4. IT risk assessment is used to identify security risk s and assessing what threat they pose.

5.

|  |  |  |
| --- | --- | --- |
| Risks, threats, and vulnerabilities | Primary domain impact | Risk impact/ factor |
| Unauthorized access from public internet | Remote Access Domain | 1 |
| User destroys data in application and delete all these files | Systems/Application Domain | 3 |
| Hackers penetrates your IT infrastructure and gains access to your internal network | LAN to WAN domain | 1 |
| Intraoffice employee romance gone bad | User domain | 3 |
| Fire destroys primary data center | Systems/Application Domain | 1 |
| Service provider service level agreement is not achieved | WAN domain | 1 |
| Workstation operating system has known software vulnerabilities | Workstation Domain | 2 |
| Unauthorized access to organization-owned workstations | Workstation Domain | 1 |
| Loss of production data | Systems/Application Domain | 2 |
| Denial of service attack on organization Demilitarized Sone and email server | LAN to WAN Domain | 1 |
| Remote communications from home office | Remote Access Domain | 2 |
| Local Area Network server OS has known software vulnerability | LAN Domain | 2 |
| User downloads and clicks on an unknown email attachment | User Domain | 1 |
| Workstation browser has a software vulnerability | Workstation domain | 3 |
| Mobile employee needs secure browser access to sales-order entry system | Remote Access Domain | 3 |
| Service provider has a major network outage | WAN Domain | 2 |
| Weak ingress/egress traffic-filtering degrades performance | LAN to WAN Domain | 3 |
| User inserts CDs and USB hard drives with personal photos, music, and videos on organization-owned computers | User Domain | 2 |
| VPN tunneling between remote computer and ingress/egress router needed | LAN to WAN Domain | 2 |
| WLAN access points are needed for LAN connectivity within a warehouse | LAN Domain | 3 |
| Need to prevent eavesdropping on WLAN due to customer privacy data access | LAN Domain | 1 |
| DoS/DDoS attack from WAN/internet | WAN Domain | 1 |

9.

Paragraph 1:

A Workstation domain is very prone to getting malicious software and vulnerabilities when it is not kept up to date. A user’s domain has vulnerabilities from the user being able to accidentally or unknowingly download from a malicious site or malware, as well as social engineering can also be used to create an attack. LANs are a trusted network where it can have software vulnerabilities and have worms spreading through the OS, which can affect other computers. WAN risks are from the service provider who can have major outages, where the server can receive a DOS or DDOS attack. System Application Domain hold several applications which are prone to be a fire hazards, which can destroy a primary data center or also have a DOS attack, or a AQL injection attack that modifies data and can allow attackers into the server/system. Remote Access Domains use VPN which has a vulnerability of being infected with a virus due to the tunneling. Lastly LAN to WAN can be penetrated from a weak ingress/egress- malicious software can also be downloaded through an unnecessary port that was open through the firewall.

Paragraph 2:

Risk are assessed from an all stages from a high, medium, or low standpoint. Risks are assessed from what the damages are- like if they loss major assets/resource, injury to the organization/individual would be considered major. A moderate or low effect would include anything that poses no immediate threat. The need to identify the level of risk is important and necessary in order to avoid any impacts it would have on the organization’s day-to-day operations. The likelihood is also a contribution to the level of risk it is.

Paragraph 3:

The following domains are at a level 1 risk: System/application domain and Remote Access Domain. The following are at a level 2 risk: WAN domain, Lan Domain, and LAN to WAN Domain. The following are at a level 3 risk: User Domain and Workstation Domain.

Paragraph 4:

After completing the risk assessment the plan would be to create and execute a mitigation plan.