International Journal of Hybrid Information Technology
Vol.9, No.4 (2016), pp. 281-290
http://dx.doi.org/10.14257/ijhit.2016.9.4.24

Risk Management Policy of Telecommunication and Engineering Laboratory

Abdul Salam Shah[1*], Muhammad Fayaz[2], Asadullah Shah[3], Shahnawaz Shah[4]

[1]SZABIST, Islamabad, Pakistan
[2]JEJU National University, South Korea
[3]International Islamic University Malaysia (IIUM), Malaysia
[4]University of Sindh, Jamshoro, Pakistan
[1]shahsalamss@gmail.com, [2]hamaz_khan@yahoo.com,*
[3]asadullah@iium.edu.my, [4]shahnawaz@usindh.edu.pk

Abstract

The Telecommunication laboratory plays an important role in carrying out research in the different fields like Telecommunication, Information Technology, Wireless Sensor Networks, Mobile Networks and many other fields. Every Engineering University has a setup of laboratories for students particularly for Ph.D. scholars to work on the performance analysis of different Telecommunication Networks including WLANs, 3G/4G, and Long Term Evolution (LTE). The laboratories help students to have hand on practice on the theoretical concepts they have learned during the teachings at the university. The technical subjects have a practical part also which boosts the knowledge of students and learning of new ideas. The Telecommunication and Engineering laboratories are equipped with different electronic equipment's like digital trainers, simulators etc. and some additional supportive devices like computers, air conditioners, projectors, and large screens, with power backup facility that creates the perfect environment for experimentation. The setup of Telecommunication and Engineering laboratories cost huge amount, required to purchase equipment, and maintain the equipment. In any working environment risk factor is involved. To handle and avoid risks there must be risk management policy to tackle with accidents and other damages during working in the laboratory, may it be human or equipment at risk. In this paper, we have proposed a risk management policy for the Telecommunication and Engineering laboratories, which can be generalized for similar type of laboratories in engineering fields of studies.

Keywords: *Assets Identification, Risk Management, Telecommunication Laboratory, Risk Assessment, Hazards, Risk mitigation, Risk Analysis.*

1. Introduction

The experimental learning is essential for Engineering and Telecommunication programs of study. The practical learning allows students to understand the theoretical, technological, scientific and quantitative concepts of Science and Engineering by conducting experiments, observing the changing phenomena'~~s~~, testing hypotheses, and after doing mistakes learning from them, so that the same can be avoided in future for achieving the desired results and conclusions [1][2].

The research is most important in every field of sciences may it be Biology, Engineering and Telecommunication or Computer Sciences, almost every postgraduate degree has the requirement to develop a research project, thesis, dissertation, case study, independent studies to graduate [3]. Every Engineering university has Laboratory to facilitate the students carrying out research in Electronics, Telecommunication, and Engineering [4].

*Corresponding Author

ISSN: 1738-9968 IJHIT

The students of other fields like Artificial Intelligence, Machine Learning, Data Mining, Image Processing, Electric Circuit Analysis, Digital Logic Design, Digital Electronics, Analog Electronics, Network Analysis, Cloud Computing, and Software Engineering also get benefit from the laboratory [5, 6, 7, 8 and 9]. The laboratory usually contains CPAL Telecommunication Trainers, Function Generators, Oscilloscope, EPAL Trainers, Microprocessors, Microcontroller Interfacing Stations, Microcontrollers and Kits, Field-Programmable Gate Array (FPGA), Digital Multi Meters, and Digital Storage Oscilloscope [4]. These laboratory equipment are expensive and needs to be handled with extra care by proper risk management policy that can tackle the risks associated with equipment, there are a varies of risks, it can be, damage, theft, explosion, fire, short circuit and many others [10].

The main objective for all universities and institutional organizations must be to deliver a reliable mechanism for the risk management of all the possible activities of an organization, for the reduction of the possibility and impact of all kinds of mishaps that can happen during working in an organizations or workplace. The identification of the hazards and the risks associated with the activities to be performed during working in the laboratory are important to make the workplace safer and reduce the risks of injury and equipment damage [11]. The possible hazards around the workplace can be of different types having a different potential level of damage ~~t~~hey cause to the equipment. There are various types of risks, these can be divided into fixed, obvious, hidden and developing risks. These all types of risks need~~s~~ to be recognized, and by taking necessary steps needs to be decreased or, if promising, to be eliminated [11].

