IT security analysis of information technology center at Sayed Jamaluddin Afghani University

Rafiqullah Baryalai

University of Sayed Jamaluddin Afghani, faculty of Computer Science, Asadabad, Kunar, Afghanistan

Abstract
Security of Information Technology is one of the important issues in the field of IT, therefore the main purpose of this paper is the IT Security analysis of Information technology Center at Sayed Jamaluddin Afghani University. As the information Technology center is the core and vital department for the University because all the valuable and confidential data of University is store in information technology center (ITC), so the protection of Hardware, Software as well as physical and logical security of Information Technology Center is indispensible, The paper Covered some general physical and logical IT security issues that many Information technology or data Center faces that. beside this the paper analysis the Current security situation of Information Technology Center at Sayed Jamaluddin Afghani University, that Mostly covered the Building Security of Information technology Center, prevention of Dust intrusion, Temperature and humidity Control, Building electrical wiring, Requirements of the rooms. And find out Many vulnerabilities, weaknesses and security holes such as: the Building of Information Technology Center was insecure inside the building all Hardware and software were not safe the paper suggested some possible solutions to the above mentioned security problems that will secure and safe the Information Technology Center (ITC) of Sayed jamaluddin Afghani University.

Keywords: IT security, information technology center, building security, Sayed Jamaluddin Afghani University

Introduction
IT Security
This is important to know that "It is the aim of IT security to protect IT processes in teaching, research, and administration from threats on a large scale and to prevent misuse in order to guarantee the working ability and to preserve the reputation of the institution" [5, 6]. There are three main IT security objectives Confidentiality, Integrity, and Availability of data. "Confidentiality is protecting access to sensitive data from those who do not have a legitimate need to use it. Integrity is ensuring that information is accurate and reliable and cannot be modified in unexpected ways. The Availability of data ensures that is readily available to those who need to use it "[10]. It should be considered when we are talking about IT security. To establish IT Center there should be consideration about physical security as well as logical IT security. physical security for the IT Center is Building, offices, equipment, employees, critical data, storage, and etc. the building of IT Center Should be secure, there should be secure walls and entrance and exit secure doors, there should be security system for the IT center such as security cameras and security guards. building security. It is important to mention that weak Building security can open the way to the theft, bad people and any other threat to create a problem as example you can see the weakness of building as following

Building Security
Security and protection of the IT Building are important IT building must be protected against external and internal hazards such as theft, lightning etc. And the construction of the IT building must be checked by IT building specialist to consider or observe deficiencies-ceilings, roof, rainwater, resistance etc. And further deficiencies like improper execution in the building process or even respect to

corruption [6, 19]. The protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, man-made catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders [1, 13]. The building security is very important issues but unfortunately in Afghanistan due to the lack of security knowledge and security policy, there is no good security system for building everything is manual and traditional and there is no strong consideration about security like cameras, sensor devices, and automatic authentication system. If you see today modern and standard IT building it has to computerize intelligent system many cameras, sensor devices and automatic authentication systems are installed that is more secure and safe. As (Kakar, 2010) [14] mentioned the building security for Information Technology Center of Kabul (ITCK) and Information Technology Center of Herat (ITCH) are a responsibility of universities administrations and there are receptions in the main entrance of the centers. Everyone who wants to enter the center has to register and put his or her backpack and any other materials with the reception. The reception can also check and observe the person who is leaving the IT center. Besides this, the guard and reception have to discourage everybody from unsocial activities like theft and damaging equipment. Regarding the burglary, the building needs to be protected with secure doors and windows. The doors and windows which are cracked are vulnerable to the break-in. the doors and windows also need to be reinforced against dust. The doors and windows all need to be removed and reinstalled. The main entrance door should be enough strength to prevent theft and dust intrusion.

