James Everett Tourtellotte IV
W. McLaughlin
9/18/2022
ITN 262

| Risks, Threats, and Vulnerabilities | Primary Domain Impacted | Risk Impact/Factor |
|---|---|---|
| Unauthorized access from public Internet | Remote Access Domain | 2 |
| User destroys data in application and deletes all files | System/Application Domain | 2 |
| Hacker penetrates your IT infrastructure and gains access to your internal network | LAN Domain | 2 |
| Intraoffice employee romance gone bad | User Domain | 3 |
| Fire destroys primary data center | System/Application Domain | 1 |
| Service provider service level agreement (SLA) is not achieved | System/Application Domain | 3 |
| Workstation operating system (OS) has a known software vulnerability | Workstation Domain | 1 |
| Unauthorized access to organization-owned workstations | Workstation Domain | 2 |
| Loss of production data | System/Application Domain | 2 |

| | | |
|---|---|---|
| Denial of service attack on organization Demilitarized Zone (DMZ) and e-mail server | System/Application Domain | 2 |
| Remote communications from home office | Remote Access Domain | 3 |
| Local Area Network (LAN) server OS has a known software vulnerability | LAN Domain | 2 |
| User downloads and clicks on an unknown e-mail attachment | User Domain | 3 |
| Workstation browser has a software vulnerability | Workstation Domain | 2 |
| Mobile employee needs secure browser access to sales-order entry system | Remote Access Domain | 3 |
| Service provider has a major network outage | System/Application Domain | 1 |
| Weak ingress/egress traffic-filtering degrades performance | LAN to WAN Domain | 2 |
| User inserts CDs and USB hard drives with personal photos, music, and videos on organization-owned computers | Workstation Domain | 3 |
| Virtual Private Network (VPN) tunneling between remote computer and ingress/egress router is needed | Remote Access Domain | 3 |
| Wireless Local Area Network (WLAN) access points are needed for LAN | LAN-to-WAN Domain | 3 |

| | | |
|---|---|---|
| connectivity within a warehouse | | |
| Need to prevent eavesdropping on WLAN due to customer privacy data access | Lan-to-WAN DOMAIN | 2 |
| Denial of service (DoS)/distributed denial of service (DDoS) attack from the Wide Area Network (WAN)/Internet | WAN Domain | 2 |

An IT Risk assessment's goal or objective is to identify risk and the cost of impact and recovery.

The listed risks, threats, and vulnerabilities depicted in the lab highlight a wide range of impacts across the seven domains of a typical IT Infrastructure. The Workstation Domain and the System/Application Domain were by far the most common in this exercise. It was shown that both of these Domains not only had the entire range of Risk Impact/Factors, but they both had Critical Risk Factors existing within them. This is a necessary finding I believe as Critical Risk Impacts are the most important for a company to tend to, when assessing or remediating their security posture.

In this report, it is recommended that the executive decisions following would be to remediate the vulnerabilities rated with to be a Critical Risk. Whether or not the assessment (lab) is correct in its findings, it is imperative to identify Vulnerabilities with Critical Risk Impact and rectify them immediately. These risks are rated as such because they have significant impact on the company, specifically legal liability. After remediation of Critical Risk Vulnerabilities, it is recommended to move to major risk elements and minor risk elements - in that order. The context provided only allows for so much risk assessment, the major and minor risks can undoubtedly become major risks if left unattended. This is why it is important to tend to them even if they do not pose a significant risk to the company, relatively speaking, like Critical Risk Elements do.

To provide a clear, and concise, risk assessment and risk impact summary of the seven domains of a typical IT Infrastructure we will start at the User Domain, and navigate our way to the Remote Access Domain. The User Domain has a Risk assessment level of 3, and its Risk Impact is Not Applicable. Failure at this domain generally poses no impact on a company, and has a minor effect if any at all. Next we have the Workstation Domain, failure at this domain would have a low impact and would be rated a 2 - deeming it a Major risk. This is because failure of a Workstation could impact the companies' mission and it impacts the CIA of an organization's intellectual property assets and IT infrastructure. The above pairing of a "Low impact" and a 2 rating for risk assessment would apply to the LAN Domain and LAN-to-WAN Domain as well. At failure, these are low impact domains that cause minor damage or financial loss at most. However, when you move to the WAN Domain the impact becomes Moderate. The risk assessment is still considered Major, a 2, but failure at the WAN Domain is in no way a Low Impact Failure. This is because the magnitude of affected infrastructure increases significantly, which is the distinction between Low impact and Moderate impact. As infrastructure increases in size, so does potential impact. Failure at the System/Application Domain would be deemed a High

Impact due to its magnitude of potential infrastructure and its level of potential loss at this Domain. Whether it is a breach in privacy, or a fire at a data center, a failure at this domain can cause a major risk to the company involved. Failure would be considered a critical risk, a 1, if given a risk assessment. Finally, we have the remote access domain. This would have a risk assessment of Major, a 2, and a Moderate Impact if the Domain fails. Any sort of failure in the CIA Triad here would cause a significant impact on mission effectiveness, significant damage to assets, or significant financial loss. Whether it is a remote employee, or a hacker that wants to breach your system, the remote access domain provides opportunity to significantly impact ones' company. This is why it is important to understand the outcomes of failure at this point.

I would recommend the following approach for remediating the risks, threats, and vulnerabilities outlined in the above table. It is imperative that executive management identifies the Critical Risks and remediates them first. From there tackle the rest of the risks, threats, and vulnerabilities in descending order. They should remediate their Major risks before their Minor risks. When they remediate their Major risks, they should identify the ones with the highest impact and fix those first. Then they can move to remediating their Minor risks.