In this paper, we have identified and considered some visible and hidden risks associated with the telecommunications laboratories and on the basis of that, proposed a risk management policy. The proposed policy is given in the subsequent section. Before going to propose risk management policy, it’s important to discuss the few important terms here to build up a background for better understanding of the terms and their importance and functioning.

Risk Management: The risk management is a predefined set of accomplishments and approaches that are adapted to bound a particular organization for controlling the associated risks that can decrease the performance of the organization and create obstacles in the way of organizational targets or goals. According to ISO 31000 2009 the risk management is an architecture for the management of possible risks. The components of the architecture include risk management principles, a risk management framework, and risk management process [12, 13, 14, and 15].

Risk Management Framework: The risk management framework as defined by ISO 31000 is a mechanism that helps and sustain the overall process that an organization follow~~s~~ for the possible risks and their management to reduce and avoid the risk that can cause the losses or have any negative impact on the overall objective of the organization [16].

Risk Management Policy: The organization's assurance to risk management and understanding of its general intention or direction for the management of risk is known risk management policy statement.

Risk Attitude: The organization’s general approach to risk is known as risk attitude. It defines that how the risks associated with particular organization are taken, on what priority they are assessed, at what level they are tolerated, how they are retained, if the organization prefer to share the risk then how they are shared, which precautions are adopted for the reduction or avoidance of risk, and addressed. In case if some organization does not implement the risk treatments measures than this also comes to the risk attitude of that particular organization.

Risk Management Plan: The risk management plan defines the steps and procedures that the organization adopts for the management of risk. The description contains the constituents, approach, and resources that will be utilized for the management of risk. The main components of the plan include procedures, practices, responsibilities, and activities.

Risk Owner: The person who has given the authority for management of particular risk and is responsible for doing so is known as risk owner.

Risk Management Process: The ISO 31000 defines as management policies, procedures and practices are systematically applied through risk management process.

Establishing Context: The definition of internal and external parameters that organizations must consider while managing risk.

External Context: The external context includes all the external environmental aspects that influence the risk management and the way to achieve the objectives.

Internal Context: The Internal context includes all the internal environmental aspects that influence the risk management and the way to achieve the objectives [16].

2. Proposed Risk Management Policy

The consistent mechanism for the risk management of all activities of an organization is most important in order to reduce the mishaps of all kinds. To make a workplace safe, the identification of hazards and assessment should be performed. The scope here is limited to just a Telecommunication and Engineering laboratory. There are different types of hazards in and around the workplace. e.g. Fixed, obvious, hidden and developing [17].

2.1. Purpose

The main purpose of this risk management policy is to reduce the risk at university's Telecommunication and Engineering Laboratory that can affect the mission and objectives of the institution.

2.2. Scope

The scope of this policy is limited to the Telecommunication and Engineering laboratory.

2.3. Hazards

A hazard can be a condition or situation that has the potential to cause loss, injury or illness at the workplace.

2.4. Risk

The risk is a measure of probability and potential of a hazard resulting in loss, injury or illness. We operate in a condition of uncertainty everywhere, in labs, offices, roads, etc. The ISO 31000, standard describes the risk as "effect of uncertainty on objectives" the effect can be positive as well as negative. With every objective, there is risk associated and it is not necessary that the things will go perfectly as we planned. All the steps toward the goal have associated a different kind of risks, sometimes we achieve the positive results and sometimes negative, and to tackle with these issues it is important to design a strong risk management policy to reduce the uncertainty and the risks to achieving positive results. The uncertainty is a deficiency of information about the event, consequence that leads to incomplete understanding.

The estimation of risk can be carried through a combination of the probability of occurrence of harm and the severity of that harm. There is always a risk associated with every process it can be high or can be low, but it can never be zero [18] [19].

For the management of every risk, first there is a need, to identify what cost-effective countermeasures can be applied. These countermeasures vary from organization to organization, it depends on their priority. The possible countermeasures are [20]:

2.4.1. Avoiding the Risk: The avoidance would mean stopping the activity that is causing the risk. For example, switching off all the switches before leaving the laboratory would avoid the risks associated with the electronic equipment's computers, trainers safe from any damage due to fluctuations of electricity [20].

2.4.2. Modifying the Risk (Likelihood and/or Impact): The modification of risk includes the selection and implementation of best possible security mechanism that reduces the likelihood of a successful attack and mishap, or the impact that would result from such an attack. For example, installing the circuit breakers with every equipment in the laboratory and with the main circuit will reduce the risk. Similarly, by installing an up to date antivirus application can prevent the attacker from using malware to gain access to the computer holding the critical data about the experiments of students and protecting the data with passwords will also keep the data safe from unauthorized access [20].

