Case study : Information security investigation and analysis at UUniversity

Q1) you have been appointed as the new InfoSec Risk manager at UUniversity. You are asked to deliver a detailed risk assessment report to the CISO, to help him understand UUniversity’s current Risk situation. Your report should consist of the following working sheets, lists and justifications:

**A-The assets inventory.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Asset ID | IT Asset | Operational  Domain | Data Category | Cost of Ownership | Impact on Reputation | Impact on Mission | Assets Weight |
| A1 | Routers | 2,3 | Unclassified (U) | 15 | 20 | 20 | 55 |
| A2 | Switches | 2,3 | Unclassified (U) | 12 | 20 | 20 | 52 |
| A3 | **Web server** | 2,3 | Confidential (C) | 28 | 30 | 20 | 78 |
| A4 | Cloud services | 3 | Confidential (C) | 23 | 30 | 10 | 63 |
| A5 | Website | 2,3 | Unclassified (U) | 10 | 20 | 20 | 50 |
| A6 | Computers | 2,3 | Unclassified (U) | 15 | 20 | 20 | 55 |
| A7 | Learning-resources | 2,3 | Unclassified (U) | 12 | 20 | 20 | 52 |
| A8 | **Network admin** | 2,3 | Unclassified (U) | 25 | 20 | 20 | 65 |
| A9 | **Credentials** | 1 | Secret Data(S) | 27 | 40 | 10 | 77 |
| A10 | Student | 1 | Unclassified (U) | 20 | 20 | 10 | 50 |
| A11 | Staff | 2 | Unclassified (U) | 20 | 20 | 10 | 50 |
| A12 | **Personal Data** | 1 | Secret data (S) | 28 | 40 | 10 | 78 |
| A13 | Academic situation | 1 | Confidential (C) | 11 | 30 | 10 | 51 |
| A14 | E-reg System | 2 | Unclassified (U) | 20 | 20 | 10 | 50 |
| A15 | Study schedule | 1 | Unclassified (U) | 10 | 20 | 10 | 40 |
| A16 | Remote Desktop | 2,3 | Confidential (C) | 18 | 30 | 20 | 68 |
| A17 | NAC | 3 | Confidential (C) | 29 | 30 | 10 | 69 |
| A18 | **Firewalls** | 2,3 | Unclassified (U) | 25 | 20 | 20 | 65 |
| A19 | **Antiviruses** | 1,2 | Unclassified (U) | 12 | 20 | 20 | 52 |
| A20 | Online Services | 2,3 | Unclassified (U) | 19 | 20 | 20 | 59 |
| A21 | Online Users | 1 | Unclassified (U) | 25 | 20 | 10 | 55 |
| A22 | **Intellectual property** | 2,3 | Secret data (S) | 21 | 40 | 20 | 81 |
| A23 | Third party application | 3 | Unclassified (U) | 15 | 20 | 10 | 45 |
| A24 | Projects | 2,3 | Confidential (C) | 15 | 30 | 20 | 65 |
| A25 | Courses | 2,3 | Confidential (C) | 15 | 30 | 20 | 65 |

***Notes:***

1. Personal data it includes dissertation materials, exam results and course grades, but since all I will grade it the same within the inventory I will all include with personal data to keep it neat and concise.
2. Local —> internal network.
3. Global —> external network.
4. The classification of data based on what I understand.

A-Unclassified is the data that is accessed by the public domain.

B-Confidential is important data but encrypted -still can be accessed not only by the owner.

C-Secret Data is the data that only accessed by its owner in a secure manner.

**A1-A2-A18-A19**-that are accessed like the firewalls locally and globally which affect the mission to be 20/30 and its unclassified since accessed by the public domain which affects the reputation by 20 the cost of routers which is max 5,000 but the switches less than routers. However, firewalls are the most expensive of both and more than anti viruses that ranges from 9.98-69.99 $. Instead, the anti-virus applied locally and to the user domain since its applied to PC and on devices within the university.

**A5-A14**-E-reg Only accessed by university domain (Locally) but the website both internally and externally and since its available for the public domain indicates that its only affect 20% of reputation because of unclassified and the E-reg system more valuable than the university website.

