Sri Lanka Institute of Information Technology

Physical and Logical Security Vulnerabilities of SLIIT.

Individual Assignment
IE2052 – Advanced Networking Technologies

Nilupul S.A
IT21167478

Contents

Abstract

Identification of the university physical and logical security risks is the goal of this study. This report's major goal is to clarify these hazards' physical and logical nature as well as their avoidance or mitigation options. Moreover, it describes how these circumstances impact the university and offers solutions. To create this report, the researchers also investigated several the proposed security threats.

Physical Security vulnerabilities in SLIIT

1. Unauthorized visitors to the University.
2. Inadequate security in Study Areas.
3. Verification of students' identity at the rear entrance of the university is not mandatory in some instances.
4. Presence of unsecured premises, which may lead to violent incidents such as theft of student equipment or assaults on students.
5. Unsecured shelves for student belongings in study areas.

Logical Security vulnerabilities in SLIIT

1. Visibility of student information while using a university identity card to confirm identity.
2. All the computers in the computer labs are very slow and no anti-virus software is used on the computers.
3. Some software in the computers in the computer labs have not been updated.
4. Intermittent non-functioning or down of servers like eduscope, courseweb etc.
5. The courseweb needs to be improved, students can register as a teacher when registering.

Physical Security vulnerabilities

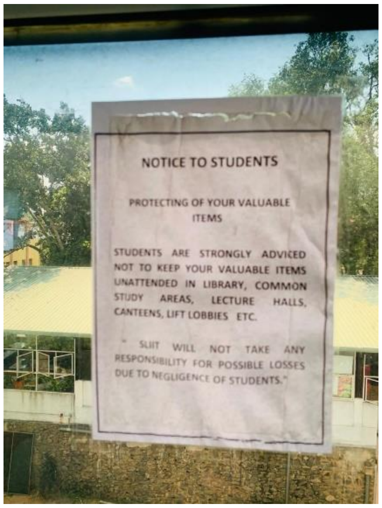
❖ Unauthorized visitors to the University.

The university has two entrance gates. There is another entrance behind the primary entrance at the front. Both these entrances have equipment to check the identity of the people entering the university, but in some cases, due to the carelessness of the security officers and guards, unauthorized persons are allowed to enter the university. And unauthorized people can still enter some areas of the university. (The recent laptop theft was a theft by unauthorized persons) Also, other people enter the university using the identity card of the students of the university. Most of the time it happens due to the carelessness of the security officials.

Solution: Unsecured areas of the university that can be entered without permission should be found and closed, and security measures should be increased by deploying several security officers in the entrance gates.

❖ Inadequate security in Study Areas.

There are several fields of study in the university. Most of the students do their studies in these areas and take their valuable devices like laptops, mobile phones etc. to these study areas. Most of the fields of study I've been to seem to have very little security. CCTV cameras in those stations are not enough and it becomes very easy for someone to steal valuable equipment. A similar theft happened recently. Therefore, the lack of security in academic areas can be seen as a physical vulnerability to the university.



NOTICE TO STUDENTS

PROTECTING OF YOUR VALUABLE ITEMS

STUDENTS ARE STRONGLY ADVICED NOT TO KEEP YOUR VALUABLE ITEMS UNATTENDED IN LIBRARY, COMMON STUDY AREAS, LECTURE HALLS, CANTEENS, LIFT LOBBIES ETC.

" SLIIT WILL NOT TAKE ANY RESPONSIBILITY FOR POSSIBLE LOSSES DUE TO NEGLIGENCE OF STUDENTS."

Solution: The security of those areas can be increased by increasing the number of CCTV cameras in those areas and the security of these areas can be increased by deploying a device for students to verify their identity with their identity card to enter these study areas.

- **Verification of students' identity at the rear entrance of the university is not mandatory in some instances.**

Security at the back entrance of the university is very low. Most of those entrances are unauthorized people entering the university. In some cases there are not even security guards. In some cases, people enter without an identity check. This is very dangerous.

Solution: University officials should be deployed along with the security officers at this entry point as well and should be handled with great attention.

❖ Presence of unsecured premises, which may lead to violent incidents such as theft of student equipment or assaults on students.

There are some parts of the campus that are not captured by any camera. Burglary and violent incidents are very likely in such areas. For example, the area where the swimming pool is made, the back area of the university, some academic fields, etc. are very poorly protected. I see such a station as a physically dangerous station in the university.

Solution: I think security should be increased in these unsafe areas. Also, cameras should be installed in the danger stations that do not have cameras.