The dedicated building of IT center in Sayed Jamaluddin Afghani University is in good security location, but still need more about security the IT building That is located on the university campus so there is one main entrance door for the university so when someone want to get IT Center then he or she need to pass first main entrance door of University and then inside again he or she need to pass another internal entrance door for IT Center. The second internal entrance door for ITC is made of metal and impossible to break but inside building doors and windows are not in standard level it needs to be reinstall, and all locks of the doors and windows wardrobe must change, alarm system, have to install walls and ceilings have to repair, diesel generator have to be outside from IT building, there should be some security policy for IT Center building, there should be restriction about smoking, eating food, drinking etc inside the IT building or rooms. because those can cause damage to the building as well as equipment. There should be guards to check the user when gets inside and outside from the IT building the most important things for IT building security is public awareness. There should be some way to make all the users of IT building aware about security, for example, there should be some banner pasted to the walls of security, and there should be presentations regarding security awareness from the IT Center staff once in the week or in a month. One person receptionist should be there to register the user or visitor to recognize who got inside and who left if some things wrong happen then receptionist can easily detect the one who created the problem. To have a best IT center building and equipments security system it has to fulfill the following Steps:

Herlitz, (2001) [13] explained: there should be a fence around the facility at least 20 feet from the building on all side, there should be a guard Kiosk at each perimeter access point, there should be and automatic authentication method for IT center employees (such as a badge reader reachable from a car).for the time being or present and initial time it would be impossible due to the lack of full time electricity as well as knowledge but it should be future plan for Sayed Jamaluddin Afghani University IT center. There should be CCTV cameras outside the building monitoring parking lots and neighboring property. There should be guards patrolling the perimeter of the property. Vehicles belonging to data center employees, contractors, guards, and cleaning crew should have parking permits. The building should not have window to outside placed in computer rooms. Such window could provide access to confidential information. The windows also cause sunlight on servers unnecessarily producing heat to the computer rooms. Computer rooms should be within the interior of the data center. If a computer room must have a wall along an outside edge of a data center there should be a physical barrier preventing close access to that wall. There should be signs at the doors making the room as restricted access and prohibiting, food, drink, and smoking in the computer room, there should be and automatic method at the entrance to the room (such as a badge reader), door should be fire proof., access should be restricted to those who need to maintain the servers or infrastructure of the room. access should be restricted to emergency access only during moratoriums for holidays. Computer room should have air filtration; computer room should have high ceilings to allow for heat dispersal. Each computer room should have temperature between 55 and 75 degrees Fahrenheit and a humidity of between 20 and 80

percent. (Safeguarding, 5:2) [1] Environment sensors should log the temperature and humidity of the room and report it to the NOC (Network operation center) for monitoring and trend analysis here must be fire extinguishers located in each computer room, there must be emergency power off switches inside each computer rooms. There may be respirators in computer rooms. There must not be wet pipe sprinkler systems installed. Computer equipment in shared spaces must at a minimum be in a locked cabinet. There should be cooling system in data center, there should must at least be battery backup power on site with sufficient duration to switch over to diesel power generator if there is no diesel backup then there should be 24 hours of battery power. There should be diesel generators on site with 24 hours of fuel also on site. A contract should be in place to get up to a week of fuel to the facility. The data center must have a disaster recovery plan. [3] Described: the walls of the building should be well protected against theft etc avoid windows if you must have windows, limit them to the break room or administrative area, and use some resistant glass in window. Limit entry points, control access to the building by establishing one main entrance, this keeps costs down too. make fire doors exit only, for exits required by fire codes, install doors that do not have handles on the outside, when any of these doors is opened, a laud alarm should sound and trigger a response from the security command center. Use plenty of cameras surveillance cameras should be installed around the perimeter of the building, at all entrance and exits, and at every access point throughout the building. Protect the building machinery; keep the mechanical area of the building, which houses environment systems and uninterruptible power supplies, strictly off limits. If generators and repair crews are accompanied by an employee at all times. Use authentication system like Biometric identification is becoming standard for access to sensitive areas of data centers. Install a visitor rest rooms. make sure to include bathrooms for use by visitors and delivery people who do not have access to the secure parts of the building.