**A3-A4**-web server accessed by users that is responsible to respond to users (students and doctors) requests which indicates that used on both locally and globally and it's not kept secret indeed it’s not unclassified since one of its aspects is confidentiality and privacy by encrypting the content of a message and obfuscating the sending and receiving parties’ identities and it’s too expensive since there are costs like 62000-39000 and others. On the other hand, cloud service accessed globally that its costly too but less than web servers that ranges from 400 monthly for one server to 15,000 for the entire backup.

**A7-A8**-both can be accessed internally and externally with respect to the university that affect the mission (20) and both unclassified since accessed by the public domain but vary on the cost since network administrator more important since it restrict what can access the network and what cannot.

**A9-A12-A13**- all are user domain (only accessed by the user such as PC) and are secret data except academic situation that is not secret but not unclassified or accessed for the public domain which means that its confidential (Private or encrypted) since student and professors can access the student academic situation and grades.

**A10-A11-A15**-since student are user domain and study schedule (for the major it’s already available on the university website) accessed by the user such as PC except staffs that are accessed within the local university domain, students and staff are important that provide 20/30 of university cost and are unclassified.

**A16-A20-A22-A24-A25**- remote desktop accessed internally and externally and its confidential since it request remove access for the university network as well online services and IP with the projects and courses it protect but they have different classification, the online services are unclassified since accessed by the public domain while the IP its secret data that is linked with the university reputation and it protects the projects as well as the courses that are confidential and needed to be protected. Online services since its publicly published its unclassified.

**A17-A21-A23**- both are globally accessed the NAC has confidential data classification since it restricts the availability of network resources to endpoint devices and users that comply with a defined security policy and has more cost as a result of NAC needs license and vendor maintenance and training for network or security administrators but the Third-Party Application has less cost. On the other hand, online users are only user domain and unclassified but has more cost than Third Party Application.

|  |  |  |
| --- | --- | --- |
| Threat ID | Threat Description | Threat Rank (1-5) |
| T1 | Malware attacks | 3 |
| T2 | Denial of service (Dos) and  Distributed denial of service (DDos) | 4 |
| T3 | Phishing Attack | 3 |
| T4 | Activity interruption | 2 |
| T5 | Theft of personal Data | 5 |
| T6 | Theft of IP  (The intellectual property) | 5 |
| T7 | gaining unauthorized access over the network to university assets. | 1 |
| T8 | Forces of Nature | 3 |

**B-Threat inventory.**

T1) **Malware Attacks**: based on many surveys 36% of users lose money online as a result of a malware attack which shows that the malware analysis can cause financial loss, it affects the reputation especially ransomware based on IBM report and backdoor (A shell is listening on the remote port without any authentication being required) that might get accessed to sensitive and personal information and modify it. Moreover, as a result of development of new and unique malware that results in high potential for the frequency of occurrence to such threat. We can protect from by stay up to date, apply patches and updates, avoid suspicious emails. (Does not require high cost just attention and focus).

T2) **Dos and DDos**: Small business lose between 8,000-74,000 for every hour of downtime which indicate that there is financial loss, it might lead to embarrassment and reputational damage to the company, based on financial loss it costs to protect from, organizations face 20-50 DDos attacks per month that is highly frequented.

T3) **Phishing Attack**: it’s type of RE that often steal the credentials that are related to the viable asset which are the customers which means that there is financial lost, reputational damage, highly occurring. We can protect data by storing the data properly in an encrypted way as well as make number of people who access such data as minimized as we can.

T4) **Activity interruption**: it might include little financial loss and reputation based on data interrupt it as well as the type of data (sensitive or other) and whether it’s encrypted or send as a plaintext as well as the interrupter action whether only to eavesdrop or eavesdrop and modify.

T5) **Theft of personal Data**: it includes reputational damage since it might consequence in customer loss and reduction in the profits. Financial loss and it requires to protect it and might cause loss in the competitive advantage by making the process less -the same applied to **IP theft**: Intellectual property is also of high value as it represents the university competitive advantage and relates to its daily operations-***Very significant***-.

T7) **gaining unauthorized access over the network to university assets:** in my own point that this threat is rare that has only potential financial loss and we can protect from by restricting the BYOD and only allow the users to use organization legitimate devices (restrict access to organization or company devices only)-***Not significant***-.