2.4.3. Transferring the Risk to others: The risk is mostly transferred to the other companies which offer insurance service and most of the organizations which contain critical and costly equipment and perform under the conditions of risk prefer insurance coverage. The laboratories which contain costly equipment can also be insured to transfer the risk from owner to insurance companies. The laboratory of university is small so the risk transferring option is not suitable in the case of Telecommunication and Engineering Laboratory.

2.4.4. Accepting the Risk: The risk Acceptance would mean choosing not to implement any of these countermeasures, choosing instead to monitor the asset for any attacks and possible damages in the laboratory [20].

2.5. Asset Identification and Classification

Before risk management and risk analysis, the step of the assets identification and classification is important this helps to list down the all possible assets available in the laboratory and in future the same list can be used for the verification of the assets at the time of the audit. In the classification of assets on the basis of the risk level associated with them and also their importance in the functioning of the laboratory, the assets are classified into critical and non-critical here.

2.5.1. Assets Identification: In the asset identification phase, the assets of Telecommunication Laboratory are listed down in the form of a document which includes all the tangible and intangible things. This list cannot be the final list as the equipment's can be in hundreds if all of them considered, but here few of them are enough for the understanding and guideline. In Case of Telecom, Lab assets are [4].

- Computers
- Telecommunication Trainers CPAL
- Function Generators
- Oscilloscopes
- EPAL, Trainers
- DSP kits
- Digital Multi-Meters
- Voltmeter
- Electronic Switches
- Networking Switches
- Keyboards
- Mouse
- Chairs
- Computer Tables
- Purchased Software's
- Projectors
- Tube lights

- Hard disks
- RAM

2.5.2. Classification of Assets: The identified assets can be classified into two categories on the basis of their importance and impact on the working of and organization. These assets can be further classified/divided on the basis of the level of criticality but here two categories are considered i.e. critical and noncritical assets [17].

Critical Assets: The critical assets are those assets that let down the entire system in the case of failure, these are also known as red-zone. These include, the electricity, computers, and electric switches [17].

Non-Critical Assets: The Non-Critical assets are those that do not let down the entire system like the critical. These include the chairs, tables and lights.

After the assets identification and classification into critical and non-critical the actual risk management process starts.

2.6. Asset Management

The process of risk management is divided into three steps i.e. Risk Assessment, Risk Analysis and Risk Mitigation [21].

2.6.1. Risk Assessment: The purpose of risk assessment is to identify the activities actually taking place and their respective risk levels. The risk assessment is further divided into three processes, i.e. risk identification, risk analysis, and risk evaluation [21].

Risk Identification: In this phase, the possible risks are identified and described the nature and potential of risks that how much they can affect the achievements of objectives of an organization [21].

Risk Analysis: In this phase, the risks previously identified are analyzed to understand their nature, their sources, and cause of the risk and try to estimate the level of risk [21].

Risk Evaluation: In this phase, the risk analysis results are compared with the risk criteria for the determination of the specified level of risk and whether it is acceptable or tolerable [21].

2.6.2. Risk Analysis: Risk can be thought of as the chance of adversative moments or damage occurring. Generally, risks can be recognized and the probability of them occurring evaluated [20].

For the qualitative analysis of risk a likelihood impact matrix is mostly created for clear representation of each risk and its impact. The matrix contains the likelihood and impact of each risk event which is assessed against a well-defined scale and plotted on a two-dimensional grid. The relative significance of each risk is represented on the grid with particular position/level. The simplest matrix is formed by classifying both likelihood and impact as either high or low, which leads to a 2 by 2 grid. This basic classification of a high or low value leads to the following rank order for tackling risks [20]:

- High-impact, high-likelihood risks.
- High-impact, low-likelihood risks.
- Low-impact, high-likelihood risks.

Among all three the low-impact, low-likelihood risks have not much importance and are probably not worth expending much effort on for mitigation, they can also be ignored to some extent to save time and extra resources. The most important and critical risks are high-impact, high-likelihood risks they need to be looked one-by-one to conclude whether there are ways either to reduce the impact, if the risk occurs or to reduce the likelihood of the risk occurring, or both [20].

The next stage is to apply quantitative techniques, based on a financial assessment of the impact of each of the risks, to put the risks into order, with the greatest risks at the top of the list [20].

