CYBER

INSIGHTS

LloydSadd

NAVACORD®

The Risk of Shadow IT

Cloud-based services are rapidly growing. With new growth comes new challenges, and shadow IT is one area of concern.

Shadow IT refers to the use of IT-related hardware—including cloud applications—without the approval of IT or a security group. Specifically, employees have become comfortable with downloading and using cloud applications for work but often do so without involving the necessary IT department. This can pose security risks such as exfiltration of sensitive data or malware spread throughout the business.

Most organizations have some level of shadow IT; however, the greater this practice's presence, the more difficult risk management becomes, as it's hard for organizations to comprehend what needs to be protected. Therefore, it's critical for organizations to understand why shadow IT occurs, be aware of the types and threats posed by it, and know how to mitigate the risks.

Common Reasons Why Shadow IT Occurs

Shadow IT is usually performed by employees looking to complete a specific task they're struggling with or to help them create work efficiencies. As such, it's important to mention that it's rarely the result of malicious intent from an employee. The following are additional common reasons shadow IT occurs:

- Lack of adequate storage space
- Lack of tool functionality
- Inability to share data with third parties
- Lack of necessary video, messaging or development tools
- Inability to quickly and efficiently request applications and services through a corporate system

Not only is it important to understand why employees may seek external assets, but it's also beneficial to know the types of shadow IT that can be seen in organizations.

Types of Shadow IT

There are two main ways that shadow IT can appear within organizations: unmanaged devices and unmanaged services. Understanding the implications of both can help employers convey their risks to employees.

Unmanaged Devices

The most understood area of shadow IT is unsanctioned devices on a network. Any device not configured by an organization will most likely fall under shadow IT. Unsanctioned devices can appear as:

- Personal devices belonging to employees being used on the core network
- Equipment that is configured incorrectly
- Smart devices that haven't been approved by IT
- Servers or Wi-Fi access points being used by employees without prior approval

Unmanaged Services

The less familiar but growing area of shadow IT is shadow cloud services. Shadow cloud services can appear as:

- Unapproved video or messaging services with no monitoring in place
- External cloud storage that employees use to share files with third parties without permission
- Unapproved tools, such as project management services used as an alternative to those already offered
- Any third-party tool that could be gathering confidential information

Regardless of the shadow IT type, both pose dangerous threats to organizations.

Threats Posed by Shadow IT

Shadow IT introduces threats not otherwise present within corporate IT. It makes risk management difficult because organizations cannot understand what they need to protect. Specific threats posed by shadow IT include:

- **Data theft**—Many security features that organizations apply to business devices and services are unlikely to have been applied to shadow IT devices, leaving them vulnerable. Although it's critical for organizations to protect their data, shadow IT makes this difficult because it's not possible to know where data is being processed or where it ends up. Ultimately, shadow IT can expose organizations to ransomware threats, legal issues surrounding data, reputational damage and recovery costs.
- **Exploitation of services or devices**—Typical risk reduction practices such as firewalls, antivirus software and multifactor authentication are not guaranteed to be in place with shadow IT devices or applications. Organizations risk being exposed to threats from malware, network monitoring and lateral movement when using shadow IT.

Risk Mitigation Strategies

With shadow IT a growing concern, it's critical for organizations to know how to mitigate related issues now and limit the occurrence of shadow IT in the future. Remember, most instances of shadow IT are not malicious acts from employees but attempts to make their jobs more efficient or to simply get their work done. In fact, most employees have no idea they are putting an organization at risk with shadow IT. To help mitigate the risks of shadow IT, organizations should consider the following guidance:

- Avoid unnecessary lockdowns of enterprise IT and ensure employees have sufficient devices, software and tools to complete all work duties.
- Implement simple processes for addressing users' requests for additional IT solutions and solve these in a timely manner.
- Create a list of resources or services that are outside of what is normally accessible and gradually make these available in a controlled and monitored way.
- Migrate data from unsanctioned services to business-controlled platforms.
- Adopt video, messaging and cloud services that support employee needs.
- Allow for open conversations about cybersecurity so employees, managers and the IT team can connect about issues across the organization that need to be addressed.

Overall, each organization should search for solutions that work best for both their employee needs and the security needs of the business.

Conclusion

The rapid growth of shadow IT creates a need for organizations to understand the significant risks it can pose. Contact us today for additional information about shadow IT and further risk management guidance.

If you have questions specific to your business, or would like additional information, please reach out to your Lloyd Sadd Advisor.

™®Local Touch. National Strength. Navacord and Navacord logo are Trademarks of Navacord. The information contained herein is general in nature and general insurance description only. The information is not intended to be insurance advice; nor does it amend, modify or supplement any insurance policy. Consult your actual policy or your broker for details regarding terms, conditions, coverage, exclusions, products, services and programs which may be available to you.

LET US HELP YOU MANAGE YOUR RISK

Edmonton: 1.800.665.5243
Calgary: 1.866.845.8330
Kelowna: 1.800.665.5243

lloydsadd.com
info@lloydsadd.com

Local Touch. National Strength.™