**C- Asset-Vulnerability matching list:**

|  |  |  |
| --- | --- | --- |
| Asset ID | Vulnerability ID | Vulnerability Description |
| A3, A4, A5, A12, A14. | V1 | The use of Remote Desktop Protocol (RDP)  It provides user interface for remote access over the network |
| A1, A2, A3, A4, A5, A6, A9. | V2 | consumerization of IT. The use of BYOD that gives users ability to bring their own devices without Vulnerability scanning and access the university assets. (The use of unmanaged devices). |
| A9, A12, A22, A24, A25. | V3 | Remote connections are not managed which may lead to unauthorized access and data leakage to sensitive data. |
| A3, A4, A9, A14, A20. | V4 | Hosting website and e-registration systems on local web servers without having high availability resources to protect them from denial of service |
| A9, A12. | V5 | Issuing credentials and verification and utilization to access online services is not managed properly for new students and staff to control access to sensitive and confidential data |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Asset/Threat | Routers | Switches | Web server | Cloud services | Website | Computers | Learning -Resources | Network Admin | Credentials |
| Malware attacks | V2  T1V2A1 | V2  T1V2A2 | V1  T1V1A3  V2  T1V2A3 | V1  T1V1A4  V2  T1V2A4 | V2  T1V2A5 | V2  T1V2A6 |  |  | V2  T1V2A9 |
| Dos/DDos |  |  |  |  |  |  |  |  |  |
| Phishing attack |  |  | V4  T3V4A3 |  |  |  |  |  | V3  T3V3A9  V5  T3V5A9 |
| Activity Interruption |  |  |  |  |  |  |  |  | V3  T4V3A9  V5  T4V5A9 |
| Theft of personal data |  |  | V2  T5V2A3  V4  T5V4A3 | V2  T5V2A4 |  |  |  |  | V2  T5V2A9  V3  T5V3A9  V5  T5V5A9 |
| Theft of IP |  |  |  |  |  |  |  |  |  |
| unauthorized access over the network to university assets. |  |  | V1  T7V1A3  V2  T7V2A3  V4  T7V4A3 | V1  T7V1A4  V2  T7V2A4  V4  T7V4A4 | V1  T7V1A5 |  |  |  | V3  T7V3A9 |
| Forces of Nature |  |  |  |  |  |  |  |  |  |
| Priority of effort | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | ……… |

**D-Threat, Vulnerability and assets (TVA) worksheet:**

V1🡪 can be mitigated by configuring the firewall to allow bypass only to specified devices.

V2🡪 can be mitigated by configuring the firewall to allow bypass only to specified devices.

V3🡪 can be mitigated by using the NAC (network access control) that support network visibility and access management through policy enforcement on devices of the users of corporate networks.

V4🡪 have no mitigation now but it can be done by tracking the server logs and automate backup of the data.

