Risk Assessment Report – Computer Laboratory and ICT Equipment at Public Schools

Alex Smetana

Risks

During our investigation we noted many notably risks.

Reputational Risks were identified. The proposal demonstrates a lack of security measures which have the potential to lead to the exposure PII of the students and staff. PII may include anything information that the students are register with seeing as that there is no software security. This has the potential to ruin the lab and any credibility that the lab has going forward.

Financial Risks were identified. The lack of security poses a high risk of financial loss as well. It seems that the only security measure noted was a bulger system, however, it included no security to the computers. Damage to theft of the computer systems and supplies as well as damage to the parts. This could end costing the lab a lot of money in the long term.

Unintentional Risks were identified. An example includes a natural disaster. For example, fire, hurricane, tornado, or flood. Students and facility also pose the greatest risk due to the lack of security measures enforced. They have the potential to download malware and unauthorized access websites unintentionally.

We have identified the potential risks:

Risk	**Description**
Loss of Reputation	• PII exposure • Damage to lab reputation
Financial Loss	• Damage to the computers • Theft of Computer Systems • Damage to the building
Physical Loss	• Damage to computer hardware • Damage to computer software
Unintentional Risks	• Students • Staff

Threats

During our investigation we noted many notably threats.

The possibility of Malware exists in today's world and the computer lab offers no protection against malware. Examples of malware include viruses, trojans, worms, ransoms, spyware, man in the middle attacks and phishing scams to name a few.

Hackers are another main threat is hackers/cyber criminals. These hackers use the internet to hurt other people on the internet. Hackers can make use of malware as well as SQL injects and password attacks. They have the potential to steal the information of the students as well as the facility.

Students as well as staff are also a threat identified. Students and staff have the potential to download malware as well as other unauthorized software to hurt the machines. The possibility of theft and damage to the lab and computers also exist.

Natural threats exist to the lab. Although unlikely, the possibility of tornados, floods, earthquakes, and hurricanes exist. Although unlikely, we have no idea what mother nature is capable of, and the lab offers no protection against such measures.

We have identified the potential threats:

Threat Source	**Description**
Malware	• Viruses • Trojans • Worms • Ransoms • Spyware • Phishing • Man in the Middle Attacks
Hackers	• SQL Injection • Password Attacks
Students/Staff	• Theft • Malware download
Natural Threats	• Flood • Hurricane • Tornado

During our investigation we noted many notably Vulnerabilities.

Password attacks. Cybercriminals/hackers have the ability gain access to students account by using password attacks. This can be done by either brute force or by phishing attacks. This leaves students accounts at risk to be hacked into.

Access controls. It appears that students can have access to every privilege allowed. Students are also able to access the computers at any time of the day. I it has the potential for dangerous outcomes for the students and the computer lab.

Lack of Documentation. Students who are in a computer lab have no protection in the event of an emergency if the data allowing for no accountability in the event of an emergency.

Use of AV software. The use of AV software is nonexistent in the proposal. This has enormous potential to let in all different types of malwares in the computer lab. This allows for the exposure of PII of the students and has the potential to render computers unusable.

SQL Injection. Hackers are able to hack into databases an manipulation the database and information through SQL.

Lack of Monitoring Traffic. All traffic is allowed throughout the network. Students with access to the entire web can access very shady software that is non-school/ work appropriate. This has the potential to have bad consequences as it introduces the possibility of malware being introduced.

We have identified the potential Vulnerabilities:

Vulnerabilities

Vulnerability	**Description**
Password Attacks	No required password lengths. This will allow for hackers to gain the account information of students.
Access Controls	Students can use the computers at any time of the day. This can lead to students accessing information at hours of the day.
Lack of Documentation	Students and staff’s information is not kept secure.
Use of Anti-Virus Software	The proposal makes no mention of AV software, which can lead to the download of dangerous malware.
SQL Injection	A common use to gain access to a database.
Lack of Monitoring Traffic	Students/Staff are free to browse anything on the web with no monitoring virtually.

-

Risk Assessment

Observation	Threat-Source/ Vulnerability	Existing Control	Likelihood	Impact	Risk Rating	Recommended Controls
Students could access to the entire internet allowing the potential for malware.	Students	N/A	High	High	High	Enable firewalls monitor the traffic flow. Install AV to block malware.
Password requirements are non-existent	Students /Staff	N/A	Medium	High	High	Enable multifactor authentication. Require a password length of a minimum of 8 characters with at lest one capital and special letter.
Lack of documentation for students and staff. Any staff or student is required as “basic knowledge of computer”	Hackers/ Students /Staff	Little	Medium	High	High	Keep track of who is using the computer to hold users accountable.
The computer lab makes no use of AV software, which has the potential for malware.	Students /Hackers	N/A	High	Low-High	High	Enable AV software and block malware.
The lab has no way to insure itself in the event of a natural disaster	Natural Disaster		Low	High	Medium	Purchase some insurance or set aside money in order to prepare for a natural disaster.