Prevent dust intrusion

75% of Hardware is caused by dirt and dust. The dust can cause very bad harm to the IT related equipments it can cause a major risk of fire hazard. The IT Center needs an effective strategy to prevent dust and particle contamination [15]. As this is clear that all IT related equipments are very sensitive with dust so in this regard it is better to strongly consider this, the building which is dedicated to the IT Center in Sayed Jamaluddin Afghani University is a bit close to the main road of Asadabad city and vehicles are causing dust so in this case it is better to have different ways to prevent or avoid the dust from the IT building the cleaner have to keep around of the building clean and also have to regularly drops the water around the IT building through water pipe another way is "the only weak spot from which the dust can easily enter is the doors and windows need to be reinstalled with better quality"[14]. There are some other important steps for preventing dust as following

- There should be super-sensitive smoke detectors system,
- There should be Alarms blaring in ITC it is of course, best avoided,
- There should be trash around IT Center building. Cabinet should be locked properly,

- There should be some soft or hard copy PDF instructions to cleaners,
- IT Manager has to have instruction to cleaners,
- When the user getting in or leaving from IT C they have to close the door and windows
- properly,
- There should be cleanliness policy posted and make sure all employees are aware of them,
- The people who are entering to IT Center have to take off the shoes and dirty cloths,
- There should not be allow the user to eat food, drinks smoke etc,
- There should be regular cleaning schedule,

Each computer room should have temperature between 55 and 75 degrees Fahrenheit and a humidity of between 20 and 80 percent (Safeguarding, 5:2) [1].

Table

Items	Equipment conditions		
Equipment status	Equipment in operation	Equipment not in operation	Recommended
Ambient temperatures C	15-32	5-45	18-27
Humidity(%RH)	20-80	20-80	60%RH or lower data center must follow conditions 5.5-6.0 C DP

Tolerances for ambient temperature and humidity[1] [1]

Building electrical wiring
Proper electrical infrastructure (wiring and cabling) is important for any building especially for IT building because in IT building there is very sensitive and expensive IT related equipment and hardware is available if the IT building is wired improperly then "any short circuit will cause serious damage to the hardware and information within the hardware. And also can cause the fire in the building which needs to be protected"[14].in this case it would be better to have electrical wiring specialist and professional to set up electrical infrastructure by proper and the standard way which will be saved and protected. Sayed Jamaluddin Afghani University IT building need to be wired by electrical infrastructure the building is independent and isolated from the other building of University it is possible that "the electrical wiring must be of three phase to distribute equal and stabilized power to supply each room and system stable power. Each room must be protected with short circuit fuses in order to prevent damage to the equipment due to short circuits" [14]. the quality of electrical cables, Sockets, Circuit boards, fuses, switches and etc are a crucial issue to consider if you do not consider the good quality electrical tools it may damage very soon and create a problem which will be insecure and that will be really a big headache for future use and beside that the good and proper set-up of wiring and cabling is important it must be correct.

---

[1] Source: "FUJITSU",
www.fujitsu.com/downloads/PRMQST/documents/PQ-Gaseous-particulate-contamination-Guidelines-Datacenter.pdf,pp, 2-2, june 2016

Requirements of the rooms
All the requirement of the rooms in the building is important, it is better to bring the example of rooms requirements which Peroz, (2009) [5, 6, 18] Stated that must be applied.
- Secure entrance door.
- Renovate of the security personnel room.
- Wardrobe and lock boxes.
- Reception table for the registration of users.
- Carpet.
- Lighting.
- Chairs and tables.
- Air conditions or fans.
- Stable power connections and secure power supply.
- Cable channels.
- Network cabling.
- Server racks in the server room.
- Air condition in the server room.
- Curtains for windows.
- Stable fire protection.
- Fire extinguisher.
- Dust sealing for all windows.
- Water dispenser.
- Electric broom.

The above-mentioned requirements for the rooms are indispensable there must be secure entrance door the locks of the door must be new and strong, there must be windows with good and secure condition of locks, the rooms should be well carpeted which do not deposit dust, there must be tables and chairs according to the requirements of the rooms, there should be Air conditions or Fans, there should be wiring and network cabling system in all rooms for the computers, printer etc., there should be stable power supply system and electrical wire infrastructure for all the rooms, there must be Server rack in the Server room as well as Air condition to keep the temperature of the server room normal, there should be ventilation system, suitable Curtains for the windows and doors, Fire protection system, alarm system, water pipe infrastructure, electrical broom for the dust, etc. the dedicated building of IT center for the Sayed Jamaluddin Afghani University is old and all the building especially rooms need renovation and before establishing IT Center all the above mentioned requirements mush be applied for the rooms because currently the rooms requirements are not fulfilled in Sayed Jamaluddin Afghani University IT Center building. the doors and windows need to be repair, electrical wiring, and network cabling system need to be set-up, water pipe infrastructure need to be set-up, walls, ceilings and roof of the rooms need to be repair and coloring, security system, fire protection system, ventilation system, alarm system, and all other requirements and systems need to be set-up. Now the question is budget, who have to support budget for all these requirements so far there is no budget for it. the solution will be that Sayed Jamaluddin Afghani University and Ministry of Higher Education (Mo HE) have to provide the budget for it and beside this my suggestion is that they have to request some foreigner organizations or donors like world bank, DAAD, USAID and others to support the budget then it will be possible to fulfill all the requirements of the rooms and establish the IT Center and its Security System at Sayed Jamaluddin Afghani University.