V5🡪 have no mitigation but it can b e done by applying multi-level encryption on the data.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Asset/Threat | Student | Staff | Personal Data | Academic situation | E-reg System | Study Situation | Remote Desktop Protocol | NAC |
| Malware attack |  |  |  |  |  |  |  |  |
| Dos/DDos |  |  |  |  | V1  T2V1A14  V4  T2V4A14 |  |  |  |
| Phishing attack |  |  | V3  T3V3A12  V5  T3V5A12 |  |  |  |  |  |
| Activity Interruption |  |  | V3  T4V3A12  V5  T4V5A12 |  |  |  |  |  |
| Theft of Personal Data |  |  | V1  T5V1A12  V3  T5V3A12  V5  T5V5A12 |  | V1  T5V1A14 |  |  |  |
| Theft of IP |  |  |  |  |  |  |  |  |
| unauthorized access over the network to university assets. |  |  | V3  T7V3A12 |  |  |  |  |  |
| Forces of Nature |  |  |  |  |  |  |  |  |
| Priority of effort | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Asset/Threat | Firewalls | Anti-virus | Online Services | Online Users | Intellectual Property | Third Party application | Projects | Courses |
| Malware Attacks |  |  |  |  |  |  |  |  |
| Dos/DDos |  |  | V4  T2V4A20 |  |  |  |  |  |
| Phishing attack |  |  |  |  |  |  |  |  |
| Activity Interruption |  |  |  |  |  |  |  |  |
| Theft of Personal Data |  |  |  |  |  |  |  |  |
| Theft of IP |  |  |  |  | V3  T6V3A22 |  | V3  T6V3A24 | V3  T6V3A25 |
| unauthorized access over the network to university assets. |  |  |  |  |  |  |  |  |
| Force Of Nature |  |  |  |  |  |  |  |  |
| Priority of effort | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Asset ID | Asset Weight | Vulnerability ID | Threat ID | Likelihood Estimation | Control Estimation | Risk Rate |
| **A1** | 55 | V2 | T1 | 0.8 | 0.20 | 57.2= (0.8\*55) -((0.8\*55) \*0.20) +((0.8\*55) \*0.50). |
| **A2** | 52 | V2 | T1 | 0.8 | 0.20 | 54.08= (0.8\*52) -((0.8\*52) \*0.20) +((0.8\*52) \*0.50). |
| **A5** | 50 | V1 | T7 | 0.5 | 0.20 | 32.5= (0.5\*50) -((0.5\*50) \*0.20) +((0.5\*50) \*0.50). |
| **A5** | 50 | V2 | T1 | 0.6 | 0.20 | 39= (0.6\*50) -((0.6\*50) \*0.20) +((0.6\*50) \*0.50). |
| **A6** | 55 | V2 | T1 | 0.6 | 0.20 | 32.5= (0.5\*50) -((0.5\*50) \*0.20) +((0.5\*50) \*0.50). |
| **A22** | 81 | V3 | T6 | 0.4 | 0.20 | 42.12= (0.4\*81) -((0.4\*81) \*0.20) +((0.4\*81) \*0.50). |
| **A24** | 65 | V3 | T6 | 0.4 | 0.20 | 33.8= (0.4\*65) -((0.4\*65) \*0.20) +((0.4\*65) \*0.50). |
| **A25** | 65 | V3 | T6 | 0.4 | 0.20 | 33.8= (0.4\*65) -((0.4\*65) \*0.20) +((0.4\*65) \*0.50). |
| **A20** | 59 | V4 | T2 | 0.7 | 0.0 | 61.95= (0.7\*59) -((0.7\*59) \*0.0) +((0.7\*59) \*0.50). |

**E-Ranked Vulnerability risk sheet:** RISK= (likelihood \* asset value)- ((likelihood \* asset value) \*control) + ((likelihood \* asset value) \*uncertainty).

**1)Routers and switches:** are vulnerable to malware attack because the university allow the use of personal devices (BYOD) without any vulnerability scanning that poses the universities routers and switches to malware attack that does not require any skills only searching for online malwares which is not a skill to be gained (0.6) and the asset kind of important (0.2) it can be controlled by disallowing BYOD and online allow the firewall to pass a specified list of devices(Firewalls are available).

**2)Website**: we can gain unauthorized access on by exploiting RDP that does not require any skills the target is it can be done by anyone but the asset value less than routers it also can be controlled by configuring the firewall. Might be also vulnerably to malware attacks by exploiting BYOD that can be controlled by the same way. **Computers:** are vulnerable to malware attack by allowing devices to access the university network without scanning (0.6 without skills and the computers cost 55).

3**)Intellectual property** as well **projects** and **courses** are vulnerable to Theft of IP because of Remote connections are not managed which may lead to unauthorized access and data leakage to sensitive data but it can be controlled by NAC since always there is potential for the threat but we can solve by removing the vulnerability the assets are important but such an exploitation cannot be done by anyone which indicate that IP are very critical to the university since it represents the university competitive advantage and relates to its daily operations.