❖ Unsecured shelves for student belongings in study areas

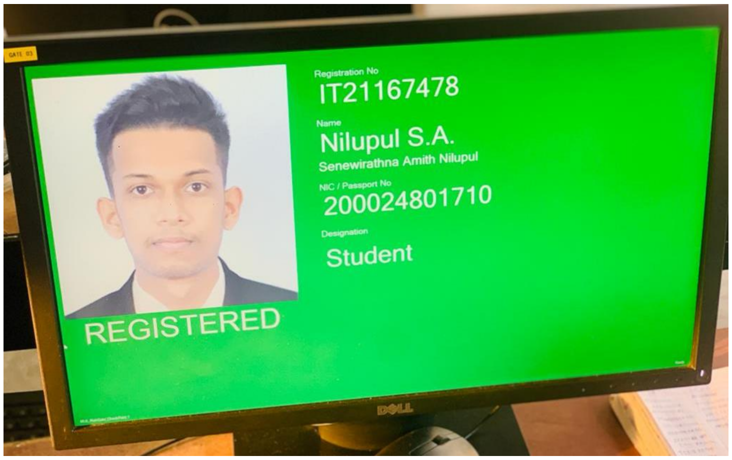
These unsecured racks are an area monitored by only two cameras without any security as far as I have seen. I have seen this a lot in front of the library. Most of the students leave their bags there. I see it here as unsafe.

Solution: This can be solved by providing a locker to all students.

Logical Security vulnerabilities

❖ Visibility of student information while using a university identity card to confirm identity.

It can be seen as a logical security risk to display all the details of the students on the computer screen so that other people around them can see the university ID cards when entering the university to confirm the identity of the students. This is because by taking someone else's details (NIC number, IT number) you can access websites like courseweb, eduscope, netexam.



Registration No
IT21167478
Name
Nilupul S.A.
Senewirathna Amith Nilupul
NIC / Passport No
200024801710
Designation
Student

REGISTERED

Solution: Reducing the quantity of data shown on the computer screen is one way to fix this. The student's name and photo might be shown on the computer screen in place of their NIC number and IT number.

❖ All the computers in the computer labs are very slow and no anti-virus software is used on the computers.

Almost 95% of computers in computer labs are running very slowly. Therefore, students and university staff who frequently use the computer labs may find it difficult to work. This is also a big problem for students. Also, not using anti-virus software on some computers is an unsafe method. Without this protection, systems are vulnerable to malware, viruses, and other security risks that can compromise personal information and cause other problems.

Solution: Hardware and software in the computer lab can be audited to find out-of-date components or programs that may be causing slow performance. To increase performance, funds should be allocated for new computers or other upgrades. And to solve this problem, a comprehensive security policy should be created which requires the installation of anti-virus and anti-spyware software on computers.

- **Some software in the computers in the computer labs have not been updated.**

Students and staff use this outdated software to reduce their time and productivity. Also, since outdated software that is not updated is downloaded in computers, they are weak, so the probability of an attack by a hacker is high.

Solution: To solve this problem, a software update policy should be introduced that requires frequent updates for all software in computer labs. To avoid any disruptions, a policy should be implemented to ensure that updates are implemented quickly and fully tested.

❖ Intermittent non-functioning or down of servers like eduscope, courseweb etc.

The university has several main web servers. The main ones are Courseweb server and Eduscope server. The Courseweb server contains data and information about all internal activities of SLIIT including lecture materials, timetables, announcements and more. And the server in Eduscope server is also in high demand. Professors and instructors often upload lecture recordings of every module belonging to all faculties. In some cases it is not possible to login to these two websites. Servers are down. This can be a big risk to information.

Solution: By making the web server network more resilient, this risk may be avoided. This denotes the placement of servers in several data centers, all of which must be physically situated nearby and connected to various networks. All network traffic will be sent to a single web server as a result.

❖ The courseweb needs to be improved, students can register as a teacher when registering.

Another vulnerability I have seen is that when registering on courseweb, there is a separate registration for students and a separate registration for teachers. But when I researched I came to know that students can also register as a teacher. When registered as such, a teacher gets access to all things (actions not accessible to students). This is a big risk.

Solution: This can be solved by giving students and teachers an access code to register and updating it on courseweb and updating the courseweb website and not giving students access to the teachers side.

References

- https://courseweb.sliit.lk/
- https://www.openaccessgovernment.org/security-vulnerabilities-education-sector-risky-business/152902/
- **I found out a lot of information by visiting and monitoring risk area at the university.**