limit exposure to shadow IT. Companies should use multi-factor authentication, role-based access controls and network segmentation to ensure only authorized users and applications interact with sensitive systems.
- **Cross-functional collaboration**—Organizations should work with employees and business units to incorporate their preferred tools into the IT ecosystem wherever possible, balancing innovation with security. Regular communication with department managers can help identify emerging technology needs and foster a cooperative approach to tool adoption.
- **Continuous monitoring**—Organizations should deploy technical solutions that provide real-time visibility into application usage across the network. Companies should leverage monitoring tools to flag unauthorized or risky behavior, detect policy violations, and identify emerging shadow IT trends.

Conclusion

While shadow IT often stems from employees' pursuit of efficiency and innovation, it can expose organizations to significant security, compliance and operational risks. However, by recognizing both its advantages and pitfalls, and implementing robust risk-mitigation strategies, organizations can effectively manage unsanctioned technology use without stifling the innovation and evolving needs of their teams.

Contact us today for additional risk management guidance.