**5)Online services:** might be vulnerable to DOS attack and there are no controls to protect from that does not require any skills can be done within the CMD or using Wireshark tool.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Asset ID | Asset Weight | Vulnerability ID | Threat ID | Likelihood Estimation | Control Estimation | Risk Rate |
| **A3** | 78 | V1 | T1 | 0.7 | 0.20 | 70.98= (0.7\*78) -((0.7\*78) \*0.2) +((0.7\*78) \*0.50). |
| **A3** | 78 | V2 | T1 | 0.7 | 0.20 | 70.98= (0.7\*78) -((0.7\*78) \*0.2) +((0.7\*78) \*0.50). |
| **A3** | **78** | **V4** | **T3** | **0.7** | **0.0** | **81.9= (0.7\*78) -((0.7\*78) \*0.0) +((0.7\*78) \*0.50).** |
| **A3** | 78 | V2 | T5 | 0.7 | 0.2 | 70.98= (0.7\*78) -((0.7\*78) \*0.2) +((0.7\*78) \*0.50). |
| **A3** | 78 | V4 | T5 | 0.7 | 0.0 | 81.9= (0.7\*78) -((0.7\*78) \*0.0) +((0.7\*78) \*0.50). |
| **A3** | 78 | V1 | T7 | 0.7 | 0.2 | 70.98= (0.7\*78) -((0.7\*78) \*0.2) +((0.7\*78) \*0.50). |
| **A3** | 78 | V2 | T7 | 0.7 | 0.2 | 70.98= (0.7\*78) -((0.7\*78) \*0.2) +((0.7\*78) \*0.50). |
| **A3** | 78 | V4 | T7 | 0.7 | 0.0 | 81.9= (0.7\*78) -((0.7\*78) \*0.0) +((0.7\*78) \*0.50). |
| **A4** | 63 | V1 | T1 | 0.4 | 0.20 | 32.76= (0.4\*63) -((0.4\*63) \*0.2) +((0.4\*63) \*0.50). |
| **A4** | 63 | V2 | T1 | 0.4 | 0.20 | 32.76= (0.4\*63) -((0.4\*63) \*0.2) +((0.4\*63) \*0.50). |
| **A4** | 63 | V2 | T5 | 0.4 | 0.2 | 32.76= (0.4\*63) -((0.4\*63) \*0.2) +((0.4\*63) \*0.50). |
| **A4** | 63 | V1 | T7 | 0.5 | 0.2 | 40.95= (0.5\*63) -((0.5\*63) \*0.2) +((0.5\*63) \*0.50). |
| **A4** | 63 | V2 | T7 | 0.5 | 0.2 | 40.95= (0.5\*63) -((0.5\*63) \*0.2) +((0.5\*63) \*0.50). |
| **A4** | 63 | V4 | T7 | 0.5 | 0.0 | 47.25= (0.5\*63) -((0.5\*63) \*0.0) +((0.5\*63) \*0.50). |

**6)Web Server:**

A- can be vulnerable to malware attack by two vulnerabilities. That both require basic skills in programming languages since RDP is used that allow the remote access to devices and BYOD that allows access devices without scanning.

1. A-RDP that can be controlled by configuration for the network firewall.
2. BYOD by preventing other devices also by configuration of the firewall.

B- The web server is an important asset that is endanger to many threats such as phishing attack if the web server is not well protected and there is no control currently for this that does not require

C- Accessing the web server does not require skill since it does not have the sufficient protection that might lead to gain unauthorized access to the network by RDP that ca be controlled, BYOD can be mitigated by listing the devices that can enter the Network or configure to and the less protection for the local web server might lead to.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Asset ID | Asset Weight | Vulnerability ID | Threat ID | Likelihood Estimation | Control Estimation | Risk Rate |
| **A9** | 77 | V2 | T1 | 0.8 | 0.20 | 80.08= (0.8\*77) -((0.8\*77) \*0.2) +((0.8\*77) \*0.50). |
| **A9** | 77 | V3 | T3 | 0.8 | 0.20 | 80.08= (0.8\*77) -((0.8\*77) \*0.2) +((0.8\*77) \*0.50). |
| **A9** | 77 | V5 | T3 | 0.8 | 0.00 | 92.4= (0.8\*77) -((0.8\*77) \*0.0) +((0.8\*77) \*0.50). |
| **A9** | 77 | V3 | T7 | 0.8 | 0.20 | 80.08= (0.8\*77) -((0.8\*77) \*0.2) +((0.8\*77) \*0.50). |
| **A9** | 77 | V2 | T5 | 0.8 | 0.20 | 80.08= (0.8\*77) -((0.8\*77) \*0.2) +((0.8\*77) \*0.50). |
| **A9** | 77 | V3 | T5 | 0.8 | 0.20 | 80.08= (0.8\*77) -((0.8\*77) \*0.2) +((0.8\*77) \*0.50). |
| **A9** | 77 | V5 | T5 | 0.8 | 0.00 | 92.4= (0.8\*77) -((0.8\*77) \*0.0) +((0.8\*77) \*0.50). |
| **A9** | 77 | V3 | T4 | 0.8 | 0.20 | 80.08= (0.8\*77) -((0.8\*77) \*0.2) +((0.8\*77) \*0.50). |
| **A9** | 77 | V5 | T4 | 0.8 | 0.0 | 92.4= (0.8\*77) -((0.8\*77) \*0.0) +((0.8\*77) \*0.50). |