It is beyond the scope of this paper to discuss these techniques which are used to categories the risks into their risk levels. Sometimes, it is hard to reach a decision about the importance of some risks until a corresponding response has been identified as well as any possible interactions between risk events and responses, so risk management is usually iterative in practice [20].

In the risk analysis phase, the risk type and its impact on assets are identified. Further the risk analysis has these few possible steps in case of the Telecommunications and Engineering Laboratory.

Hazard Identification: There are three types of hazards, i.e. Visible Hazards, Hidden Hazards and Developing Hazards. In this study we consider only former two; visible and hidden hazards.

Visible hazards: Visible hazards are the obvious defects that can be readily seen and identified by inspection. To handle with visible hazards is easier as compared to the hidden hazards [22, 23, 24, 25 and 26]. Here we have identified few possible visible hazards associated with Telecommunication and Engineering Laboratory, the hazards cannot be limited to these, but most frequent possible visible hazards are:

Missing Computer Parts: The missing parts of computers can cause the financial loss as well as loss of important data in case: a hard disk is missing or corrupted which contains the important data of students or some critical nature of experimental data.

Missing or Damaged Electronic Equipment's: The equipment's include trainers, voltmeters, digital matters and all the other which are used for experimentation. These equipment's are costly and due to mishap can cause financial loss as well as other damage.

Broken or damaged Chairs: The broken chairs can harm a person like they can cause a serious injury.

Missing lights: The missing lights will cause the low light problem in the laboratory, which can lead to a big problem e.g. cables of an equipment wrongly connected due to dim light.

Missing or damaged Switches: In case of the damage to networking switches, the internet connectivity of laboratory will be heavily affected. The same may happen to the electronic boards/switches which can interrupt the smooth working of the laboratory equipment's.

Damaged Security Cameras: With the damage of security cameras, the security or monitoring of the laboratory will be affected due to which the chances of stolen off the assets increases.

Damaged Electrical Wiring: In this case the loss can be of huge impact like if someone changed the wiring sequence it can cause the serious expulsion/fire and damage the whole laboratory equipment's as well as can damage the physical structure of laboratory.

Hidden Hazards: Hidden hazards are not readily seen without your attention [10]. Examples of hidden hazards are:

Copying data from computers: Copy critical data from the computer for illegal use or stolen personal ideas stored in laboratory taking snapshots of important project diagrams etc.

Changing Default Settings of Trainers: The students mostly change the settings of trainers intentionally or unintentionally that can cause damage to the trainers and other electronic equipment's.

The Toxic gas inside a confined space: Any toxic gas inside the laboratory which can be due to the burning of wires or anything else it can harm the persons working in that place.

Deletion/Change of important data: Intentionally delete data of user or make some minor changes, for example, some student has performed experimentation and stored data in the computer the unauthorized person make some changes into the results.

Stolen Passwords: The unauthorized person grabbed the saved passwords from the laboratory computers for illegal use.

2.7. Risk Mitigation: The mitigation phase is concerned with the reduction of risk. What kind of steps should be taken to reduce the risks?

The risk mitigation means every step take to avoid the risk or automatic solution for mitigation of risk. The key part during this phase is the availability (presence) of spare parts, replacing, auto scanning, self-reboot.

A risk can be mitigated through different ways which are [10].

Automatic risk mitigation means availability of alternative resources. Reactive risk mitigation means risk occurred then mitigate after an occurrence.

So in the given scenario of Telecommunication Laboratory if the risk of Human Resource absence occurs due to some emergency we must have an assistant in the backup to avoid Human Resource absence risk, automatic updating of software's to avoid the risk of corruption, availability of generators to avoid the risk of power failure.

2.7.1 Dealing with Hazards

After identification of a hazard, the need arises to fix it or put it in place controls that minimize the risk of exposure.

2.7.2. Dealing with visible hazards: Proposed Solutions of visible hazards are:

Missing Computer Parts: To avoid the missing of computer parts the list of computers with their full specification should be maintained and the responsible person should be asked to report on monthly basis about the present condition of computers or an audit should be carried out frequently.

Missing or Damaged Electronic Equipment's: To avoid any kind of mishap the students must be guided before using any equipment they refer user manual of the equipment's further during laboratory session the instructor should stay in the laboratory and monitor the students during lab session. Before using the equipment's the person responsible for laboratory will check the equipment's either they are in working condition or not. Further, the Lab In-charge must check the equipment's before and after lab session to ensure that all equipment's are present. For this purpose, he must maintain the list containing equipment's quantity details.

