**Understanding Shadow IT**

With the increase in technologies and innovative ways to tackle the different types of cyber crimes that are lurking from behind, the increase in the types of cyber-attacks has seen to come to the forefront. One of the common cyber-attacks that organizations face is Shadow IT.

Shadow IT is the use of rogue or unsanctioned IT systems. This could be hardware, software, or cloud services. It is something that has been implemented without the prior knowledge of the organization’s It department. For example, this could be as simple as someone using dropbox or something as complex as a department head going out and getting a brand new system implemented for them. Some people point to the cloud or bring-your-own-device as somehow having created Shadow IT which does not hold. Shadow It has been with people since the sanctioned It.

**Risks of Shadow IT**

Since the IT systems of the organizations do not know the implementation of Shadow IT, there are numerous security and compliance risks associated with this. Many organizations, however, consider this to be a risk while some consider it to be a necessary step, keeping in mind the fast-changing world around us. There are various risks associated with Shadow IT. Below are some of them.

**1. Security Risks**

Since the IT department of any organization does not participate in this and does not know the implementation of this, various loopholes are created due to this. Shadow IT introduces security risks and weakens the security section of an organization. Although some of the applications seem to be not harming the organization and sharing confidential information, various SaaS applications require exchanging of sensitive and confidential data between various groups or chats for a varied number of reasons. Without the knowledge of what is getting used and how the professionals can’t find out ways to solve the issue.

**2. Inefficiency In Collaboration**

Collaboration is an important aspect of any organization. When different teams work together, collaboration and teamwork are important factors. But this aspect is affected due to the dependency of employees on various applications which differ from one department to the other. On average, there are 55-60 different types of file sharing devices used by the organization which causes this inefficiency. If it is reduced to four or five, this inefficiency will improve.

**3. Risk in managing configurations**

Every organization must maintain a database where they store the details of the applications which are being used and introduced. This helps in maintaining the configuration details. But, since Shadow It works without the consent and knowledge of the organizations, those new applications will not be stored in the database. Thus, there will be mismanagement in this regard.

**4. Risks related to costs**

Another risk associated with the use of SaaS applications is that the cost suffered by the organization goes high. When the Shadow IT system becomes a part of the project, the professionals need to increase the resources, which in turn increases the cost in an unjustified manner.

**How does attack surface management help to tackle the risk?**

There are various ways by which attack surface management can help in mitigating the risks associated with Shadow It. Below are some of them.

**1. Communication**

There must be a clear understanding of the needs of the IT users. There must be transparency and honest communication between the IT professionals and the IT users to have a clear understanding of the needs, experiences, and ways of improvement.

**2. Educating the employees**

The employees and the users should be informed about the various types of risks that are associated with Shadow IT and the possible means by which the risks can be mitigated. Those who are educated on this will be more likely to comprehend the associated risks and find solutions accordingly.

**3. Use of technologies**

Technologies that can detect and find Shadow It and any unknown systems must be implemented.

**4. Mitigating risks**

Continuous evaluation must be done to seek novel ways to tackle different associated risks as not all Shadow IT technologies have the same risk and impact.

**References**

1.<https://www.bmc.com/blogs/shadow-it/#_Risks_Associated_with>

2.<https://www.techtarget.com/searchcloudcomputing/definition/shadow-IT-shadow-information-technology>

3.<https://www.comparitech.com/blog/information-security/shadow-it/>

4.<https://kmicro.com/what-is-shadow-it/>

5.<https://www.cloudflare.com/en-in/learning/access-management/what-is-shadow-it/>

6.<https://www.techtarget.com/searchcio/tip/6-dangers-of-shadow-IT-and-how-to-avoid-them>

7.<https://www.sailpoint.com/identity-library/how-to-mitigate-common-shadow-it-risks/>