**7)Cloud services:** Accessing the cloud services requires a lot of skills such as Database, Network management, Cloud security and others and it’s a valuable asset that the vulnerability cannot be easily exploited. Cloud services cannot be easily accessed it requires skills and its valuable asset that cannot be done by anyone unless they were skilled enough to do that. That we can access remotely by RDP and BYOD but it can be mitigated by configuration and the use of firewalls but the unprotection for the web server the controls are not available to find the residual risk of using the current controls.

**8)Credentials:** Anything related to the credential provide a high risk since its critical and there are no mitigation controls available. Except in the cases of remote access can be mitigated by the NAC and firewalls being configurated. Accessing the credential does not require skill and they are a valuable asset that we can protect from BYOD to prevent spreading of malware by scanning the devices or configuring them with the available firewalls (Making a list of acceptable devices to access the university network).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Asset ID | Asset Weight | Vulnerability ID | Threat ID | Likelihood Estimation | Control Estimation | Risk Rate |
| **A14** | 50 | V1 | T2 | 0.4 | 0.20 | 26= (0.4\*50) -((0.4\*50) \*0.2) +((0.4\*50) \*0.50). |
| **A14** | 50 | V4 | T2 | 0.4 | 0.00 | 30= (0.4\*50) -((0.4\*50) \*0.0) +((0.4\*50) \*0.50). |
| **A14** | 50 | V1 | T5 | 0.6 | 0.20 | 39= (0.6\*50) -((0.6\*50) \*0.2) +((0.6\*50) \*0.50). |
| **A12** | 78 | V3 | T3 | 0.6 | 0.20 | 60.84= (0.6\*78) -((0.6\*78) \*0.20) +((0.6\*78) \*0.50). |
| **A12** | 78 | V5 | T3 | 0.6 | 0.00 | 70.2= (0.6\*78) -((0.6\*78) \*0.0) +((0.6\*78) \*0.50). |
| **A12** | 78 | V3 | T4 | 0.6 | 0.20 | 60.84= (0.6\*78) -((0.6\*78) \*0.2) +((0.6\*78) \*0.50). |
| **A12** | 78 | V5 | T4 | 0.7 | 0.00 | 81.9= (0.7\*78) -((0.7\*78) \*0.0) +((0.7\*78) \*0.50). |
| **A12** | 78 | V1 | T5 | 0.8 | 0.20 | 81.12= (0.8\*78) -((0.8\*78) \*0.2) +((0.8\*78) \*0.50). |
| **A12** | 78 | V3 | T5 | 0.8 | 0.20 | 81.12= (0.8\*78) -((0.8\*78) \*0.20) +((0.8\*78) \*0.50). |
| **A12** | 78 | V5 | T5 | 0.8 | 0.00 | 93.6= (0.8\*78) -((0.8\*78) \*0.0) +((0.8\*78) \*0.50). |
| **A12** | 78 | V3 | T7 | 0.8 | 0.20 | 81.12= (0.8\*78) -((0.8\*78) \*0.2) +((0.8\*78) \*0.50). |

**9)E-Reg System:** might be accessed remotely by RDP and not providing the sufficient protection for the web server that can gain unauthorized access as well as causing Dos or DDos attack and the unprotection of the web server might endanger the ability of remote access.

**10)Personal Data:** there is no skills required to be done as well as it might cause theft of personal data which is a critical and important asset within the university that does not require any skills and can be done by any, BYOD can cause also theft of personal data but the difference that it can be controlled by the available controls by configuring the firewalls as well as using NAC that manage the access of a proprietary network. Personal data can be accessed by unauthorized if we use RDP that allows access remotely and we can mitigate by configuration as well as the use of Firewalls.