Broken or damaged Chairs: The record of chairs should be maintained in case of damage to chairs the responsible person will report or will explain the cause of damage immediately and the damaged chairs must be replaced with new one.

Missing lights: The missing lights must be reported and must be changed within the certain limit of time after fault identification.

Missing or damaged Switches: In Case of the damage to networking switches, it might be replaced with new one for smooth functioning and same may be reported.

Damaged Security Cameras: The security or monitoring of the laboratory is a critical issue; to avoid any mishap the cameras may be installed on multiple places in lab in case if the one of them damaged the other will remain functioning and the cameras must be monitored from a central control room to avoid entrance of any unauthorized person in the lab the recording of cameras can be also used to identify any mishap.

Damaged Electrical Wiring: To avoid any mishap the wires must be used of good quality and regular checks must be done to identify any fault in the wiring or electric boards.

2.7.3. Dealing with hidden Hazards: Hidden hazards are not readily seen without attention. Proposed solutions of hidden hazards are:

Copying data from computers: To avoid the copying of critical data the Computer systems must be password protected and the external hard disks must be used in the case of very sensitive data and for the backup of important software.

Changing Default Settings of Trainers: The changes in settings can be added into visible hazards, but they require close attention to identifying the changes that's why we included this section. To avoid any damage, the lab In-charge insure after every lab session that the equipment'~~s~~ are set to default settings.

The toxic gas inside a confined space: For the detection of toxic gas, the sensors must be installed inside laboratory which indicate the presence of toxic gasses to avoid any mishap.

Deletion/Change of important data: The frequent backup of data must be kept in the locked folder of computer or in the external hard disk and also the computer must be password protected.

Stolen Passwords: To avoid this passwords must not be saved in computer systems and the auto password save option must not be kept to true.

3. Conclusion

In this paper we have proposed a risk management policy for Telecommunication and Engineering laboratory, we have tried to cover all the possible risks associated with laboratory but still there is need of improvements. In next step, we will improve it further and will increase the scope of the work as well so the same can be implemented at the university level. The assets we included here do not cover all the equipment's because it was not possible to cover all of them in a short paper but we tried to cover all the most important assets. The management of these assets will be the responsibility of laboratory in-charge he will report after every laboratory to the manager of all the laboratories of the university.

References

[1] Y. Zhang and X. Chen, "Developing Digital/Analog Telecommunication Laboratory", American Society for Engineering Education, **(2011)**, pp. 1-11.

[2] G. Moore, "The Development of a Digital Telecommunication Laboratory", ASEE Annual Conference & Exposition, **(2007)**.

[3] F. Wahid, M. Fayaz and A. S. Shah, "An Evaluation of Automated Tumor Detection Techniques of Brain Magnetic Resonance Imaging (MRI)", International Journal of Bio-Science and Bio-Technology, vol. 8, no. 2, **(2016)**.

[4] http://www.szabist-isb.edu.pk/Facilities.asp#TelecomLab.

[5] A. Waqas, Z. M. Yosuf, A. Shah and N. Mahmood, "Sharing of Attacks Information Across Clouds for Improving Security: A Conceptual Framework", International Conference on, Computer, Communications, and Control Technology (I4CT), **(2014)**; Langkawi, Malaysia.

[6] A. Shah, A. Raza, B. Hassan and A. S. Shah, "A Review of Slicing Techniques in Software Engineering", International Conference on Engineering and Technology ICET, **(2015)**; Siri Lanka.

[7] A. Zia, and M. N. A. Khan, "A Scheme to Reduce Response Time in Cloud Computing Environment", International Journal of Modern Education and Computer Science (IJMECS), vol. 5, no. 6, **(2013)**, pp. 56-61.

[8] A. Zia, and M. N. A. Khan, "Identifying Key Challenges in Performance Issues in Cloud Computing", International Journal of Modern Education and Computer Science (IJMECS), vol. 4, no. 10, **(2012)**, pp. 59-68.

[9] A. S. Shah, M. N. A. Khan and A. Shah, "An Appraisal of Offline Signature Verification Techniques", International Journal of Modern Education and Computer Science, vol. 7, no. 4, **(2015)**, pp. 67-75.

[10] http://www.ksgroup.com.au/data/KSF%20LUEZ%20Guidelines%20Nov%202010.pdf

[11] J. H. Nichols, "Laboratory Quality Control Based on Risk Management", Annals of Saudi Medicine, vol. 31, **(2011)**, pp. 223-228.

