Jackson Warren

Jeremy Bergen

CSCI 370

9/3/21

Week 1 Lab: Performing a Qualitative Risk Assessment for an IT Infrastructure

IT Risk Assessment is done to point out weaknesses in a system. It is done to proactively aid in stopping any potential future threats/attacks that could potentially hurt a company or its people in the future. Then, a thorough analysis will consider the level of each risk as well, ranging from “Immediately Dangerous” to “Very Low Risk”.

|  |  |  |
| --- | --- | --- |
| **Risks, Threats, and Vulnerabilities** | **Primary Domain Impacted** | **Risk Impact/ Factor** |
| Unauthorized access from public Internet | WAN | 1/2 |
| User destroys data in application and deletes all files | User | 3 |
| Hacker penetrates your IT infrastructure and gains access to your internal network | LAN - WAN | 1 |
| Intraoffice employee romance gone bad | User | 3 |
| Fire destroys primary data center | System | 1 |
| Service provider service level agreement (SLA) is not achieved | WAN | 2 |
| Workstation operating system (OS) has a known software vulnerability | Workstation | 3 |
| Unauthorized access to organization-owned workstations | LAN | 1/2 |
| Loss of production data | System | 2 |
| Denial of service attack on organization Demilitarized Zone (DMZ) and e-mail server | System | 2/3 |
| Remote communications from home office | Remote User | 3 |
| Local Area Network (LAN) server OS has a known software vulnerability | LAN | 2 |
| User downloads and clicks on an unknown e-mail attachment | User | 3 |
| Workstation browser has a software vulnerability | Workstation | 2 |
| Mobile employee needs secure browser access to sales-order entry system | Remote Access | 3 |
| Service provider has a major network outage | WAN | 1 |
| Weak ingress/egress traffic-filtering degrades performance | LAN - WAN | 3 |
| User inserts CDs and USB hard drives with personal photos, music, and videos on organization-owned computers | User | 2 |
| Virtual Private Network (VPN) tunneling between remote computer and ingress/egress router is needed | LAN - WAN | 2/3 |
| Wireless Local Area Network (WLAN) access points are needed for LAN connectivity within a warehouse | WAN to LAN | 2 |
| Need to prevent eavesdropping on WLAN  due to customer privacy data access | LAN to WAN | 1 |
| Denial of service (DoS)/distributed denial of service (DDoS) attack from the Wide Area Network (WAN)/Internet | WAN | 1 |

1. To summarize my findings, local problems will usually be much less substantial. Most of these things would only affect immediate employees and could be solved without much risk of damage. Higher level problems, at or above the WAN level, appear much more significant. Loss of service is a major issue and will pose a huge risk to a company causing loss of profits as the company is unable to operate. Leaking information or getting penetrated security also poses a huge threat, making outside sources a very high-risk factor. Although some local problems do pose very large threats to a company, I believe higher level domains are harder to control.
2. My approach to assigning these values, as mentioned before, mostly had to do with control of a problem. Remote access, System issues, WAN issues, all are large threats and would affect the entire company. A DDoS attack on a company website could pose a very large risk to a company. Losing service could shut down a company for hours resulting in losing thousands in sales. User problems and LAN problems appear to be much easier to solve to me. One employee is affected, or a small group, but not the entire company being halted like some of the higher risk problems. While some of these issues that were more local may very well be high risk, I based my ideology on the idea that higher domain level problems were harder to solve and more people were impacted.
3. For very high-risk assessments, it is ideal to address all of these areas as quickly as possible. All boxes marked with a “1” could be detrimental if not solved somewhat quickly, meaning the risk impact would be very great. Then, deciding which ones to address next becomes somewhat conditional. From here, the 7 domains could become much more important. Once again, addressing the higher-level domains should come first. These domains are usually more threatening and can create more damage companywide due to a larger number of people exposed or leaking the entire company’s info, rather than just a single user facing an issue that could be a secluded issue. The risk impact for these cases would be much lower to the company as a whole, meaning these can wait to be addressed.
4. For next steps, as mentioned before, the high-risk assessment topics will have high risk impact, and should all be addressed as soon as possible. Speed of solving, and man power should be considered, but all should be solved. Once these are addressed, looking at the domains affected are going to be more relative. Should high level domains have a larger number of individuals affected, these should be addressed next. Then, after all the problems that are going to create somewhat major issues for the entire company are addressed, it becomes a question of the difficulty of solving the problem. Resolving a relationship gone wrong will be very easy to solve, and will require very little man power to do so, but may not be a large threat to the company. Finding a new browser that has a vulnerability may be much harder to do, and might not be worth the change, even though it’s higher risk. Taking domain level, number of individuals affected, man power required to fix it, and price to fix it all become very relevant for each issue from this point on.