Fig 1: Building security [3].

The Offices and rooms of IT Center should be secured, there should be restriction on unauthorized or unfamiliar people to enter the offices or rooms without permission of Authority each employee of the office should keep the door and windows close when he/she leaving the rooms or offices, each employee should be responsible for keeping all sensitive data or devices secure, Critical and stored data devices like CD/DVDs, USBs, hardcopy files or documents and all physical IT related devices should be secure and safe. There should be the strong attention of employees to it, there should be strong consideration about security holes or weakness you can see the insecure example of it in the following Diagram.

Fig 2: Insecure office Example [3].

1. Doors and windows are open: Computer and equipment are free gifts for every thief,
2. Monitor shows secrets,
3. A sheet of paper with passwords,
4. A CD-Rom with Backup written on it,
5. Prints and copies with confidential information are open to see for everyone,
6. Computer with connection to the internet without firewall protection,
7. Private CD-ROMs can infect the Campus network with Malware,
8. Fluids are dangerous to Hardware,
9. Smoking may light the fire, [3, 9, 10].

Logical security of IT Center is another important Issue that need highly consideration. it means that electronic data is not 100% safe because of vulnerability, therefore it must be considered to protect the data from vandalism, loss, Misuse, Malicious destruction, and theft, as well as from incorrect use and loss due to technical malfunction [5, 6, 18]. Thus, Operating System (OS) of Servers, Desktop, Laptop and all other IT Center devices should be secured from unauthorized users as well as internal and external attacks and threats. Such as external hacker, Malware infection, Human errors so on. The resources which really need security should be specified As Peroz, (2009)[18] Recommended It is recommended that both the ministry of Higher Education and the universities collaborate on an IT security directive. It is the job of the CIO's, in collaboration with the IT security officers, the Ministry, and the universities, to work on a proposal which should contain the following elements:

▪ Determining the resources that have to be protected,
▪ Taking appropriate measures in case of resources,
▪ Commitment to documenting the IT resources,
▪ Duty to report security incidents,
▪ Training of system administrators and IT users.

Now to apply the IT Security for the Sayed Jamaluddin Afghani University IT Center, it is challengeable because, up to now the system is traditional and lack of IT in university. The staff of University is unfamiliar with the modern IT system they even do not know that what is Server, router, and as whole IT Center and how it work. And how the IT security is important therefore there should be high consideration of MoHE and University of Sayed Jamaluddin Afghani that means before establishing of IT Center there should be some basic training about IT security. Suggestions there should be specific security team who just responsible for the security purposes and Mo HE should provide facility and professional IT security training to them and have to train them well, then after that this team will be able to train other staff of IT center as well as University administrative staff and others. There should be security awareness program because by the help of security awareness it is possible to reduce the security risk, there should be security policy for both physical as well as Logical security for the IT Center. And Manager of IT Center will be responsible for writing security policy for the IT Center use.