[12] ISO 31000:2009, Risk Management — Principles and Guidelines.

[13] ISO/IEC Guide 2, Standardization and Related Activities — General vocabulary.

[14] ISO/IEC Guide 51, Safety Aspects — Guidelines for Their Inclusion In Standards.

[15] ISO 10241, International Terminology Standards — Preparation and Layout.

[16] Plain English ISO 31000, Risk Management Dictionary, available at http://www.praxiom.com/iso-31000-terms.htm, **(2009)**.

[17] T. S. Coleman, "A Practical Guide to Risk Management", Research Foundation Publications, **(2011)**, pp. 1-212.

[18] ISO 3534-1, Statistics — Vocabulary and Symbols Part 1: General Statistical Terms and Terms Used In Probability.

[19] S. W. Njoroge and J. H. Nichols, "Risk Management in the Clinical Laboratory", Annals of Laboratory Medicine, vol. 34, **(2014)**, pp. 274–278.

[20] ------"Introduction to Cybersecurity", Open University Lecture Notes, https://www.futurelearn.com/courses/introduction-to-cyber-security, **(2015)**.

[21] https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en.

[22] ISO 9000, Quality Management Systems — Fundamentals and Vocabulary.

[23] R. Antunes and V. Gonzalez, "A Production Model for Construction: A Theoretical Framework", Buildings, vol. 5, no. 1, **(2015)**, pp. 209–228.

[24] ISO 704, Terminology Work — Principles and Methods.

[25] ISO 860, Terminology Work — Harmonization of Concepts and Terms.

[26] ST020 Risk Management, http://www.safetyrisk.net/wpcontent/uploads/downloads/2010/08/RiskManagement_Text.pdf.

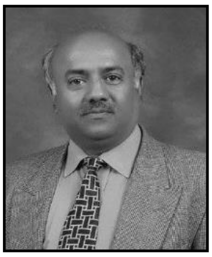
Authors

Abdul Salam Shah, has completed MS degree in Computer Science from SZABIST, Islamabad, Pakistan in 2016. He did his BS degree in Computer Science from Isra University Hyderabad, Sindh Pakistan in 2012. In addition to his degree, he has completed short courses and diploma certificates in Databases, Machine Learning, Artificial Intelligence, Cybercrime, Cybersecurity, Networking, and Software Engineering. He has published articles in various journals of high repute. He is a young professional and he started his career in the Ministry of Planning, Development and Reforms, Islamabad

Pakistan. His research area includes Machine Learning, Artificial Intelligence, Digital Image Processing and Data Mining.

Mr. Shah has contributed in a book titled "Research Methodologies; an Islamic perspectives," International Islamic University Malaysia, November, 2015.

Muhammad Fayaz, is currently perusing Ph.D. in Computer Science from, JEJU National University, South Korea. Before joining the JEJU National University, he has also completed the course work of Ph.D from University of Malakand, Chakdara, KPK, Pakistan. He received MS in Computer Science degree from SZABIST, Islamabad, Pakistan in 2014. He did MSC from the University of Malakand, KPK, Pakistan in 2011.



Asadullah Shah, is working as Professor and Head of department of Information Systems (HOD) at the Kulliyyah of ICT, International Islamic University Malaysia (IIUM) before joining IIUM, he worked as Head of Telecommunication Engineering & Management department, IoBM Karachi Sindh, Dean Faculty of Computer and Management Sciences, Isra University Hyderabad Sindh and Head of Telecommunication Engineering and IT, Sukkur IBA, Sindh-Pakistan.

He did his Ph.D. from the university of Surrey UK, in 1998, with the specialization in Multimedia Communication. He started his academic carrier from University of Sindh Jamshoro, Pakistan in 1986 as a lecturer.

He has published 200 research articles in highly reputable international and national journal in the field of computers, communication and IT. Also, he has published 12 books in his 30 years of the academic carrier. Currently he is supervising great number of postgraduate students, working in multiple disciplines, specially, animation, social media and image processing in the Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia.

Shahnawaz Shah is working as Lecturer at the Institute of Information and Communication Technology, University of Sindh, Jamshoro, Pakistan. He is also pursuing M.Phil. Degree in Telecommunication from the University of Sindh, Jamshoro, Pakistan. He did his BS degree in Telecommunication from University of Sindh, Jamshoro, Pakistan, in 2007.