**Personal Data**

1. Might be vulnerable to data leakage because of unmanaged network connection that is not mitigated and cannot by the current control but it requires skills that does not require that much skills only the phisher use sniffers as a tool.
2. As well as the unmanaging for the credential

That both cause phishing attack as well as Activity interruption and both vulnerabilities are not controlled and asset value high and does not require any skills.

It can cause Theft of personal data by

1. Using RDP that can be controlled and does not require any skills and we can mitigate by current controls.
2. Unmanaging of network connection no skills and controls.
3. Unmanaging of credentials that might have no skills and controls.

**Discussion Questions:**

**Q1: Which IT assets did you prioritize as critical to UUniversity Mission and why:**

**The assets I prioritize more**

1. Web server since its critical asset that is accessed locally and globally that make it vulnerable to additional risks (Larger domain of access means more potential threats within the asset) and is responsible for sending response based on the user request and when it get hacked might expose the user credentials that are stored on the server and is accessed to the application server by servlet request to the Application server that contains the web services.
2. Credentials and personal data since its linked whin the university reputation and if it was compromised the university might lose reputation, financial lose and the potential students.
3. Network Admin that he is responsible for many tasks within the network.
4. such as install, configure and maintain network hardware and software such as routers and switches.
5. Protect network from unauthorized access through physical and technical means.
6. Setup and maintain Virtual Private Network (VPN).
7. Intellectual Prosperity: Intellectual property is also of high value as it represents the university competitive advantage and relates to its daily operations as well as it is related to the university reputation and protects courses and projects as well as research data and result.
8. Firewalls and anti-viruses: since it provides protection for many threats that targeted the university such as

|  |
| --- |
| The use of Remote Desktop Protocol (RDP)  It provides user interface for remote access over the network |
| consumerization of IT. The use of BYOD that gives users ability to bring their own devices without Vulnerability scanning and access the university assets. (The use of unmanaged devices). |

**Q2) Describe three top security risks that UUniversity is currently exposed to, with a focus on threat definition, impacts, consequences, likelihood and severity impact:**

**1-**Personal Data (A12)🡪 As a result of Theft of personal Data the users (student and doctors) credentials will be compromised and stolen and might sell them on the dark web that affects the university reputation as well as the student trust

Likelihood of this threat High The threat source highly motivated and very capable, and controls to prevent the exploitation of the vulnerability are ineffective.

Severity scale is critical

**2**-Web server-🡪 as a result of phishing attack it causes loss of credentials and users (employee and doctors) that affects the loss of university productivity and customers.

Likelihood of this threat High The threat source highly motivated and very capable, and controls to prevent the exploitation of the vulnerability are ineffective.

Severity scale is critical

**3-**Credentials 🡪as a result of Activity interruption it causes loss in data that affects the university value to be decreased as well as the reputation of the university

Likelihood of this threat High The threat source highly motivated and very capable, and controls to prevent the exploitation of the vulnerability are ineffective.

Severity scale is critical

**Q3)** **Given the potential risks that you have identified, what IT security policies and countermeasures would you recommend be created and implemented at UUniversity to help mitigate each of the identified risks in your report.**

**1)**Avoid the usage of devices from outside the university domain in order to be involved in the scanning process to avoid spreading malwares to network devices and others.

**2)** Use firewalls (both software and hardware where available) to restrict access to remote desktop listening ports (default is TCP 3389). Using an RDP Gateway is highly recommended for restricting RDP access to desktops and servers as well as the anti-viruses should be applied on the different stages within the university not only on the network level.

**3)T**o protect from unauthorized access we have to stay up to date by applying the latest security updates and patches as well as to use the network segmentation by defining boundaries within different types of internal networks.

**4)**Provide the sufficient protection for the web server since it’s a critical component by tracking server logs by storing them in a segmented manner and at the end of the day to be able to identify the unsuccessful login attempts, if you give equal access to all the users on the server, then, anyone can get into the important data, and manipulate the data. The possible way out is to give role-based privileges to users, and don’t give anyone access to backend databases, unless they are security experts dealing with all the internal server activities.

**5)**Need to apply multi-level encryption on the data and to be aware of social engineering by using the zero-trust policy that secures the university by eliminating the implicit trust and continuously validate every stage of digital interaction.