Infrastructure
Building
The University of Sayed Jamaluddin Aghani (SJAU) has building for establishing ITC. But the building is a bit old to have a standard and modern building according to the norms of IT then it needs Renovation or Repairing, and furnishing. Such as The building walls, Ceiling, windows, doors, colors, Carpets, electricity wiring, bulbs, water pipe infrastructure locks and every other related thing of building need to be repaired to be clear it is important to strongly consider the building repair for IT Center. As Peroz (2009) [18] mentioned: Currently, most of the buildings and rooms at Afghan Universities and faculties are not suitably equipped for the use of IT, For the use of computers and servers, the buildings must be secured and protected against dust, coldness, heat, and theft. To construct or repair the building it is advisable to interest a local and skilled building

specialist with checking the building for possible serious deficiencies, since the danger of collapse and insecurity against earthquakes will need to be ruled out beforehand, the additional consultation of a specialist is optional. Yet, this specialist could also be helpful in controlling the process of grounding and installing the lightning rod. For the establishing IT Center the renovation is indispensable because Since we are planning to create a Physical Topology inside this dedicated building and place a Server Computers Which will control and will be the main Storage System of this ITC, so in order to apply the topology we need to accomplish wiring where they would be safe from physical damage so we need cable channels to put wires through them. And since a server is the main storage system and the controlling center, so the server must physically and logically secure.

- By physically means that it should be safe from natural and human causing damage like rain, breaking up and so on.
- By logical means that it should be secured from unauthorized users.

The IT equipment and computer hardware are very fragile and sensitive to dust, heat, and cold. And also the misuse of IT and computer equipment are creating problems, as well as theft and burglary within the building and the premises of ITC. As result, protection measures are to be taken into consideration to protect the equipment from the mentioned threats [14, 17].

Results and Discussion

Security of Information Technology Center (ITC) is the requirement of 21 Century for each administration especially for the Universities, therefore in this paper the IT Security for the protecting and securing of Information Technology Center at Sayed Jamaluddin Afghani University has analyzed and discussed and the following result has been achieved: at current time the University do not has any Security system and security policies for the Information Technology Center, Beside that there were lack of IT Security Professionals and Expert staff, IT Security public awareness, IT Security Education, etc… in the University 75% percent of formal personnel has the lack of Security knowledge and risks just 25% percent of University staff had public awareness about the risks of information Technology Center and all IT related Hardware that was belong to Computer Science staff. everything was Traditional and there was no any good security system, Most of the personnel was complaining from the damage of important Hardware and data that faces Many Problems due to the performance of good services, bad economic state etc… to overcome all above mentioned problems it needs to establish Security policies for the Information Technology Center, IT Security Trainings for the University staff, hire IT Security professional staff, now the Big Challenge is Budget for the establishment of Security policies, Therefore I have Developed General IT Security Concept and possible solutions to secure and safe The Information Technology Center (ITC)at the University of Sayed Jamaluddin Afghani. Staff Salaries: this is the first challenge, because in Afghanistan the IT is new, there are lack of IT Security professional and expert staff and very rare expert are available to hire, another problem is at the moment IT expert has very high expectation of Salary and university could not provide very high salary for the lack of Budget, in this regard the government of Afghanistan especially Ministry of Higher Education need to pay Strong Consideration of IT Security Professional staff Salaries, because without IT Security Professional it is impossible to protect the Information Technology Center. Electricity /Power supply: as the power is the soul of Information Technology, therefore this is another Budget Challenge of Information Technology Center, Currently in the University there is lack of Stable power supply, in this case at the moment Solar power system is the Best solution Hence a source of fund is required to supply sustainable power supply for the IT Center. It would be better to find fund and estimate budget to provide solar power for IT center. Solar power though requires High initial investment but very low running cost. It is most suitable for IT center. Internet: Secure internet is another indispensable Requirement of Information Technology Center that to find out the sustainable source of fund for it, if the University request the Ministry of Higher Education and some NGOs and donors to Convince them that Financially support the each part of Information Technology Center such as: Building security, IT Security Staff Salaries, Secure Internet, Maintenance of ITC, Power Supply, Multimedia, New Software and Updates, Hardware, installation/Configuration etc… but the main solution for the IT Security purpose Budget Plan of Information technology Center is the requirement of sustainable support, therefore for the whole Information Technology Center it will be better that University have to have special budget for the Security of Information Technology Center.

Conclusion

This Paper developed the IT Security concept for the Information Technology Center at Sayed Jamaluddin Afghani University for this purpose the challenges and problems of IT Security has been mentioned and possible solutions are suggested, like the Creation of Security Policies, Stable power supply system, the Secure Internet, hardware and software Security for the Information Technology Center. building security, renovation of building and requirements of the rooms, electricity and software use and all other Security requirements of Information Technology Center has been point Out. beside these the general IT Security for the organizational structure and staff for the Information Technology Center who need to operate the Information Technology Center safely, like Manager of IT Center technical staff, (system administrators, Network administrator, database administrator, application administrator, electricity as well as hardware support technical staff),IT education like lecturers and tutors. And guards and cleaners for the IT Center security purpose explained. Beside these the Building security, stable electricity, protection of dust intrusions, Temperature and humidity Control, room protections and Hardware and Software Security both Physical and logical Security for the Information Technology Center has covered. Famous examples of Security related have mentioned and all the vulnerability, weaknesses and security holes has been explained with elaborations and possible ways and solutions has suggested. To conclude that in this paper the main concentration was on General IT Security of Information Technology Center, that Shown the possible ways of multiple solutions to the

Current Challenges and problems, if the University applies this suggested solutions of IT Security for the Information Technology Center, then it is possible to Protect the information Technology Center and important data of Information Technology Center at Sayed Jamaluddin Afghani University.

References

1. Catalogues IG. Bundesamt für Sicherheit in der Informations technik (BSI), 2015.
2. Marshall G, Ruohonen M. (Eds.) Capacity Building for IT in Education in Developing Countries: IFIP TC3 WG3. 1, 3.4 & 3.5 Working Conference on Capacity Building for IT in Education in Developing Countries 19–25 August 1997, Harare, Zimbabwe. Springer Science & Business Media, 1998.
3. Scalet SD. (19). Ways to Build Physical Security into a Data Center. CSO Security and Risk, Data Protection How-tos. Retrieved on, 2016. From http://www.csoonline.com/article/2112402/physical-security/physical-security-19-ways-to-build-physical-security-into-a-data-center.htm
4. Mahr B, Peroz N, Balschun A, Hoffmann E, Suhr J, Tippmann D. Establishing Academic Structures in Computer Science at Herat University. IKO Verlag, 2006.
5. Peroz N. Establishing IT Structures at Kabul University. IKO, Verlag für Interkulturelle Kommunikation, 2008.
6. Peroz N. Framework for a Functional IT Supply in Higher Education in Afghanistan LIT Verlag Münster, 2009, 63.
7. Safi A. Sayed Jamaluddin Afghani University: History, Development and IT infrastructure. Sayed Jamaluddin Afghani University, 2015.
8. Ministry of Communication and IT of Afghanistan, ICT POLICY FOR AFGHANISTAN: A digital agenda for development and social change, 2015. Kabul: MCIT. Retrieved from http://mcit.gov.af/Content/files/Draft-ICT%20Policy%20Document.pdf
9. Tipton HF, Krause M. Information security management handbook. CRC Press, 2003.
10. Feinman T, Goldman D, Wong R, Cooper N. Price water house Coopers L L. P. Security basics: a whitepaper. Resource Protection Services, PricewaterhouseCoopers, London, 1999.
11. Noorzai R. Communication and development in Afghanistan: A history of reforms and resistance (Doctoral dissertation, Ohio University), 2006.
12. Hamdard J. The state of telecommunications and internet in Afghanistan six years later 2006-2012. USAID Assessment Report, 2012.
13. Herlitz R. Qualification of lecturers for the establishment of Computer Science faculties at Afghan universities. Berlin: Technische Universität Berlin, 2009. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.507.4092&rep=rep1&type=pdf
14. Kakar, Abdul Sattar. A Concept of an IT Center in Kandahar University. Berlin: Technische Universität Berlin, 2010.
15. Khadka G. Innovation and information technolgy (Master Thesis). Roskilde University, 2014.
16. Da Silva LF, E Abreu FB. Patterns for IT Infrastructure Design. In Proceedings of Euro PLoP, Irsee Monastery, 2010.
17. Baryalai, Rafiqullah. Developing a concept to establish an IT center at Sayed Jamaluddin Afghani University in Kunar/Afghanistan, 2016.
18. Peroz N. 10th IT Conference: Information Technology for Higher Education in Afghanistan. Berlin: Technische Universität Berlin, 2015. Retrieved from https://www.ziik.tu-berlin.de/fileadmin/fg53/ZiiK/ZiiK_Reports/ZiiK_Report_Nr.37.pdf